Ikt.sz.: MATE-K/234-28/2021
Intézményi azonosító: FI51129

MAGYAR AGRÁR- ÉS ÉLETTUDOMÁNYI EGYETEM

30/2021 (XI.04.) számú rektori utasítás az INFORMÁCIÓ BIZTONSÁGI SZABÁLYZAT kiadásáról

A Magyar Agrár- és Élettudományi Egyetem (a továbbiakban: Egyetem vagy MATE) Rektora a nemzeti felsőoktatásról szóló 2011. évi CCIV. törvény felhatalmazása, valamint az Egyetem Szervezeti és Működési Szabályzata I. kötetét képező Szervezeti és Működés Rend (a továbbiakban: SZMR) 54. § (12) bekezdése, valamint az SZMR 7. számú melléklete alapján:

1.§

A Magyar Agrár- és Élettudományi Egyetem tulajdonában vagy kezelésében lévő informatikai rendszerelemek, azaz tárgyak, eszközök, programok, adatok, adathordozók, dokumentumok és az informatikai rendszerekkel kapcsolatba kerülő kezelő, üzemeltető, kiszolgáló, karbantartó és felhasználó személyek vonatkozásában irányadó intézményi szabályokról a jelen utasításhoz mellékleve kiadom az Információ Biztonsági Szabályzatot.

2.§

(1) Jelen utasítás, és ezzel az Információ Biztonsági Szabályzat 2021. november 05. napján lép hatályba.
(2) Jelen utasítás hatályba lépésével hatályát veszti a jogelőd Szent István Egyetem Szenátusa által 2012. október 24-i ülésén a 30/2021/2013 SZT számú határozatával elfogadott Információbiztonsági Szabályzat.
(3) A szabályzat személyi és tárgyi hatályát a melléklet rögzíti.
(4) Az utasítás közzététele az Egyetem honlapján található Munkatársak felületen történik.

Gödöllő, 2021. november 4.

Prof. Dr. Gyuricza Csaba
rektor

Magyar Agrár- és Élettudományi Egyetem 4.

Magyar Agrár- és Élettudományi Egyetem

2100 Gödöllő, Páter Károly u. 1.

INFORMÁCIÓ BIZTONSÁGI SZABÁLYZAT

ver: 1.0

Gödöllő, 2021. november 04.

Jóváhagyta

.....

Prof. Dr. Gyuricza Csaba
rektor

Magyar Agrár- és Élettudományi Egyetem
4.

I. AZ IBSZ VERZIÓSZÁM-KÖVETÉSI TÁBLÁZAT

Ezen táblázat az IBSZ-ek öröklődő részét képezi.

Sorszám	Verzió-szám	Hatályba Lépés ideje	Következő felülvizsgálat várható ideje	Megjegyzés / Módosítás, változás oka	ELRENDELŐ Vezetői Aláírás
1	**1.00**				
2					
3					
4					
5					
6					
7					
8					
9					
10					

II. HELYETTESÍTŐ MÁTRIX

A helyettesítő mátrix a sürgős helyzetek (betörés, természeti katasztrófa, szabotázs, támadás stb.) esetén az azonnal beavatkozást elrendelők és kezdeményezők sorrendjét hivatott feltüntetni.

A táblázatnak minden esetben aktualizáltnak és könnyen elérhetőnek kell lenni.

1. számú melléklet

III. TARTALOMJEGYZÉK

IV. ÁLTALÁNOS RENDELKEZÉSEK

Az Információ Biztonsági Szabályzat (továbbiakban: IBSZ) tárgya a **Magyar Agrár- és Élettudományi Egyetem** (továbbiakban: MATE) tulajdonában vagy kezelésében lévő informatikai rendszerelemek, azaz tárgyak, eszközök, programok, adatok, adathordozók, dokumentumok és az informatikai rendszerekkel kapcsolatba kerülő kezelő, üzemeltető, kiszolgáló, karbantartó és felhasználó személyek.

Az IBSZ célja és rendeltetése

Az IBSZ

a) a hatályos jogszabályokkal,
b) a Közigazgatási Informatikai Bizottság (KIB) ajánlásaival,
c) a Nemzeti Információs Infrastruktúra Fejlesztési Programról szóló 5/2011. (II.3.) Korm. rendeletben meghatározott, a Fejlesztési Program keretében működtetett számítógép-hálózat használati szabályzatával,
d) az MSZ ISO/IEC 27001:2014 szabvánnyal,
e) 2013/ L. törvény (ibtv),
f) valamint a MATE működési és ügyrendi előírásaival összhangban teremti meg a MATE információinak biztonságát.

Az IBSZ kiadásának általános célja a MATE rendszereiben kezelt adatok bizalmasságát, sértetlenségét és rendelkezésre állását illetve a rendszerek funkcionalitását fenyegető veszélyforrások elleni védelmi intézkedések szabályozása, ezáltal a MATE alaprendeltetésből adódó célkitűzései és feladatai teljesítésének biztosítása.

g) Az elektronikus információs, informatikai rendszer és az általa kezelt adatok bizalmasságának, sértetlenségének és rendelkezésre állásának megőrzéséhez kapcsolódó folyamatok az érintett Központok informatikai rendszerének IT Biztonsági Szabályzatában (továbbiakban: IBSZ) leírtakon túlmutató, egyedi, elektronikus információs rendszer specifikus szabályainak meghatározása a MATE IT Biztonsági Politikájában meghatározott, információbiztonsági- és IT szolgáltatás biztonsági alapelveivel összhangban.
h) Az elektronikus információs rendszer fejlesztésében, üzemeltetésében, karbantartásában, támogatásában és használatában résztvevő szervezeti egységek, szerepkörök, munkatársak és külső szervezetek feladat-, felelősség és hatáskörének meghatározása az elektronikus információs rendszer teljes életciklusára vonatkozóan.
i) Az információbiztonság és az IT szolgáltatás biztonság teljes körű szabályozása az elektronikus információs rendszer egyes elemeire a vonatkozó kockázatelemzésre alapozva.
j) Az érintett Központok informatikai és adatbiztonság kialakítása mellett, az Európai-, törvényi, emberi-, informatikai-, adat-, és információ biztonsági elvárásoknak való megfelelés, és rendszerszintű kialakítás.

Az IT Biztonsági Szabályzat célja, hogy meghatározza az adatvédelemmel és információbiztonsággal kapcsolatos fizikai-, logikai-, és adminisztratív feladatokat és felelősségeket, megteremtse az MATE Információbiztonsági és Adatvédelmi-, Adatkezelési és Biztonságtudatossági rendszerének összhangját és elvárásait.

AZ IBSZ HOSSZÚ TÁVÚ CÉLJA AZ INFORMÁCIÓS RENDSZEREK, MARADÓ BIZTONSÁGI KOCKÁZATÁNAK, ELFOGADHATÓ SZINTEN TARTÁSA.

Az IBSZ jellege és kiadásának, módosításának módja

Ez egy korlátozott hozzáférésű dokumentum, amely a MATE egyes informatikai rendszereire részletesen lebontott, az Általános Informatikai Biztonsági Szabályok helyi speciális rendelkezéseit, meghatározó szabályokat tartalmazza. Az IBSZ tartalma a környezet- az alkalmazott eszközök, alkalmazások és technológiák változása okán folyamatosan változhat és változik.

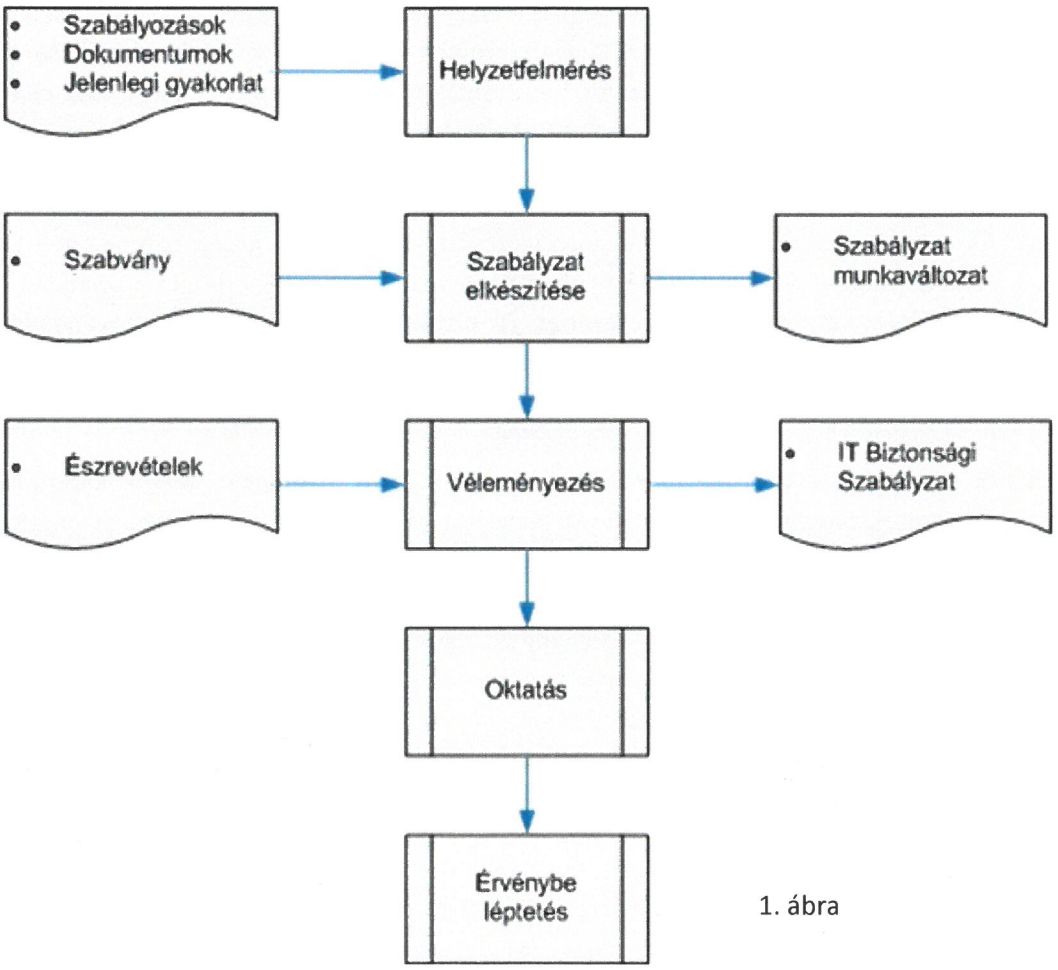
Az IBSZ eljárásrendszere az alábbi munkautasításokat tartalmazza:

a) A MATE informatikai rendszerének, valamint az ehhez kapcsolódó elemeknek a hozzáférési jogosultságok kezelését, az Informatikai rendszer mentési-, archiválási rendjét-, a vírusvédelmi-, információvédelmi rendszer üzemeltetését, a MATE informatikai eszközeinek telepítési és migrálási szabályait, az informatikai erőforrások biztonsági besorolását, és incidens kezelését.

b) Az időszakosan vagy a változásokat megelőző, illetve követő kockázat elemzések rendszerét, és az elvárt kockázati szintek betartásának módszerét.

c) A fejlesztésekhez kapcsolódó kockázatok és elvárások besorolásait, valamint a törvényi jogszabályi biztonsági elemzési követelmények iránymutató alapjait.

d) Meghatározza a jelen szabályzat változtatásának és nyomon követésének rendszerét és módszerét. (1. ábra)



1. ábra

Az IBSZ minősítése

A MATE IBSZ **belső használatú dokumentum.** A belső használatú dokumentumot a MATE munkatársai és szerződéses felei megismerhetik és birtokolhatják, de illetéktelenek részére nem adhatják tovább.

Az IBSZ hatálya

Az IBSZ végrehajtását a hatályba lépésnek megfelelően, kihirdetéstől kezdődően meg kell kezdeni. Az IBSZ a biztonságos információ ellátás érdekében utasításokat tartalmaz, amelyek hatálya kiterjed a MATE informatikai rendszereinek teljes életciklusára (tervezés, fejlesztés, beszerzés, bevezetés, üzemeltetés, kivonás).

Személyi-szervezeti hatály

Az IBSZ személyi-szervezeti hatálya kiterjed:

a) A MATE valamennyi informatikát alkalmazó vagy az informatika környezetében működő szervezeti egységére.
b) A MATE informatikát alkalmazó vagy az informatika környezetében dolgozó valamennyi alkalmazottjára.
c) A MATE-val szerződéses kapcsolatban álló informatikai vagy informatikához kapcsolódó munkát végző természetes és jogi személyekre.
d) Más szervezetek képviseletében a MATE informatikai eszközeit használó munkahelyein vagy ezek környezetében tartózkodó személyekre.

Tárgyi hatály

Az IBSZ tárgyi hatálya kiterjed:

a) A MATE tulajdonában lévő valamennyi informatikai berendezésre (számítógépek, nyomtatók, külső háttértárolók stb.), a számítástechnikai eszközre (aktív hálózati elemek, adathordozók stb.).
b) A MATE területén ideiglenesen használt, a MATE informatikai infrastruktúrájához bármilyen módon kapcsolódó, más szervezetek vagy személyek tulajdonát képező informatikai berendezésekre.
c) A MATE teljes informatikai infrastruktúrájára (szerverek, kliensek, nyomtatók, rack-szekrények, számítógépes vezetékes illetve vezeték nélküli hálózatok, hálózati aktív eszközök, szünetmentes áramforrások stb.).
d) A MATE munkavállalói által használt, a MATE adatvagyonához, vagy informatikai infrastruktúrájához kapcsolódó számítástechnikai eszközökre.
e) A MATE által használt szoftverekre (rendszerprogramok, segédprogramok, alkalmazások, adatbázis kezelők, fejlesztő eszközök, operációs rendszerek, firmware-ek stb.).
f) A MATE informatikai folyamataiban használt összes dokumentációra (tervezési, fejlesztési, üzemeltetési, szervezési, műszaki, informatika biztonsági, fizikai biztonsági dokumentációk stb.).

A papír és elektronikus alapú információk kezelését a MATE Iratkezelési Szabályzata rögzíti.

Területi hatály

Az IBSZ területi hatálya kiterjed a MATE minden alárendelt szervezeti egységére, területi elhelyezkedéstől függetlenül.

Az IBSZ további hatálya

Az IBSZ további hatálya kiterjed:

a) A védelem körébe vont adatok és információk teljes körére, felmerülésüktől, feldolgozási helyüktől és az adatok fizikai megjelenési formájától függetlenül.

Az adminisztratív biztonsági intézkedések életciklusa

Utasítások készítése

Az utasításokat az érvényben levő szakmai, ügyviteli folyamatokra, a folyamatokban résztvevő informatikai rendszerekre és fizikai környezetükre vonatkozó nemzetközi és hazai szakmai szabályok, normák, szabványok előírásait, ajánlásait figyelembe véve és követve kell kialakítani, melyért az Informatikai Igazgatóság felelős.

Érvényesítés

a) Az IBSZ-ben előírt eljárások és szabályok érvényesítése hagyományos vezetési eszközökkel történik, melynek elemei:
   1. Irányítás (tervezés, feladatszabás, előírások stb.)
   2. Ellenőrzés
   3. Felelősségre vonás

Az IBSZ megismerhetősége

a) Részben és egészben minden olyan érintett személyek megismerhetik a jelen IBSZ-t, akik a Szervezet alkalmazásában állnak, illetve annak területén a Szervezet részére végzendő munkájukhoz, tevékenységükhöz szükséges (munkavégzésükhöz szükséges- és elégséges módon) nagyságrendben kell, hogy megismerjék az IBSZ tartalmát.

b) Az általános Informatikai Biztonsági Szabályok összefoglalják az informatikával dolgozó alkalmazottak, felhasználók kötelességeit, az általuk elvégezhető és tiltott tevékenységeket, a számonkérés formáját, valamint a biztonsági események jelentésével kapcsolatos kötelezettségeiket.

c) A MATE területére a MATE IT rendszeréhez kapcsolódó belépő vendégek, külsős személyek, szerződéses alkalmazottak, illetve szerződött partner alkalmazottai részben a belépés során, az IT hálózathoz történő csatlakozást megelőzően, részben a munkavégzés helyén lévő vendég és külsős személyek részére készített kivonatolt IBSZ leírásból vagy az alkalmazottak általi tájékoztatásból csak a tevékenységükhöz szükséges és elégséges mértékben ismerhetik meg.

Az IBSZ oktatása

a) Az IBSZ-t meg kell ismertetni, és a biztonságtudatosság kialakítása miatt oktatni a szervezet minden tagja számára oly módon, hogy a munkájukhoz és munkavégzésükhöz szükséges minden informatikai biztonsági szabályzatot ismerjenek.

b) Az informatikával és adatkezeléssel foglalkozók ismerjék meg a fenyegetettség és a biztonság kérdéseit, kapjanak tájékoztatást a szabályzat betartásának szükségszerűségeiről és sajátítsák el a Szervezet biztonság tudatossági elvárásait.

c) Az IBSZ oktatását **meg kell ismételni minden** az IBSZ-t érintő változás esetében a változás tárgyáról, valamint ennek hiányában, **évente egyszer** a biztonságtudatosság fenntartásának és az új fenyegetések megismertetésének érdekében.

d) Az IBSZ oktatását a helyzettől és a dolgozók feladatainak mennyiségétől függően lehet direkt, személyes oktatással vagy e-learning oktatással teljesíteni.
e) Az oktatásban részesülők aláírásukkal igazolják és ezzel elfogadják és tudomásul veszik, hogy az IBSZ-t és a személyükre vonatkozó tartalmi szinten megismerték és kötelezően betartják (az aláírt az oktatás rendszerét és tematikáját tartalmazó aláírt nyomtatványokat a munkatárs munkaügyi nyomtatványai között 5 évig meg kell őrizni). E-learningben történő oktatás esetén nincs szükség a résztvevők aláírására.

V. AZ INFORMÁCIÓ BIZTONSÁGI RENDSZER MŰKÖDTETÉSE

1.1 Megfelelés a jogszabályoknak és a belső szabályzatoknak

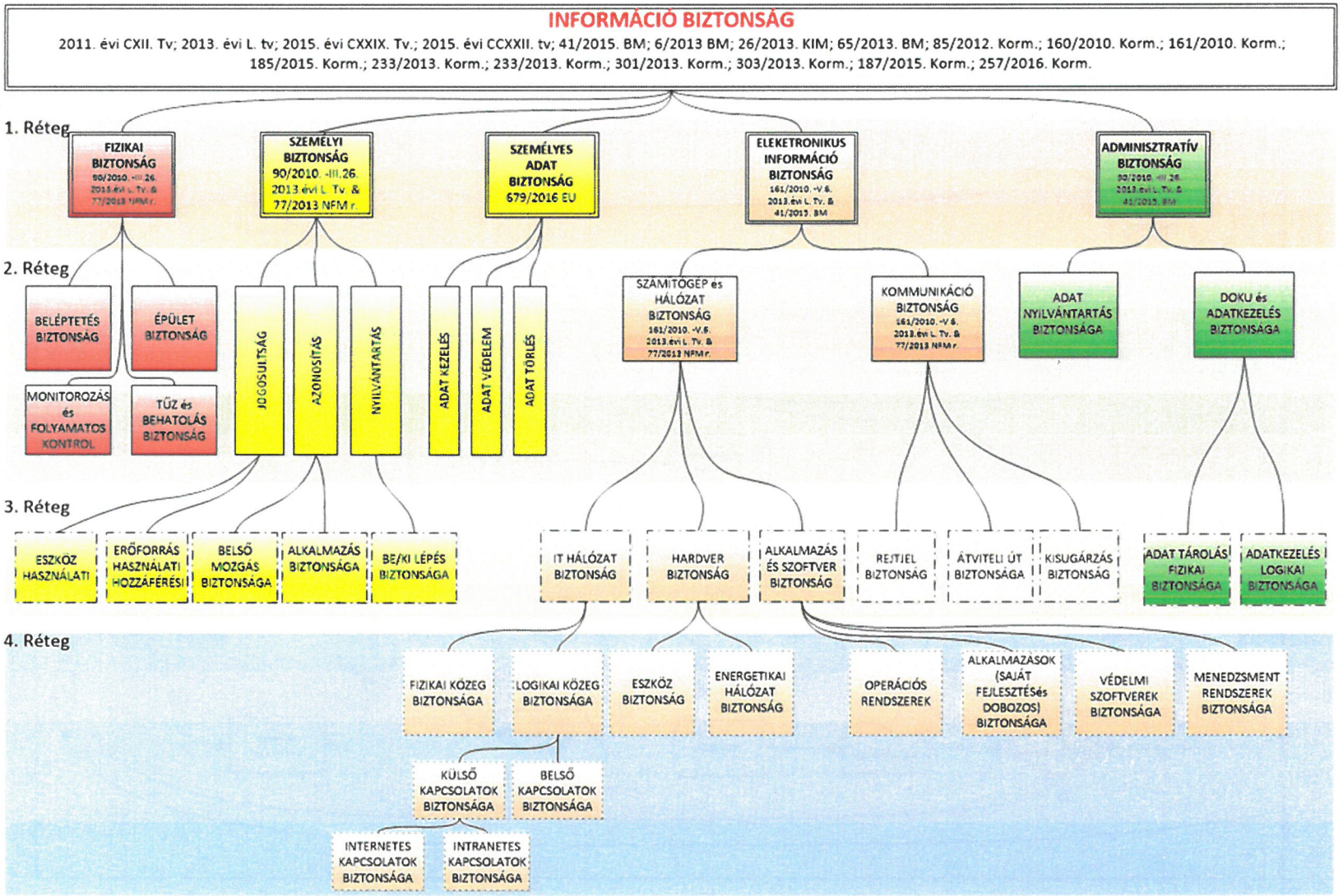
Az IBSZ kialakításának, valamint a szabályozott tevékenységek és rendszerek körénél figyelembe kell venni a következő jogszabályokat, szabványokat és ajánlásokat:

a) **2015. évi CCXXII**. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól
b) Az Európai Parlament és az Európai Tanács 2016/679 Rendelete. Általános Adatvédelmi Rendelet (GDPR)
c) **2013. évi L**. törvény
d) **2009. évi CLV** törvény a Minősített Adat Védelemről MAV tv
e) **2011. évi CXII** törvény Az információs önrendelkezési jogról és infószabadságról
f) **2015. évi CXLIII.** törvény a közbeszerzésekről
g) **2011. évi CCIV.** törvény a nemzeti felsőoktatásról
h) **466/2016. (XII.28.)** Kormányrendelet a Kormányzati Adat Tárházról
i) **41/2015. (VII.15.)** BM rendelet az állami és Központi szervek elektronikus információ biztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről
j) **42/2015. (VII. 15.)** BM rendelet az elektronikus információbiztonságról szóló törvény hatálya alá tartozó egyes szervezetek hatósági nyilvántartásba vételének rendjéről
k) **187/2015. (VII. 13.)** Korm. rendelet az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről
l) **185/2015. (VII.13)** Korm. rendelet az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról 26/2013 (X.21) KIM_rendelet az Információ biztonsági felelősök oktatásáról
m) **1139/2013. (III.1.)** Korm. határozat a Kiberbiztonságról
n) **78/2010 (III.25)** Korm. rend Az elektronikus aláírás közig használatának szabályairól
o) **161/2010 (V.6)** Korm. rendelet a minősített adat biztonságáról és rejtjeltörvényről
p) **MSZ ISO 27001-2014** Információ Biztonság-irányítási rendszerek követelményei (szabvány ajánlás)
q) **MSZ ISO/IEC 15408-1; 2; 3 Common Criteria –CC-** (Ajánlás az Informatikai és biztonság szabályozásáról)
r) **COBIT 4** ajánlás
s) **KIB 19-29** (kormányzati informatikai bizottság ajánlásai)

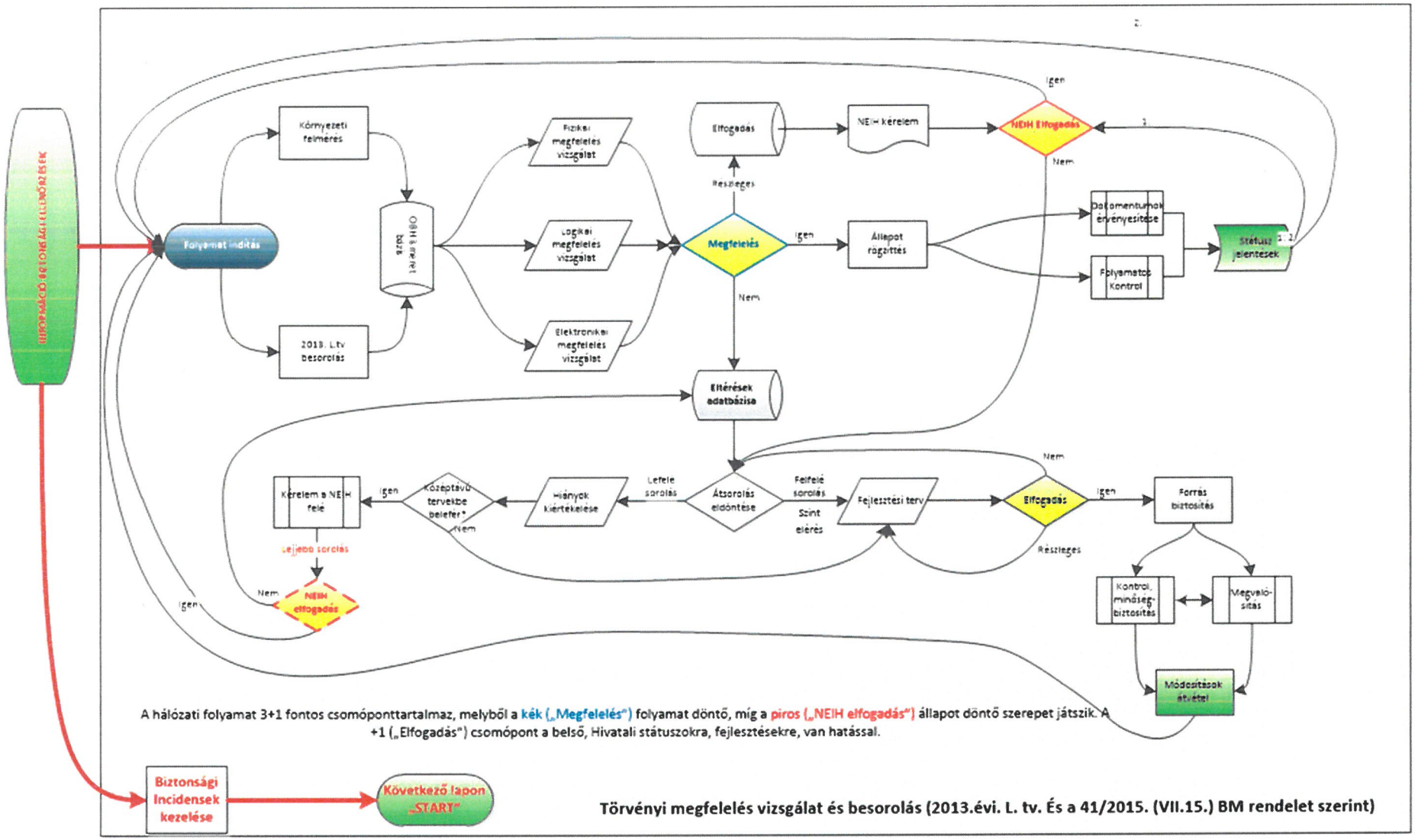
Továbbá a MATE működése követi a rá vonatkozó törvényi előírásokat és jogszabályokat, valamint a jelen IBSZ-en túl a következő belső szabályzatokat:

1. A MATE Szervezeti és Működési Rendje
2. A MATE Iratkezelési Szabályzata
3. A MATE Adatvédelmi Szabályzata
4. A MATE Beszerzési Szabályzata
5. A MATE Vírusvédelmi Szabályzata
6. A MATE Leltározási Szabályzata

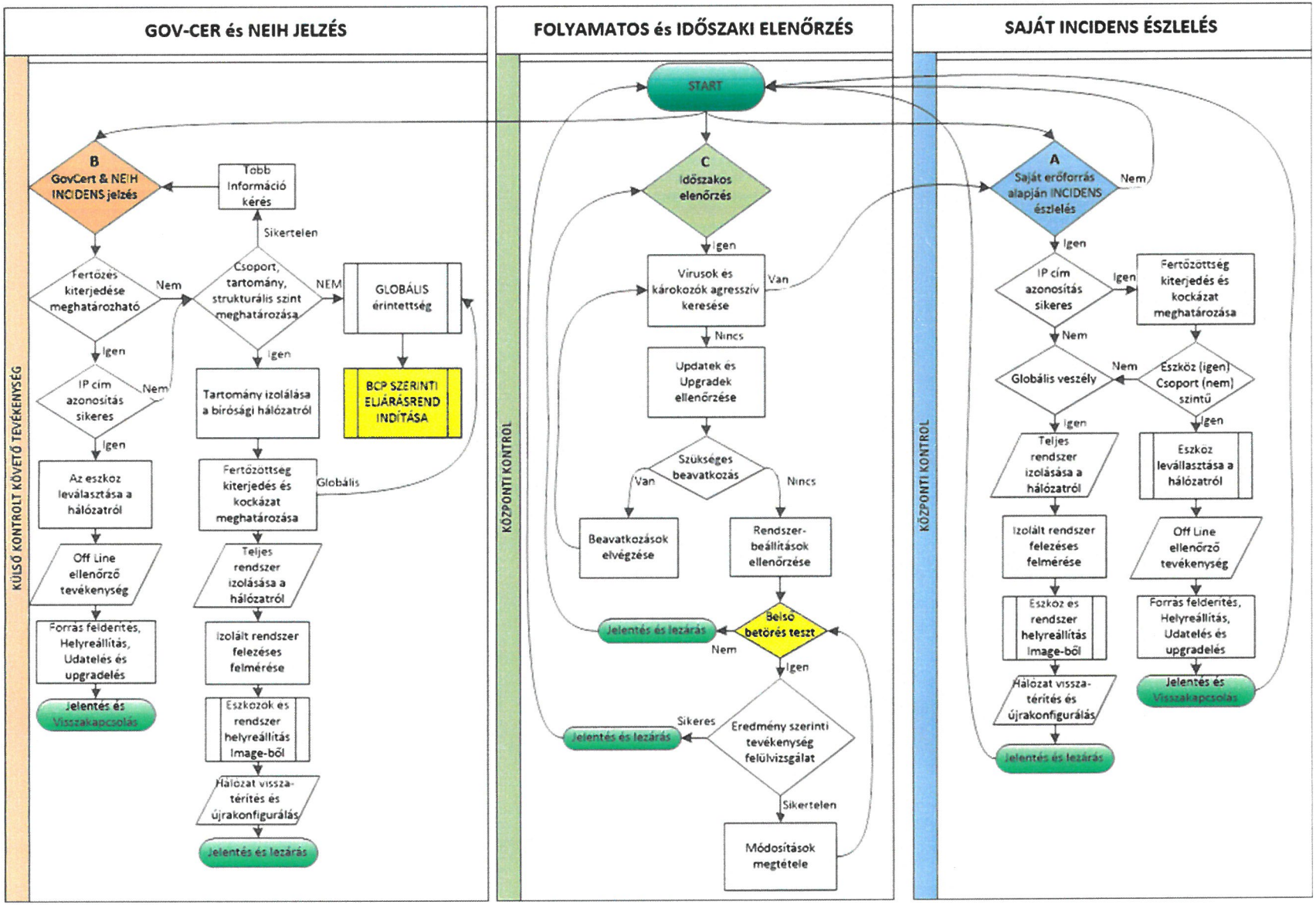
1.2 Információ Biztonság Érintett Területei



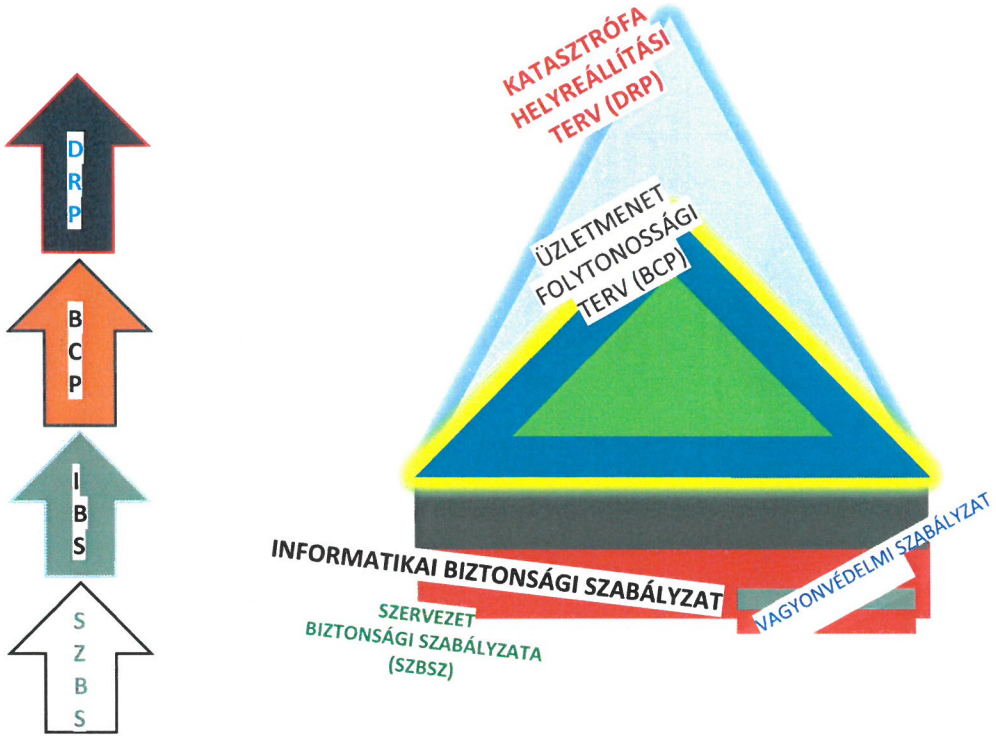
1.3 Információbiztonsági Vizsgálatok Folyamata (4. sz. ábra)



1.4 Incidens kezelés folyamata (5. sz. ábra)



Az IBSZ és társ dokumentumok kapcsolat:



2. ábra

Helyesbítő-megelőző intézkedések rendszere

Azokra a fenyegetettségekre, amelyekre szabályzatban nem rögzített eljárások, előírások, illetve a technikai eszközök nem adnak megoldást, az alábbi eljárásrend érvényes:

Az információbiztonsági rendszerrel kapcsolatos nem megfelelő működésekről, észrevételekről, javaslatokról a MATE bármely dolgozója köteles tájékoztatni az adott intézeti/alkalmazásgazdáját vagy az Informatikai igazgatóság illetékes informatikusát, illetve az adatvédelmi tisztviselőt.

A bejelentésekről az Informatikai igazgatóság illetékes informatikusa tájékoztatja az adatvédelmi tisztviselőt, illetve az informatikai igazgatót.

Az adatvédelmi tisztviselő és az informatikai igazgató, bejelentéseket megvizsgálja, azokra intézkedési terveket dolgoz ki, amelyeket a MATE vezetője elé terjeszt jóváhagyásra. Jóváhagyás esetén az információbiztonsági rendszer fejlesztése, módosítása az adatvédelmi tisztviselő és az informatikai igazgató felügyelete mellett történik.

VI. AZ IBSZ FELÜLVIZSGÁLATI KÖTÖTTSÉGE

Az IBSZ időszakos karbantartási és felülvizsgálati célja, hogy az IBSZ tartalma mindenkor megfeleljen az aktuális üzemeltetési és felhasználói környezetnek, a benne szabályozott feladatok végrehajthatók legyenek és ezáltal számon kérhetők.

Jelen IBSZ esetében kétfajta dokumentum karbantartást írunk elő:

a) RENDSZERES, legalább évente egyszer
b) ESETI, minden a szabályzatot érintő elem (HW, SW, Infrastruktúra) változás esetére

Az IBSZ-t verziókövetéses adatlappal kell ellátni, tartalmát megújítani a változáskövetést igénye szerint.

Rendszeres karbantartás

A szabályzatban meghatározott gyakorisággal (évente egyszer), az ezzel megbízott személynek át kell tekintenie a Szabályzat aktualitását és a változásokat a MATE engedélyeztető testületi elfogadása után a verziókövető lapra rá kell vezetni.

Eseti karbantartás

Új eszközök (hardver, szoftver) bevezetése, az üzemeltetési vagy a működési folyamatok változása miatt eltérés alakulhat ki a szabályozás és a gyakorlat között. Ezeket a változásokat úgy kell végrehajtani, hogy azok bevezetésével egy időben a biztonsági intézkedések felülvizsgálata és azok szabályozásának felülvizsgálata is megtörténjen és a szükséges módosítások dokumentálásra kerüljenek.

Fontos, hogy az éves tervek és célkitűzések tükrözzék a hiányok és javítások koncepcióját, valamint az új beruházások a 41/2015 (VII.15) BM rendelet és a 42/2015 (VII.15) BM rendelet szellemében illetve az ott felsorolt elvárásokkal összhangban legyenek.

VII. A MATE ÁLTAL KEZELT ADAT TÍPUSOK

Az elektronikus információs rendszerben tárolt személyes és iparági- és szellemi termék adatok kezelése csak meghatározott célból, megfelelő védelemmel történnek, és a törvény által biztosított módon, csak a szükséges mértékben és szükséges céllal, ideig és jogcímmel kerülnek tárolásra.

A nevezett elektronikus információs rendszerben kezelt felhasználók nyilvántartott személyes adatai a következők:

Adatok megnevezése	Adatkezelés jogcíme	Adatkezelés célja / időtartama
a) Személyes adatok b) Különleges személyes adatok c) Oktatással összefüggő személyes adatok d) Szellemi termékek köre (tudományos kutatások és eredményeik) e) Adózást érintő adatok f) Cégadatok	a) Adózásra vonatkozó törvény b) Munkavállalási szerződés szerint c) Tanulmányi szerződés d) Kutatás-, innovációs tevékenységek eredményei és szabályai e) Nemzeti Minősített Adatkezelés	A vonatkozó törvények és rendelkezések szerinti időtartamban és céllal. A jogszabályokban meghatározott időtartamban, formában és védelemmel.

1.1 A MATE ÁLTAL KEZELT SZEMÉLYES ADAT TÍPUSOK

A MATE az EU parlament és tanács 679/2016 rendelete (GDPR) értelmében a személyes adatok kezelésének a szervezetnek a magyar jogszabályi célhoz kötöttségi kezelésen kívül (**2011. évi CXII** törvény Az információs önrendelkezési jogról és infószabadságról), csak a 679/2016. EU Parlament és Tanács rendeletének megfelelő időtartamig és formában kezelheti.

A jogszabályi hivatkozások alapján a MATE által kezelt személyes adatokról az adat tulajdonosokat tájékoztatni kell, valamint az általuk adott engedélyeket írásos (személyes aláírt papírt, vagy elektronikusan aláírt elektronikus dokumentum) formájában a jogszabályi elvárások szerint, de legfeljebb a szükséges adatkezelést (kilépést) követően azonnal, vagy a jogszabályi engedmények szerint maximum két évig lehet megőrizni. A személyes adatok törlését az érintett személy tudomására kell hozni.

Nem törölhetők azon személyes adatok melyek a személy életútjára vonatkozó szervezeti szintű kötelező igazolásokat jelentik (egészségügyi biztosítás, adózás rendje, nyugdíj jogviszony számítás igazolása).

Személyes adatok kategóriája	**Adatkezelés jogcíme**	**Adatkezelés célja/időtartama**
a) Személyes adatok b) Különleges személyes adatok c) Oktatással összefüggő személyes adatok	a) Munkaviszonyból adódó adózás rendje b) Egészségbiztosítás rendje c) Nyugdíjbiztosítási életút d) Szellemi tevékenység jogállása e) Tanulmányi szerződés	A vonatkozó törvények és rendelkezések szerinti időtartamban és céllal.

VIII. A MATE INFORMATIKAI RENDSZERÉNEK ELVÁRT BIZTONSÁGI OSZTÁLYA

Az elektronikus információs rendszer a 3. legmagasabb biztonsági osztályba került besorolásra a következő kockázati tényezők szerint:

ELVÁRT Osztály és szintek			
Védelmi intézkedések szerint	**A felmérés szerint elvárt kockázati osztály**		
	Bizalmasság	**Sértetlenség**	**Rendelkezésre**
Adminisztratív védelem szempontjából:	3		
Fizikai védelem szempontjából:	3		
Logikai védelem szempontjából:	3	3	3

A biztonsági osztályba sorolást annak elérése után évente felül kell vizsgálni és az esetleges eltéréseket a NKI felé írásban jelenteni kell.

IX. A MATE INFORMATIKAI RENDSZERÉNEK FELMÉRT BIZTONSÁGI OSZTÁLYA

A MATE a jogszabályi felméréseket elvégezve a 41/2015 (VII.15.) BM rendelet szerint a HTTP://NKI.GOV.HU/URLAPOK SZVI és OVI lapjának kitöltésével a MATE Informatikai rendszerének jelenlegi biztonsági osztályai a következők:

TÉNYLEGES (felméréskori) osztályok és szintek	
Védelmi intézkedések szerint	**A tényleges (elért) biztonsági osztálya**
Adminisztratív védelem szempontjából:	3
Fizikai védelem szempontjából:	1
Logikai védelem szempontjából:	2

Az 1. szintű osztályeltérést a Központ a törvényileg előírt 2 év alatt teljesíti. A szintlépésekre a Központ elkészíti a Cselekvési tervet.

A MATE a felmérést követően a 2013.évi L: törvény szerint köteles 90 napon belül elkészíteni a biztonsági osztály szintjavításához szükséges cselekvési tervet.

X. A BIZTONSÁGI INCIDENSEK KEZELÉSE, JELENTÉSE

1.1 Alapszabályok

Minden biztonsági incidenst, mely a MATE-t, illetve annak informatikai rendszerét Információvédelmi szempontból érinti, köteles a megnevezett szervezeteknek (GOVCERT, NKI) irányában jelenteni.

A folyamatos ellenőrzés és felügyeleti tevékenységet a 4. sz. és 5. sz. ábra folyamatai szerint kell elvégezni.

A biztonságot érintő eseményeket a törvényi megfelelés szerinti szervezetek mellett a szervezet vezetője felé is azonnal jelenteni szükséges.

1.2 Incidens jelentésnek tartalmaznia kell:

a) Az incidens helyét.
b) Az incidensben érintett csoport, gép azonosítását (IP cím, MAC cím, operációs rendszer, érintett adatbázis, érintett applikáció neve, típusa).
c) A vírusvédelmi rendszer és az operációs rendszer utolsó frissítésének (upgrade) idejét.
d) Az incidensben érintett személyeket.
e) Az incidens környezeti paramétereit (hozzáférhetőség, logikai, fizikai).
f) Az Incidens vélelmezhető bekövetkezésének okát.
g) Az incidens kivizsgálását végző személy(ek) adatait.
h) Az incidens során érintett adat(ok) sérülékenységét (adatvesztés, adatszivárgás, kockázat mértéke).
i) A jelentett esemény a MATE informatikai rendszerekre gyakorolt hatását
j) Az eddig megtett elhárító intézkedések sorát.

k) Az események kapcsán tervezett rendszervédelmi intézkedések és kidolgozásainak határidejét.
l) Az incidens kapcsán sérül-e a besorolási (elvárt, elért) biztonsági szint.
m) Szükséges-e sérülékenység vizsgálatot futtatni?

1.3 A GOVCERT incidens bejelentési szabályai

Címe: HTTP://WWW.CERT-HUNGARY.HU/INCIDENSBEJELENTES

„Az incidens bejelentéseket célszerű elektronikus levél formájában elküldeni Központunknak a leggyorsabb és leghatékonyabb incidenskezelés és információ közlés érdekében, az alábbi elérhetőségen:
E-mail: CERT@CERT-HUNGARY.HU
PGP: HTTP://WWW.CERT-HUNGARY.HU/PGP/TEAM

Az egyes bejelentések kapcsán a GOVCERT kéri minden rendelkezésre álló releváns információ (e-mail fejléc, naplófájl, stb.) megküldését, mely szükséges az incidens teljes megértéséhez, így segítve a CERT Központot a megfelelő intézkedések mihamarabbi megtételében."

Az elektronikus levélen kívül lehetőség van Központtal telefonon vagy faxon is kapcsolatba lépni, az alábbi elérhetőségeken:

Tel.: 00 36 (1) 336 4833
Fax.: 00 36 (1) 336 4886

FONTOS:
A GOVCERT felhívja az érintett szervezetek figyelmét, hogy amennyiben még nem éltek bejelentési kötelezettségükkel, úgy az első kapcsolatfelvétel alkalmával kiküldött visszaigazoló levelet mindenképpen küldjék vissza a CERT Központnak, mivel ellenkező esetben a rendszerük a bejelentést kéretlen levélnek minősíti.

1.4 Az információbiztonsággal kapcsolatos felügyeleti szervezetek

A MATE informatikai rendszeréért és biztonságáért a törvény szerint a szervezet vezetője vagy az általa ezzel megbízott személy felel. (2013.évi L. tv. 11.§)

Az Információbiztonsági felügyeletet a kinevezett, és a NKI (Nemzeti Kibervédelmi Intézet) által elfogadott információvédelemért felelős személy látja el, aki rendelkezi a 2013.évi L. törvényben foglalt elvárásokkal és közvetlen az MATE vezetőjének irányítása alatt működik.

Minden incidens, információ biztonságot érintő esemény az Információ védelmi felelős fennhatóságába tartozik.

Az információbiztonsággal kapcsolatos események, észrevételek bejelentése mindenki számára kötelezőek.

A bejelentés módja azonnal telefonon és írásban, e-mailben lehetséges az esemény részletes leírásával (mi történt, hol történt, melyik és milyen eszközön történt, mikor történt, történt-e azonnali ellenintézkedés).

1.5 A NKI hatósági jogköre

A 2013. évi L. törvény szerint a MATE és a MATE ASP rendszer felsőbb (kormányzati és hatósági) ellenőrzését a **Nemzeti Elektronikus Információbiztonsági Hatóság** (NKI, elérésük: WWW.NKI.GOV.HU, tel: 00 36 (1) 336 4833, fax: 00 36 (1) 336 4886, e-mail: CERT@CERT-HUNGARY.HU) látja el együttműködve a Nemzeti Kiberbiztonsági tanáccsal, a Nemzeti Biztonsági Felügyelettel, valamint a GOVCERT-tel egyetemben.

A MATE Rektora tudomásul veszi, hogy a NKI jogkörénél fogva hiány, nem megfelelés esetén, külön Információbiztonsági Felügyelőt delegálhat a szervezethez a kritikus állapot kiküszöbölése végett a (2013. évi L. törvény 16.§ (3) c) pontja értelmében. A szervezet köteles együttműködni a delegált felügyelővel valamint az azt támogató Nemzeti Biztonsági Felügyelettel. A MATE tudomásul veszi, hogy a NKI a nem megfelelés és súlyos hiányok esetén pénzügyi bírsággal is sújthatja az egyetemet.

Az már ismert, vagy várható információbiztonságot érintő eseményekről és incidensekről a GOVCERT-hungary.hu (Kormányzati eseménykezelő Központ) ad jelzést illetve küld figyelmeztető e-mailt. A jelezett események kezelése azonnali hatályú.

1.6 NKI és GOVCERT ELÉRHETŐSÉGEK (jelentési címek)

	GOVCERT
Telefonos bejelentés / elérhetőség	00 36 (1) 336 4833
Faxon történő jelentés:	00 36 (1) 336 4886
Elektronikus elérhetőség / bejelentés	CERT@CERT-HUNGARY.HU
PGP Elektronikus elérhetőség	HTTP://WWW.CERT-HUNGARY.HU/PGP/TEAM
Segítség kérés	HTTP://WWW.CERT-HUNGARY.HU/INCIDENSBEJELENTES

1.7 A bejelentendő incidensek rendszere

A **X. 1.2.** pontbeli felsorolás szerint kell, hogy történjen, figyelembe véve a **X. 1.8** bekezdésben foglalt elvárásokat.

1.8 A bejelentendő incidensek típusai

A szervezetnél bekövetkező incidenseket (rendkívüli információbiztonsági eseményeket, melyek a szabályos működést megzavarják, illetve a szervezet adatvagyonában vagy annak közvetlen környezetében káros változásokat okoznak), jelenteni kell A HelpDesk felé, aki szükség esetén értesíti a MATE vezetőjét illetve az Információbiztonsági felelőst, aki lejelenteni a NKI és a GOVCERT felé:

a) **Sikeres vírustámadás** (nem jelentendő a vírusvédelmi rendszer által detektált és kiszűrt alacsonyabb szintű, automatikusan elhárított vírusészlelés).
b) **Ransomware (zsaroló vírus)** megjelenése (támadás szempontjából sikertelen és sikeres esetben is), a fertőzés azonosítója és vagy típusa (sikeres támadás esetén a képernyőkép).

c) **Behatolási detektálás** (tűzfal, szerver, kliens gép esetén) szerinti felderítése a behatolás mértéke és a vizsgálat módja, az ellenintézkedés megtételének módszere.
d) **A rendszert ért sikeres külső internetes támadások** mindegyike (a támadás módja és formája).
e) **Az incidensek által bekövetkezett kár mértéke és formája** (típus, értékvesztés, értékviszony a szervezet információs vagyonához viszonyítva).
f) **A fizikai támadás (betörés, hozzáférés, lopás stb.) esetén** az érintett számítógép típusa, azonosítója (IP, MAC, gyári szám); az számítógépen tárolt (amennyiben helyi tárolás is történik) adat típusa, mennyisége; a kompromittálódott adat és belépési pontok (név, jelszó stb.) típusa formája és jogosultságai, adatbázis elérési kapcsolatai.
g) **A támadások közben-, után megtett biztonsági intézkedések típusai,** formái és végrehajtói.
h) **A támadás utáni kárenyhítés során végrehajtott kivizsgálások** és tevékenységek dokumentumai.

Minden lejelentésnek és vizsgálati anyagnak a szervezet vezetője vagy megbízottja által aláírt, információvédelmi felelős által elkészített dokumentumnak kell lennie. A lejelentés formája szerint e-mailen (elektronikusan és szkennelt PDF dokumentum formájában) kell megtörténnie.

Minden, a X. 1.8 pontban felsorolt bekövetkezett incidenst az incidens felderítését követően 72 órán belül a megadott (X. 1.6 pont) címeken jelenteni kell.

XI. AZ IBSZ-BEN HASZNÁLT SZEREPKÖRÖK ÉS JOGKÖRÖK

1.1 Üzemeltetésért felelős szervezeti egység (szolgáltató)

Az IT Biztonsági Szabályzatban általános jelleggel meghatározott feladatokon túlmenően az elektronikus információs rendszer biztonságával kapcsolatosan feladatai a következők:

a) Jelen IBSZ-ben foglaltak betartása és annak betartatása,
b) Információbiztonság és IT szolgáltatás biztonság szintjének megőrzése,
c) Elektronikus információs rendszer üzemeltetésének és üzemeltetési körülményeinek biztosítása,
d) Felhasználói hozzáférés jogosultsági kérelmek beléptetése, engedélyezése és visszavonása, felhasználói jogosultságok beállítása azon rendszereknél, ahol ez az üzemeltető informatikus feladata,
e) Kapcsolódó dokumentumok és adatok külső partnerek részére történő átadásának a Szervezet vezetői engedéllyel és dokumentáltan történő kivitelezése (szükség esetén),
f) Adatkörök bizalmasságával, sértetlenségével és rendelkezésre állásával kapcsolatos vétlen károkozások vagy tudatos visszaélések kivizsgálása, a védelmi intézkedések és a szükséges szankciókra javaslat tétel, új elvárások érvényesítése,
g) Elektronikus információs rendszer eléréséhez használt számítógépeken üzemeltetett szoftvereszközök jogtisztaságának biztosítása,
h) Az üzemeltetett rendszerek biztonsági szintjének megtartatása mellett a maradvány kockázatok minimalizálása,
i) Az időszakos kockázatfelmérésekben történő aktív közreműködés a szervezet Információbiztonsági felelősével.

1.2 Az informatikai rendszer tulajdonosa

Az informatikai és elektronikus eszközök tulajdonosai és elérhetőségeik:

Magyar Agrár- és Élettudományi Egyetem

2100 Gödöllő Páter Károly u. 1.

A **MATE** által az informatikai biztonsággal kapcsolatos feladatkiadásra, teljesítésigazolásra és kapcsolattartásra jogosultak: *2. számú melléklet*

Információ Biztonsági Felelős

3. számú melléklet

Az intézmény vezetője által kinevezett azon vezető, aki az IBSZ kiadásáért és megfelelőségéért felel, továbbá:

a) Mindazon anyagi és erkölcsi feltétel biztosítása, amely szükséges az elektronikus információs rendszer, rendszerbiztonsági tervek megvalósításához, valamint a jelen IBSZ által meghatározott módon és mértékben az elektronikus információs rendszer biztonságos és megbízható üzemeltetéséhez,
b) Az elektronikus adatfeldolgozó és kezelő rendszer, valamint annak személyi és fizikai környezete minden elemén a teljes körű, zárt és a kockázatokkal arányos szintű védelem biztosítása, és ennek ellenőrzési felügyelete,
c) Döntés az Elektronikus információs rendszer törvényi biztonsági osztályba sorolásáról,
d) Az információbiztonsági és IT szolgáltatás biztonsági követelmények betartásának ellenőrzése,
e) Elektronikus információs rendszerben a felhasználók jogosultságainak jóváhagyását, ellenőrzését végző felelős személy kijelölése, és/vagy a személyek jogosultsági szintjeinek meghatározása,
f) Információbiztonsági incidens esetén az intézkedések kezdeményezése és végrehajtásuk ellenőrzések, a vizsgálat során feltárt hiányosságok megszüntetésére az intézkedések elrendelése,
g) Vizsgálati eljárás kezdeményezése és lefolytatása a tudomására jutott biztonságsértő eseményekkel kapcsolatosan,
h) Észlelt biztonsági események rögzítése és az ezzel kapcsolatos információk eljuttatása az IT biztonság irányításáért felelős személyhez,
i) Súlyossági fokozattól függően munkaügyi szankciók vagy büntetőjogi eljárás kezdeményezése az elektronikus információs rendszer biztonságát sértő biztonsági események bekövetkezése esetén,
j) Az információbiztonsági felelős beszámoltatása és ellenőrzése az intézmény vezetője vagy helyettese által.

A biztonsággal összefüggő operatív ügyekben a megbízásából és nevében az elektronikus információs rendszer üzemeltetéséért / támogatásáért felelős szervezeti egység vezetője jár el.

1.3 Üzemeltetésért / támogatásért felelős személy (szervezet)

Az üzemeltetésért / támogatásért felelős szervezeti egység vezetője: *4. számú melléklet*

Az üzemeltetésért / támogatásért felelős szervezeti egység szerepkör szintű feladatai, felelősségei és hatáskörei az alábbiak:

a) Szervezet vezetőjének megbízása alapján végzi az elektronikus információs rendszer üzemeltetéséhez/támogatásához kapcsolódó operatív tevékenységeket (pl.: mentések elvégzése, jogosultság kiadás, visszavonás ellenőrzése, naplózási eseményekről szóló jelentések fogadása, jelentési kötelezettség és kapcsolattartás a Központ vezetőjével, valamint az informatikai incidensek elhárításának irányítása stb.),
b) Hatáskörében javaslatot tesz az elektronikus információs rendszer üzemeltetéséhez/támogatásához szükséges anyagi és személyi erőforrások biztosításának allokálására, beszerzésére,
c) Hatáskörét túllépő döntések esetén a feladatot a Szervezet vezetője felé eszkalálja, a döntés meghozatalához szükséges információkat átadva,
d) Elektronikus információs rendszer működését/támogatását veszélyeztető biztonsági incidensekről haladéktalanul jelentést tesz elsősorban a Szervezet vezetőjének (vagy az általa kijelölt helyettesítő személynek), továbbá az Informatikai biztonság felelős személy felé.

1.4 Kiemelt felhasználók (adminisztrátori jogkörrel rendelkezők)

A kiemelt felhasználók (adminisztrátorok, illetve adminisztrátori joggal rendelkező személyek) szerepkör szintű feladatai, felelősségei és hatáskörei az alábbiak:

a) Elektronikus információs rendszer kiemelt felhasználóinak feladata a felhasználók kötelezettségén túl a felhasználói szerepkört betöltő munkatársak szakmai támogatása, biztonságtudatának erősítése, biztonsági problémáik megoldásának segítése, javaslattétel új biztonsági megoldások bevezetésére,
b) Az információbiztonsági ismeretek átadása és a felhasználói információbiztonság tudatosságának ellenőrzése.

A kiemelt felhasználók kiválasztása során mind szakmai, mind biztonsági szempontból fokozott gondossággal kell eljárni. Ilyen jogosultság megadásához legalább 1 éves, a szervezetnél fennálló folyamatos munkaviszony vagy vezetői beosztás szükséges.

Az ilyen jellegű tevékenység végzésekor, külsős szervezet, szolgáltató, ilyen szerepkört betöltő alkalmazottai csak a MATE rektorának vagy az általa kijelölt személy jóváhagyásával, és/vagy az azonos szerepkört betöltő felhasználójának felügyeletével férhetnek hozzá az elektronikus információs rendszerhez.

1.5 Felhasználók

A felhasználók szerepkör szintű feladatai, felelősségei és hatáskörei az alábbiak:

a) A legjobb tudásuk szerint, körültekintően és az általa kezelt rendszerre odafigyeléssel, a biztonsági szabályok betartásával végzik feladatukat,
b) Elektronikus információs rendszer használata során az azonosítási és hitelesítési, a rendszerhasználati és a jogosultsági szabályokat betartják,
c) Elektronikus információs rendszer használata során az észlelt szokatlan, rendkívüli vagy biztonsági eseményeket azonnal a közvetlenül fölé rendelt vezetőnek vagy az elektronikus információs rendszer felhasználói adminisztrátorának, a MATE Információbiztonsági felelősének haladéktalanul jelentik (jelzik),
d) Információbiztonságot és IT szolgáltatás biztonságot sértő esemény kivizsgálása esetén a tudomásukra jutott adatokat és információkat a vizsgáló bizottságnak a legjobb tudásuk szerint átadják,

e) Megismerik és betartják a jelen IBSZ és az elektronikus információs rendszer Felhasználói Kézikönyvében rögzített információbiztonsággal kapcsolatos szabályokat és a megismerés tényét aláírásukkal ismerik el az IBSZ megismerési és oktatási nyilatkozaton.

1.6 Külső szervezetek feladat- felelősség- és hatáskörei

A MATE információbiztonságán tevékenykedő külső szervezeteket és tevékenységüket éves szinten minősíteni, véleményezni szükséges, és a minősítésnek megfelelően, amennyiben szükséges, a szerződéseket felül kell vizsgálni és aktualizálni. *5. számú melléklet*

A SZÁLLÍTÓ / FEJLESZTŐ / KARBANTARTÓ / RENDSZERTÁMOGATÓ / STB. SZERVEZET(EK) MEGNEVEZÉSE(I) ÉS ELÉRHETŐSÉGE(I) *6. számú melléklet*

A SZÁLLÍTÓ / FEJLESZTŐ / KARBANTARTÓ / RENDSZERTÁMOGATÓ / STB. SZERVEZET(EK) **NEVÉBEN MUNKÁT VÉGZŐ(K)** és/vagy kapcsolattartásra jogosult(ak) neve(i) és elérhetősége(i): *7. számú melléklet*

XII. VÉDELMI INTÉZKEDÉSEK MEGHATÁROZÁSA

1.1 Az adatok és eszközök biztonsági besorolása és ellenőrzése

Számadási kötelezettségek az informatikai eszközökkel kapcsolatban

A MATE minden informatikai eszköze nyilván van tartva. A leltár elkészítéséről a MATE Leltározási Szabályzata rendelkezik.

Az adatok osztályozása

Az adatok osztályozásának célja, hogy a különböző osztályozási kategóriába sorolt adatokhoz, illetve a kezelésüket megvalósító eszközökhöz különböző szintű védelmi intézkedéseket, eljárásokat lehessen rendelni.

Az adatok osztályozásának irányelvei

A MATE-nál kezelt adatok osztályba vannak sorolva annak érdekében, hogy az egyes adattípusokhoz különböző védelmi intézkedéseket lehessen rendelni.

Az információk osztályozását bizalmasság, sértetlenség és rendelkezésre állás szempontjából osztályozni kell, amelyet az alábbi három szinten kell megvalósítani. Az osztályozási szinteket a táblázat foglalja össze (részletesebben lásd: *8. számú melléklet*).

Osztályozási szintek	Bizalmasság	Sértetlenség	Rendelkezésre állás
1. Nyilvános	Nyilvános	Nem védett	Általános
2. Bizalmas	Bizalmas (belső használatra)	Védett	Fontos
3. Titkos	Titkos	Fokozottan védett	Kritikus

Az egyes adatcsoportok (rendszerek, alkalmazások) osztályba sorolási kategóriáját az határozza meg, hogy az adatok bizalmasságának, sértetlenségének és rendelkezésre állásának sérüléséből a MATE-nak milyen hátránya, anyagi kára származhat.

Az egyes biztonsági osztályba sorolt adatokhoz, és az adatokhoz tartozó adatkezelő rendszerekhez, infrastrukturális elemekhez különböző szintű védelmi intézkedések vannak hozzárendelve.

Az adatok osztályozását az adatgazdák végezik.

Az adatok osztályozása után meg kell határozni az osztályba sorolási szintnek megfelelően az adatok elvárt rendelkezésre állását is. Ennek alapján az adatvédelmi tisztviselővel közösen, meg kell határozniuk azokat az információ-kezelő eszközöket is, amelyek szükségesek az adatok rendelkezésre állásához (szerverek, tárolók, aktív eszközök, adathordozó médiák stb.). Ha az eszközök különböző rendelkezésre álló adatokat kezelnek, akkor azok közül a legszigorúbb követelményt kell figyelembe venni.

A személyes adatok osztályozásának irányelvei

A személyes adatok osztályozásának az alapja a 2011. évi CXII. törvény és a 679/2016 EU Tanácsi rendelet.

A személyes adatok csoportjainak figyelembe vételével az EU GDPR rendeletével (679/2016 EU Tanácsi rendelet) összhangban kiemelt fontosságú védelmet élveznie, mind az EU tagállamokból érkezett személyek és a harmadik országból az EU területére érkezett személyeknek.

A személyes adatok osztályozása szerint:

Törvény	Adat típus	Adat tartalom	Megjegyzés
2011 évi CXII. tv 3§ 2. pont	Személyes adat	az érintettel kapcsolatba hozható adat – különösen az érintett neve, azonosító jele, valamint egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző ismeret –, valamint az adatból levonható, az érintettre vonatkozó következtetés;	Illetve személy igazolvány, TAJ szám, Adószám, Útlevél szám, Személyi szám, Jogosítvány száma; Illetve minden olyan azonosító mely alapján a sokaságból egy személy kijelölhető (pl. Magyarország űrhajósa)
2011 évi CXII. tv 3§ 3. pont	Különleges adat	a)[2] a faji eredetre, a nemzetiséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdek-képviseleti szervezeti tagságra, a szexuális életre vonatkozó személyes adat, b) az egészségi állapotra, a kóros szenvedélyre vonatkozó személyes adat, valamint a bűnügyi személyes adat;	
679/2016 EU Tanácsi rendelet 13.; 34; 35. pont	Genetikai adat	13.)„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 említett természetes személyből vett biológiai minta elemzéséből ered; 34.) A genetikai adatot olyan, a természetes személy örökölt vagy szerzett genetikai jellemzőivel összefüggő személyes adatként kell meghatározni, és amely az érintett személytől vett biológiai minta elemzésének – különösen kromoszómaelemzésnek, illetve a dezoxiribonukleinsav (DNS) vagy a ribonukleinsav (RNS) vizsgálatának, vagy az ezekből nyerhető információkkal megegyező információk kinyerését lehetővé tevő bármilyen más elem vizsgálatának – az eredménye. 35.) Az egészségügyi személyes adatok közé tartoznak az érintett egészségi állapotára vonatkozó olyan adatok, amelyek információt hordoznak az érintett múltbeli, jelenlegi vagy jövőbeli testi vagy pszichikai egészségi állapotáról. Ide tartoznak az alábbiak: a természetes személyre vonatkozó olyan személyes adatok, amelyeket az egyénnek a 2011/24/EU európai parlamenti és tanácsi irányelvben (1) említett egészségügyi szolgáltatások céljából történő	

		nyilvántartásba vétel, vagy ilyen szolgáltatások nyújtása során gyűjtöttek, a természetes személy egészségügyi célokból történő egyéni azonosítása érdekében hozzá rendelt szám, jel vagy adat, valamely testrész vagy a testet alkotó anyag – beleértve a genetikai adatokat és a biológiai mintákat is – teszteléséből vagy vizsgálatából származó információk, és bármilyen, például az érintett betegségével, fogyatékosságával, betegségkockázatával, kórtörténetével, klinikai kezelésével vagy fiziológiai vagy orvosbiológiai állapotával kapcsolatos információ, függetlenül annak forrásától, amely lehet például orvos vagy egyéb egészségügyi dolgozó, kórház, orvostechnikai eszköz vagy in vitro diagnosztikai teszt.	
2011 évi CXII. tv 3§ 4. pont	Bűnügyi személyes adat	A büntetőeljárás során vagy azt megelőzően a bűncselekménnyel vagy a büntetőeljárással összefüggésben, a büntetőeljárás lefolytatására, illetve a bűncselekmények felderítésére jogosult szerveknél, továbbá a büntetés-végrehajtás szervezeténél keletkezett, az érintettel kapcsolatba hozható, valamint a büntetett előéletre vonatkozó személyes adat;	
2011 évi CXII. tv 3§ 5. pont	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, kérésre az állampolgárok és média részére kiadható
2011 évi CXII. tv 3§ 6. pont	Közérdekből nyilvános adat	a közérdekű adat fogalma alá nem tartozó minden olyan adat, amelynek nyilvánosságra hozatalát, megismerhetőségét vagy hozzáférhetővé tételét törvény közérdekből elrendeli;	Megjelentetése a törvény szerint a nyilvános és kötelező

A személyes adatok kezelésénél betartandó szabályok a 679/2016 EU tanácsi rendelet szerint:

a) Adat tulajdonos hozzáférési joga
b) Adat tulajdonos személyes adat kezelési engedélye (amennyiben törvény vagy jogszabály másként nem rendelkezik)
c) Adat tulajdonos, adat visszavonási joga (amennyiben törvény vagy jogszabály másként nem rendelkezik)
d) Adat tulajdonos korlátozási joga (amennyiben törvény vagy jogszabály másként nem rendelkezik)
e) Adat tulajdonos adatkezelés megismerési joga
f) Adat tulajdonos, adat módosítási joga
g) Adat tulajdonos felhasználási és időbeli korlátozási joga (amennyiben törvény vagy jogszabály másként nem rendelkezik)

h) Adat tulajdonos, adat törlési joga (amennyiben törvény vagy jogszabály másként nem rendelkezik)

A fenti jogokban eset sérelem és szabálytalanság kivizsgálását szervezeti szinten az Adatvédelmi tisztviselő kezeli.

Személyes adatkezelési incidens bejelentése

Az adatvédelmi tisztviselő elérhetőségét a szervezet web lapján publikálni kell, illetve az adatvédelmi tisztviselő személyét a NAIH (Nemzeti Adatvédelmi és Információszabadság Hatóság) részére be kell jelenteni.

A NAIH elérhetősége

1125 Budapest Szilágyi Erzsébet fasor 22/c

tel: +36 1 391 1400

fax: +36 1 391 1410

e-mail: UGYFELSZOLGALAT@NAIH.HU

Minden személyes adatvédelmi incidens a DPO (Data Protect Officer), Adat Védelmi Tisztviselő felé be kell jelenteni.

Adatok nyilvántartása

A MATE adatait nyilván kell tartani. A nyilvántartásnak az alábbiakra kell kiterjedni:

a) Az adat, vagy adatcsoport megnevezése
b) Az adatosztályozási szint bizalmasság, sértetlenség és rendelkezésre állás szerint
c) Az adatgazda megnevezése
d) Az adatokat kezelő eszközök megnevezése

A nyilvántartás vezetéséért az adatgazdák felelősek.

Az adatok nyilvántartási követelményei az ***1. számú mellékletben*** találhatók.

Az adathordozók biztonságos kezelése

Az adathordozók biztonságos kezelésének kialakítása elősegítheti a MATE magasabb szintű adatbiztonsági kategóriákba besorolt adatainak védelmét, illetéktelen kézbe való kerülését, sérülését, elvesztését.

A MATE tulajdonában lévő, a magasabb szintű adatbiztonsági kategóriákba besorolt adatok tárolására használt adathordozókat, amennyiben az a kockázati értékelésen egy előzetesen meghatározott értéket elér, azokat egyedi azonosítóval kell ellátni, nyilvántartást kell vezetni róla. Az adathordozóra tett címkén, **az adattal dolgozó** MATE **alkalmazottnak** fel kell tüntetnie az adott tartalomra vonatkozó bizalmassági kategóriákat. Kezelését ennek megfelelően kell megvalósítani.

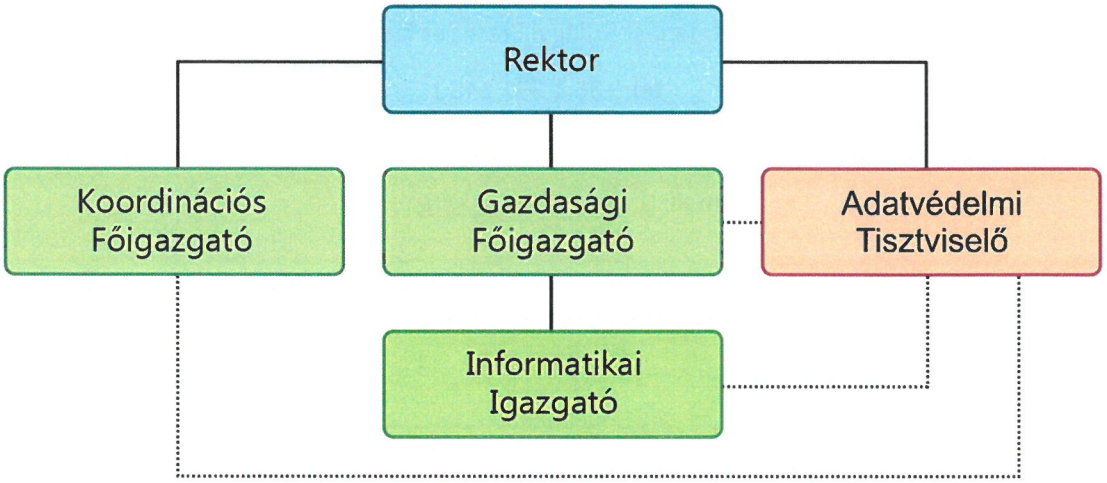
Adathordozók tárolására vonatkozó szabályok

a) Figyelembe kell venni a gyártó által meghatározott tárolási környezetre vonatkozó paramétereket.

b) Az adatbiztonsági kategóriákba besorolt adatokat tartalmazó adathordozók tárolásánál figyelembe kell venni a szabályzat adatok kezelésével kapcsolatos előírásaiban megfogalmazottakat.
c) Több példányban való tárolás esetében a tároló helyet úgy kell kiválasztani, hogy szükség esetén az arra jogosult akadálytalanul és viszonylag gyorsan hozzáférhessen, de célszerűen egymástól fizikailag távol. Ezzel megakadályozva a több példány egyidejű megsemmisülését katasztrófa esetén.

Az információ biztonsági szervezet működései rendje

Az információbiztonsági szervezet felépítése



Információbiztonsági szervezet felépítése

Információbiztonsági feladatkörök

INFORMATIKAI IGAZGATÓ SZMSZ-BEN RÉSZLETEZETT FELADATAIN TÚL:

a) Felelős a kockázatkezelési feladatok rendszeres végrehajtásáért, a feltárt kockázatok csökkentésére vonatkozó akciótervek végrehajtásának ellenőrzéséért MATE szintjén.
b) Gondoskodik a MATE biztonsági alapdokumentumainak (stratégia, politikák, szabályzatok, utasítások, vészhelyzeti tervek, stb.) kidolgozásáról. Felelős az alacsonyabb szintű, eljárás- vagy eszköz/technológia specifikus biztonsági dokumentumok elkészítéséért, vagy illetékes felelős kijelöléséért központi szinten.
c) Felügyeli a kockázatmenedzselési folyamatokat.
d) Együttműködik az adatvédelmi tisztviselővel az informatikai rendszerek védelmére megvalósítandó rendszer biztonsági követelmények kialakításában, az információbiztonság fokozása, a biztonsági incidensek elhárítása érdekében.
e) Ellenőrzi az informatikai rendszerfejlesztések, bővítések, beszerzések, ezekre vonatkozó szolgáltatási, rendelkezésre állási és más egyéb (pl. szállítási) szerződések egységes rendszer, hálózat és biztonsági szempontból való megfelelőségét MATE szinten.
f) Felügyeli a belső és külső informatika biztonsági ellenőrzések végrehajtását.
g) Együttműködik az adatgazdákkal és a létesítmény biztonsági vagy műszaki felelősével az információ biztonsághoz kapcsolódó feladatokban központi szinten.
h) Részt vesz a rendszer biztonsági oktatások tematikájának meghatározásában, szakmai felügyeletében központi szinten.

ADATVÉDELMI TISZTVISELŐ FELADATAI:

a) Felelős a kockázatkezelési feladatok rendszeres végrehajtásáért, a feltárt kockázatok csökkentésére vonatkozó akciótervek végrehajtásának ellenőrzéséért MATE szinten.
b) Javaslatot tesz az informatikai igazgatónak a felvállalható rendszer biztonsági kockázatokra, felhívja a figyelmét a nem felvállalható kockázatokra.
c) Felelős az adatosztályozási folyamat fenntartásáért.
d) Kezeli, és rendszeresen felülvizsgálja a MATE által életbe léptetett biztonsági alapdokumentumait (stratégia, politikák, szabályzatok, utasítások, vészhelyzeti tervek, stb.). Kijelöli az alacsonyabb szintű, eljárás- vagy eszköz/technológia specifikus biztonsági dokumentumokat.
e) Együttműködik a MATE informatikai igazgatóság munkatársaival az informatikai rendszerek védelmére megvalósítandó rendszer biztonsági követelmények kialakításában, az információbiztonság fokozása, a biztonsági incidensek elhárítása érdekében.
f) Ellenőrzi az informatikai rendszerfejlesztések, bővítések, beszerzések, ezekre vonatkozó szolgáltatási, rendelkezésre állási és más egyéb (pl. szállítási) szerződések egységes rendszer, hálózat és biztonsági szempontból való megfelelőségét MATE szinten.
g) Együttműködik az adatgazdákkal és a létesítmény biztonsági vagy műszaki felelősével az információ biztonsághoz kapcsolódó feladatokban MATE szinten.
h) Részt vesz a rendszer biztonsági oktatások tematikájának meghatározásában, szakmai felügyeletében MATE szinten.

Adatgazdák információbiztonsági feladatai

Az adatgazdák a MATE ügyviteli, oktatási és kutatási feladatait támogató folyamatok kijelölt tulajdonosai. Az adatgazdákat a szakmai szervezetek állományából kell kijelölni. Feladatai az alábbiak:

a) Részt vesz a Jogosultsági rendszer kidolgozásában, egységesítésében.
b) Elbírálja az általa felügyelt rendszerhez a jogosultság igénylés menetének megfelelően benyújtott hozzáférési igényeket.
c) Meghatározza az igényelt, kezelt, szolgáltatott strukturált és strukturálatlan adatok körének, formájának, biztonsági besorolását, aktualizálási gyakoriságát az ügyviteli és kutatási terület munkafolyamatainak megfelelően.
d) Részt vesz a MATE adatnyilvántartásainak kialakításában, naprakészen tartásában.
e) Rendkívüli események esetére meghatározza a maximális átállási időt (sebezhetőségi ablakot).

Informatikai igazgatóság munkatársai

Feladataik az alábbi négy fő terület szerint csoportosíthatók:

VÍRUSOK

a) Folyamatosan figyeli a megjelenő vírusokról és sérülékenységekről szóló jelentéseket, szükség esetén javaslatokat tesz az adatvédelmi tisztviselőnek, felettesének a védelmi szint emelésére.
b) Szükség esetén értesíti a vírusvédelmi felelőst, a vírusvédelmi rendszer felmerült üzemeltetési problémáinak, illetve vírusvédelmi vészhelyzet elhárítása miatt.
c) Napi rendszerességgel ellenőrzi a vírusvédelmi rendszer állapotát, a vírusvédelmi eszközök vírusadatbázisát.
d) Statisztikákat készít a vírusvédelmi incidensekről, és azokat háromhavonta jelenti az adatvédelmi tisztviselőnek.
e) Szükség esetén beavatkozik, illetve végrehajtja a vírusmentesítést.
f) Elvégzi a MATE-nál használt szoftverek, alkalmazások biztonsági frissítéseit.

g) Javaslatokat tesz a vírusvédelmi szabályzat módosítására.

HATÁRVÉDELEM CAMPUS/TELEPHELYI SZINTEN

a) Folyamatosan figyeli a megjelenő sérülékenységekről szóló jelentéseket, szükség esetén javaslatokat tesz a felettesének a védelmi szint emelésére.
b) Végzi a tűzfal- és egyéb határvédelmi eszköz napi, rutinszerű üzemeltetési, és ellenőrzési feladatait.
c) Elvégzi vagy külső szolgáltató esetén ellenőrzi a tűzfal, és egyéb határvédelmi eszköz biztonsági frissítéseit. Gondoskodik a frissítések végrehajtásához szükséges licencek felméréséről, valamint az igények továbbításáról az informatikai igazgatóság vezetője felé.
d) Adatvédelmi tisztviselő/ informatikai Igazgató jóváhagyása esetén végzi a tűzfalon és egyéb határvédelmi eszközön beállított szabályok szükséges módosításait, mentését, illetve gondoskodik azok rendszeres felülvizsgálatáról.
e) Javaslatokat tesz a szabályzat határvédelmi fejezeteinek módosítására.

ADATMENTÉS

a) Részt vesz a mentési, archiválási rend kialakításában.
b) Rendszeresen ellenőrzi a beállított automatikus mentések végrehajtását. Szükség esetén végrehajtja a mentéseket manuális módon.
c) Az archiválási rendnek megfelelően végrehajtja az adatok archiválását, illetve a mentési, archiválási média biztonságos tárolását.
d) Adatvesztés, vészhelyzeti terv aktiválása esetén végzi az adatok visszatöltését.
e) Követi a mentési média életciklusát, szükség esetén másolással hosszabbítja meg az adatok visszaállíthatóságát.
f) Gondoskodik a mentési média rotációjáról, újra hasznosításának szakszerű végrehajtásáról.

JOGOSULTSÁGKEZELÉS

a) Részt vesz a jogosultsági rendszer kialakításában.
b) Végrehajtja a szabályzatnak megfelelő jogosultság kezelési feladatokat (kiadás, módosítás, felfüggesztés, visszavonás).
c) Végrehajtja a jogosultságok nyilvántartásával kapcsolatos adminisztratív feladatokat.
d) Fogadja az intézet/campus/telephely/MATE informatikai rendszerével kapcsolatos incidens jellegű bejelentéseket.
e) Végrehajtja azoknak a biztonsági incidenseknek az elhárítását, amelyekhez kompetenciája van.
f) A kompetenciáján kívül eső incidensek elhárítására, értesíti az incidensek kezeléséért felelős személyeket.
g) Dokumentálja a biztonsági incidensek kezelésének teljes ciklusa alatt felmerült problémákat, tevékenységeket, megoldásokat.
h) Valamennyi biztonsági incidensről jelentést tesz az adatvédelmi tisztviselőnek, informatikai főigazgatónak.

A személyekhez kapcsolódó biztonsági előírások

Az információbiztonság szintjének fenntartása, mint kiemelt feladat, a MATE-ban a teljes személyi állomány felelőssége. Az információbiztonság minimálisan betartandó előírásait jogviszony keletkezésekor, a MATE informatikai rendszerének használata előtt meg kell ismernie és annak tudomásul vételét dokumentálni szükséges.

Fegyelmi eljárások, szankcionálások

Az információbiztonsági előírások súlyos megsértése esetén azonnali felfüggesztést kell alkalmazni az informatikai rendszerek használatával kapcsolatban és fegyelmi eljárást kell indítani a szabálysértő személyével szemben, ha:

a) a szabálysértés valamely rendszer hozzáférési adatainak illetéktelen személynek történő tudomására hozatalával (pl.: személyes jelszó elmondása, vagy hozzáférhető helyre történő feljegyzése) kapcsolatos.
b) a szabálysértés következtében a MATE „Bizalmas", vagy annál magasabb minősítésű adata, dokumentuma kerül illetéktelen kezekbe.
c) a szabálysértés következtében a MATE „Fontos" vagy annál magasabb minősítésű rendelkezésre állás szerint minősített adata, dokumentuma a rendelkezésre állási követelménynek nem tud eleget tenni.
d) a szabálysértő a MATE „Védett", vagy annál magasabb sértetlenség szerint minősített adatát, dokumentumát szándékosan meghamisította vagy megsemmisítette.
e) a szabálysértés következtében a MATE biztonsági rendszerének védelmi megoldásai illetéktelenek kezébe jutottak.
f) a szabálysértés következtében bekövetkezett vagyoni hátrány (vagyoni kár, többletköltség) eléri, vagy meghaladja a jogszabályban meghatározott alsó határt. A szabálysértővel kapcsolatban anyagi felelősséget is meg kell állapítani.
g) a szabálysértés következtében súlyosan sérül a személyes adatok védelméről, és nyilvánosságra hozataláról szóló jogszabályok,
h) bűncselekmény gyanúja áll fenn.
i) Az információbiztonsággal kapcsolatos fegyelmi eljárás lefolytatását az alábbi személyekből álló bizottság hajtja végre a munka törvénykönyvéről szóló 2012. évi törvény 56. §-a alapján:

    1. Informatikai Igazgató, vagy az általa delegált személy
    2. HR illetve munkaügyi vezető, vagy az általa delegált személy
    3. A szabálysértő személy közvetlen munkahelyi vezetője
    4. egyetemi adatvédelmi tisztviselő,
    5. MATE rektora.

Amennyiben a fegyelmi eljárás a felsorolt személyek valamelyikére irányul, új tagságot kell kijelölni, melyhez az érintett személy helyett a munkahelyi vezetője jelöl ki delegált személyt. Ha a felhasználó által okozott szabálysértés anyagi kárral is jár, anyagi felelősséget is meg kell állapítani, és az okozott kárt a törvényeknek megfelelően ki kell fizettetni a kár okozójával.

Információ biztonság tudatosítása

A személyi kockázatok csökkentése érdekében meg kell oldani a MATE informatikai rendszerének üzemeltetőinek, használó alkalmazottainak a biztonsággal kapcsolatos tudatosítását.

Az alkalmazottak információbiztonság oktatása a MATE-nál központilag kerül koordinálásra, az alábbiak szerint:

Az informatikai igazgató elkészíti a központi „Oktatási tematikát", melyet átad az adatvédelmi tisztviselőnek, minden év február 15-ig. Az oktatási tematika részletesen tartalmazza az oktatási témákat, amelyeket tárgyévben oktatni kell, illetve az **alkalmazottak részére** rendszeres biztonsági tájékoztatásokat.

Az informatikai igazgató, az adatvédelmi tisztviselő az oktatási tematika alapján elkészítik az „Információbiztonsági oktatási tervet" április 1-ig, amely tartalmazza:

a) Az oktatási napokat, naponként témákra lebontva
b) Az oktatás biztosítási feltételeit (oktatás helye, vagy eszköze)

Az információbiztonság oktatásában az e-learning rendszert kell előnyben részesíteni, igény esetén hagyományos oktatást kell biztosítani. Az oktatási anyagból vizsgát kell tenni. A hagyományos oktatáson való részvételt minden vizsgázónak aláírásával kell igazolnia.

A rendszeres biztonsági tájékoztatást elektronikus eszközök felhasználásával kell megoldani (pl. tájékoztató e-mailek, portál stb.).

Külső személyek általi hozzáférések

A MATE informatikai rendszerein csak regisztrált, egyéni hozzáférési engedéllyel rendelkező felhasználók dolgozhatnak.

Külső személy részére csak megadott feladat elvégzésének időtartamára adható hozzáférési jogosultság a MATE rendszereihez.

Megbízási illetve ***önkéntes szerződéssel alkalmazottak*** számára a rendszerhez való hozzáférési jogosultságot elektronikus vagy papír alapon, a MATE iktatási és dokumentum-kezelő rendszerében rögzítetten, a MATE oldali szerződő fél igényelhet. A jogosultság csak a jogviszony időtartamára igényelhető.

Vállalkozási támogatási szerződés esetén jogosultság csak konkrét személynek kérhető (a rendszerekhez hozzáférőket nevesíteni kötelező). Ezen személyek számára a rendszerhez való hozzáférési jogosultságot elektronikus vagy papír alapon, a MATE iktatási és dokumentum-kezelő rendszerében rögzítetten, a MATE oldali szerződő fél igényelhet. A jogosultság csak a jogviszony időtartamára igényelhető.

Külső személynek távoli elérés csak indokolt esetben, a külső személy (cég) megbízhatóságáról történő meggyőződés és titoktartási nyilatkozat tétele után biztosítható.

Az Eduroam felhasználókra a nemzetközi jogszerinti eduroam.hu oldalon megtalálható szabályzatok érvényesek.

Az engedély kiadásában

a) A MATE központi informatikai rendszerei esetén az informatikai igazgatónak vétójoga van. A vétójog a jogosultság szerződésben rögzített tartalmára, illetve a jogosultság kiadására terjed ki. A vétójogot csak a koordinációs főigazgató utasítására lehet feloldani, aki a kockázatokról a szükséges tájékoztatást megkapja. Ebben az esetben a jogosultsággal kapcsolatos kockázatokat a rektor felvállalja.
b) A MATE intézeti informatikai rendszerei esetén az adatvédelmi tisztviselőnek és az informatikai igazgatóság munkatársának van vétójoga. A vétójogot csak a intézet vezetőjének utasítására lehet feloldani, aki a kockázatokról a szükséges tájékoztatást megkapja. Ebben az esetben a jogosultsággal kapcsolatos kockázatokat az intézet vezetője vállalja fel.
c) Külső személyek hozzáférésének szabályozását a szerződésben kell explicit módon rögzíteni.

A felhasználók jogai

a) A felhasználóknak joga van a rendelkezésükre bocsátott informatikai eszközök szabályszerű, rendeltetésszerű használatára a saját munkájuk támogatása érdekében.
b) A felhasználóknak joga van a számítógépes tevékenységük során felmerült problémák, akadályok elhárításához támogatást kérni, és kapni. A segítségnyújtáshoz az igényt az informatikai Igazgatóság munkatársainál kell bejelenteni.
c) A felhasználónak joga van a rá vonatkozó törvények, és szabályzatok megismeréséhez.
d) A felhasználónak joga van a munkájához szükséges információbiztonsági eljárások, ismeretek megismeréséhez.
e) A felhasználóknak joga van megtagadni a számítógépes munkát, ha
    1. A számítógépes munka törvénysértéshez vagy bűncselekményhez vezet.
    2. A tevékenység veszélyezteti az informatikai rendszer rendelkezésre állását.

A felhasználóknak joga van a számítógépes munkával kapcsolatos sérelmeinek jogorvoslati kezelésére. Jogorvoslati kérdésekben az adatvédelmi tisztviselő, magasabb szinten az informatikai igazgató, végső esetben a rektor áll rendelkezésre.

Felhasználói felelősségek

A felhasználó felelősséggel tartozik:

a) A hivatkozott törvények betartásáért,
b) A MATE szabályzataiban megfogalmazott előírások betartásáért,
c) A jogviszony keletkezésekor felelősséget vállalt előírások betartásáért,
d) A törvényekben, szabályzatokban megfogalmazott előírások bárki által történő megszegésének a jelentéséért,
e) Az információbiztonságért felelős személyekkel való együttműködésért.

Az informatikai biztonság személyi vonatkozásai

Az informatikai biztonság a MATE teljes személyi állományának felelőssége. A személyi kockázatok csökkentése érdekében:

a) Biztosítani kell a felhasználók rendszeres információbiztonsági oktatását, tudatosítását, tájékoztatását.
b) A felhasználóknak rendelkezniük kell a munkaköri kötelességük ellátásához szükséges számítógépes ismeretekkel. A szükséges kompetenciákat a munkaköri leírás tartalmazza.
c) Amennyiben a felhasználó nem rendelkezik a munkakör betöltéséhez szükséges informatikai ismeretekkel, azt maximum három hónapon belül igazolható módon pótolnia kell.
d) Valamennyi alkalmazott részletes munkaköri leírásában szerepeltetni kell az adott munkakörre vonatkozó biztonsági követelmények meghatározását.
e) Tájékoztatni kell a felhasználókat az információbiztonsággal kapcsolatos feladataikról, és felelősségeikről.
f) Minden felhasználónál tudatosítani kell a biztonsági szabályok megsértésével járó szankciókat, és azokat következetesen be kell tartatni.

Fizikai és környezeti biztonság

A MATE-nál három kategóriát különböztetünk meg a fizikai és környezeti biztonság szempontjából:

a) Azok a helyiségek, ahol nincs informatikai eszköz elhelyezve, vagy azoknak folyamatos, állandó felügyelete (személy vagy kamera által) biztosított.
b) Azok a helyiségek, ahol a felhasználói informatikai eszközök vannak elhelyezve.

c) Szerverszobák (kiszolgálók és hálózati aktív eszközök).

Ugyan ezeket a kategóriákat alkalmazzuk a papíralapú információk biztonsági kezelésénél. Ebben az esetben az egyes zónák besorolásánál az alábbi meghatározások érvényesek:

a) Azok a helyiségek, ahol nincs papíralapú bizalmas információ elhelyezve, vagy azoknak folyamatos, állandó felügyelete (személy vagy kamera által) biztosított.
b) A bizalmas információkat tartalmazó zárható elemek helyiségei.
c) A titkos adatok (személyiségi jogokat, gazdasági vagy üzleti titkos adatokat, vagyonleltárt, szigorú számadásra kötelezett nyomtatványok és dokumentumok) és a bizalmas események ténydokumentumainak tároló helye (lemezszekrények, zárható iratszekrény a MATE Adatvédelmi szabályzata szerint).

A fenti kategóriákat a bennük folyamatosan tárolt, vagy rajta keresztül elérhető információk bizalmasságára, sértetlenségére és rendelkezésre állására vonatkozó osztályozási szintek alapján illetve az információkezelő eszközök kockázati besorolása alapján kell kialakítani.

A biztonsági zónákat és a hozzájuk tartozó főbb követelményeket a *9. számú melléklet* tartalmazza.

Helyhez kötött eszközök kivitele

Az eszközök átmeneti kivitele

A MATE irodahelységeiből kiszállítandó informatikai berendezésekre vonatkozó szabályok:

a) a MATE tulajdonában lévő, minden nem személyre kiadott informatikai eszköz irodahelységeiből történő kivitele csak HelpDesken történt bejelentés után az informatikai igazgatóság előzetes engedélyével, illetve az adott szervezeti egység leltárfelelős írásbeli tájékoztatása mellett lehetséges.

A MATE campus/telephelyeiről kiszállítandó informatikai berendezésekre vonatkozó szabályok:

b) a MATE tulajdonában lévő, minden személyi használatra kiadott informatikai eszköz épületből történő kivitele csak az adott szervezeti egység vezetőjének előzetes írásbeli engedélyével lehetséges,
c) a kivitt eszközért a kiszállítót anyagi és erkölcsi felelősség terheli,
d) a ki- és beszállításokat minden esetben dokumentálni kell szállítólevél alkalmazásával, amelyen az adott informatikai eszköz egyedi azonosítóját fel kell tüntetni (típus, gyári szám, leltári szám), illetve nagy mennyiség esetén csatolt mellékletben kell felsorolni az egyedi azonosító adatait,
e) a szállítólevelet a kiinduló és a fogadó helyen a szállítást engedélyező és a szállítmányt fogadó személynek kézjegyével ellen kell jegyeznie, ezáltal nyomon követhetővé válik az eszköz útja.

Az eszközök végleges kivitele

A MATE tulajdonából véglegesen (pl. selejtezés miatt) kikerülő informatikai eszközökre vonatkozó szabályok:

a) az informatikai eszközökön tárolt adatokat az informatikai igazgatóság munkatársának visszaállíthatatlanul törölnie kell vagy selejtezéskor használhatatlanná kell tenni az adattárolót,
b) a kiszállítást dokumentálni kell szállítólevél alkalmazásával, illetve selejtezéskor – mivel az elektronikus eszközök és berendezések veszélyes hulladéknak minősülnek – a

környezetvédelmi törvénynek és előírásoknak megfelelően dokumentáltan, az erre jogosítvánnyal rendelkező céggel kell elszállíttatni.

c) a szállítólevél kiállításának feltétele a kiállított számla, vagy a selejtezési Megbízókönyv.

Külső szervezet által biztosított eszközök

a) Idegen eszközt csak szerződéses formában, az informatikai igazgató jóváhagyásával lehet elhelyezni.

b) A szerződésben rögzíteni kell az információbiztonsági szempontokat az elhelyezésre, működtetésre és felügyeletre, illetve az elszállításra vonatkozóan.

XIII. INFORMÁCIÓTECHNOLÓGIAI FOLYAMATOK BIZTONSÁGA

1.1 Informatikai rendszerek tervezése és jóváhagyása

Az informatikai rendszerek, vagy egyes rendszerelemeinek tervezéskor a funkcionalitáson, a gazdaságosságon túl a biztonsági szempontokat is figyelembe kell venni.

Az intézeti adatvédelmi tisztviselőnek az informatikai igazgatóság kijelölt munkatársával együttműködve a teljes tervezési ciklust felügyelni kell annak érdekében, hogy tervezéskor a biztonsági megoldások is hangsúlyt kapjanak.

A tervezés során az alábbi biztonsági szempontokat kell figyelembe venni:

a) A rendszer együttműködése a meglévő rendszerelemekkel.
b) Beépített biztonsági megoldások.
c) Az informatikai rendszer hozzáférési megoldásai (jogosultság kezelés, titkosítás, stb.).
d) Az informatikai rendszer rendelkezésre állást támogató megoldásai (karbantarthatóság, javíthatóság, van-e szupport, mentések végrehajthatósága, stb.).
e) Az informatikai rendszer menedzselhetősége (központilag menedzselhető, vagy helyileg).
f) Az informatikai rendszer ellenőrizhetősége (naplózhatók-e a kritikus folyamatok, távoli elérés biztosított-e stb.).
g) A MATE szoftveres, hardveres illetve egyéb standardjainak való megfelelés.

Informatikai eszközök beszerzésének biztonsága

Az informatikai eszközök (hardver, szoftver) beszerzésének biztonsága érdekében a MATE-ra érvényes és központilag kidolgozott szabályokat, eljárásokat kell foganatosítani annak érdekében, hogy biztosítható legyen az eszközök funkcionalitása, homogenitása, a központi és intézeti rendszerek együttműködése, illetve a rendszer előírt biztonsága.

Az üzemeltetés biztonsága

A megbízható és biztonságos üzemeltetés érdekében intézkedési terveket kell kidolgozni az informatikai rendszerhez kapcsolódó folyamatok – javítások, karbantartások, szoftvertelepítések és beállítások stb. – végrehajtására.

A szabályokat, eljárásokat össze kell hangolni az érvényben lévő információbiztonsági szabályokkal, eljárásokkal. Az üzemeltetési eljárásokat dokumentálni szükséges annak érdekében, hogy az elvégzett feladatok nyomon követhetőek legyenek.

Az informatikai rendszerterveket, és a biztonsági megoldásokat tartalmazó egyéb dokumentumokat „Titkos" információként kell kezelni.

Az üzemeltetési dokumentációk elkészítéséről az üzemeltetésért felelős informatikai igazgatóság munkatársa gondoskodik. Az adatvédelmi tisztviselő feladata a dokumentációk évenkénti felülvizsgálata.

A fejlesztés, bővítés biztonsága

A biztonságos fejlesztés és rendszerbővítés érdekében ki kell dolgozni a fejlesztési, bővítési folyamatot, a hozzátartozó feladatokkal, és felelősségekkel annak érdekében, hogy az információbiztonsági, homogenitási és központi menedzselhetőségre vonatkozó elvárások maximálisan érvényesíthetők legyenek a fejlesztés és bővítés folyamatában, és a fejlesztett, bővített rendszerekben.

A fejlesztés és bővítés folyamatait dokumentálni kell. Az információbiztonsági előírásokat érvényesíteni kell a fejlesztéssel, bővítéssel kapcsolatos szerződésekben, megállapodásokban. A fejlesztési, bővítési dokumentációk elkészítéséért a fejlesztésért felelős az informatikai igazgató által kijelölt személy gondoskodik. A fejlesztési és bővítési dokumentációkat „Bizalmas" minősítésű információnak kell tekinteni.

A fejlesztési, bővítési és egyéb rendszerdokumentációk biztonságos tárolásával kapcsolatos ellenőrzés az adatvédelmi tisztviselő feladata

Informatikai igazgatóság munkatársa tevékenységének naplózása

A MATE üzemeltetésű rendszereken informatikusi tevékenységként értelmezzük a MATE alapfeladatát támogató informatikai rendszer üzemeltetetési, javítási, karbantartási munkáit.

Ezen tevékenységek megkezdését a felelős informatikai vezető tudtával, beleegyezésével és szükség esetén koordinálásával/felügyeletével kell az informatikai igazgatóság arra kijelölt/megbízott munkatársának kell elvégeznie. Az elvégzett munkát vagy tevékenységet, amennyiben az elektronikusan a hardver eszközökön nem automatikusan rögzített, naplózni kell írásos, vagy elektronikus formában (pl. szerver napló). Célszerű lenne központosított elektronikus naplózás bevezetése.

Biztonsági incidensek kezelése

A biztonsági incidensek kezelése a **X.** fejezetben leírtak szerint hajtandó végre.

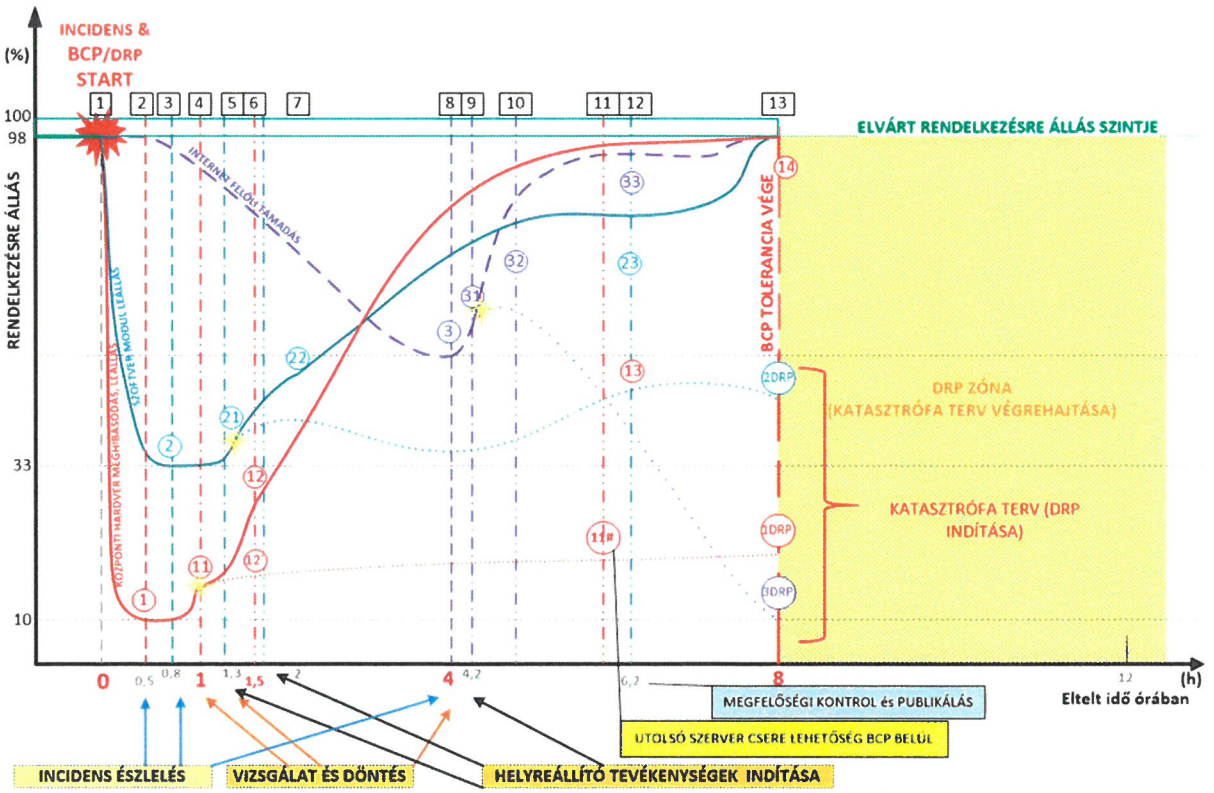
XIV. Az Üzletmenet Folytonossági Szabályzat (BCP), DRP és az IBSZ kapcsolata

A katasztrófa jellegű események két folyamatot indítsanak el. Egyrészről a katasztrófa elhárítási terv (DRP) alapján a kiesett erőforrások visszaállítását, másrészről a kiesett erőforrások nélküli lehető maximális funkcionalitást biztosító folytatódó működést.

Az üzletmenet folytonossági terv (BCP) célja az üzleti folyamatokat támogató informatikai erőforrások meghatározott időben és funkcionális szinten történő rendelkezésre állásának biztosítása, valamint váratlan események (incidensek) által okozott károk minimalizálása. Gyakorlatilag azon feladatok összessége, amelyek számba veszi az egyes folyamatok fenyegetettségeit és ezek valószínűségét, valamint a folyamat kieséséből származó esetleges károkat. A kockázatelemzés eredményeképpen (üzleti hatás elemzés – Business Impact Analysis) adja meg a szervezet működésének fenntartáshoz szükséges eljárásokat.

A katasztrófa elhárítási terv helyettesítő megoldásokat és eljárásokat határoz meg a súlyos károkat és az informatikai szolgáltatás tartós meghiúsulását okozó események bekövetkezésére, úgy, hogy a következmények negatív hatásai minimalizálhatók, és az eredeti állapot visszaállítása elfogadható költségek mellett meggyorsítható legyen. Olyan intézkedési terveket és feladatokat tartalmaz, amelyeket abban az esetben kell végrehajtani, ha szervezet működése szempontjából kritikus folyamatok, illetve az azokat támogató (IT) erőforrások súlyosan sérültek (a kritikus folyamatok nem tarthatók fenn.)

A két folyamat egymáshoz való viszonyát az alábbi ábra szemlélteti.



A BCP minden esetben elindul, ha valamely, üzleti folyamatot támogató erőforrás kiesik. A DRP viszont csak akkor indul el, ha az erőforrás várható visszaállítási ideje meghaladja a maximálisan tolerálható

kiesési időt. Ha ezen belül vissza lehet állítani az erőforrást, akkor nincs szükség a DRP aktiválására, hiszen az üzleti terület tolerálja a kiesést, nem következik be katasztrófahelyzet.

Jelen dokumentum a katasztrófa elhárítási terv és üzletmenet folytonossági terv tárgykörébe tartozó kérdéseket nem tárgyalja. Az ezzel kapcsolatos feladatokat és eljárásokat külön dokumentum kell, hogy tartalmazza.

1.1 Üzletmenet Folytonosság (BCP) alapértékei

A MATE rendszerében szereplő redundancia lehetővé teszi, a meghibásodás esetén történő másik szerverre való átállást. Mivel a rendszer jelenlegi alap BCP paraméterei a következők:

Rendszer Neve	Működési követelmény (7x24 óra 5x10óra stb)	Elvárt rendelkezésre állás %	Megengedhető maximális kiesési idő (perc)	Áthelyezés esetén a kijelölt szerver azonosítója/neve

Ezért a maximálisan megengedett kiesési időtartományba belefér a meghibásodott rendszer újraindítása, vagy az alkalmazás áthelyezése másik szerverre.

1.2 A rendszerbiztonsági terv és tartalma

A MATE egyedi eszköz meghatározása és az eszközök rendszerszintű biztonsága (egység és megismételt összeállíthatóság) kérdésében a rendszer elemeinek száma miatt: *10. számú melléklet*.

Amennyiben a rendszerben eszköz meghibásodás miatt kliens gép kiesik a munkából és a várható kiesési idő nagyobb, mint az SLA-ban megengedett idő, akkor a gép hiányát a központi raktárból kell időlegesen pótolni, a meglévő és a gépen szükséges alkalmazások feltelepítésével.

A MATE a jelen dokumentum mellett el kell, hogy készítse a Szervezeti szintű Informatikai Rendszerbiztonsági tervét melynek alapja az Informatikai Rendszerek Adatlapja. A rendszerbiztonsági terv tartalmazza a kliens és szerver oldali pótlási és csere lehetőségek rendszerét, mely biztosítani tudja az üzletmenetben leírt elvárások teljesülését.

1.3 Konfiguráció kezelés

A MATE számítógépeinek mennyisége, egységessége és az alkalmazások által nem támasztott speciális igények okán egyedi és típus konfiguráció kezelés előírása nem szükséges.

A MATE alkalmazásai futtathatók bármely az adott informatikai rendszert futtatni tudó gépen.

Speciális célrendszerek esetében a gyártó által előírt konfigurációt kell alkalmazni.

A szerverek esetében a rendszerbiztonsági tervben meghatározott alap konfiguráció a betartandó elvárás.

XV. DÖNTÉSI SZINTEK

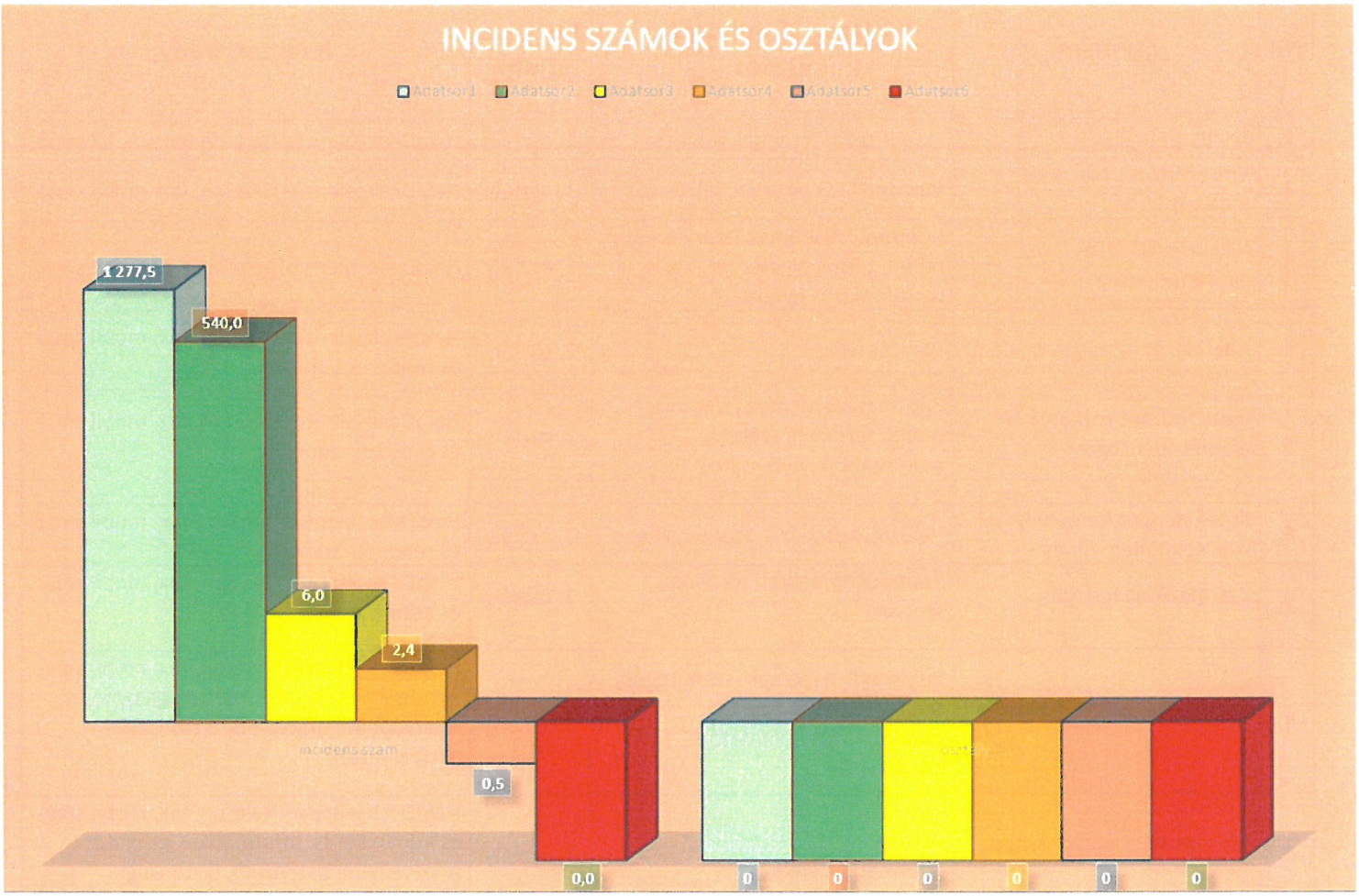
Az incidensek kezelésekor és rendezésekor az incidenseket kezelő (megoldó) csoportokat, szervezetet a következő támogatási szintekbe soroljuk:

SZINTBE-SOROLÁS	SZÍNKÓD	INCIDENS NAGYSÁGA	TÍPUS	CSOPORTOK	SZEMÉLYEK
1.		JELENTÉKTELEN	Alap, Támogatás	HELPDESK	
2.		ENYHE	Támogatás, Nyomelemzés	informatikai igazgatóság munkatársa	rendszer alkalmazások és támogató alkalmazások adminjai
3.		KÖZEPES	Nyomelemzés/ Kivizsgálás	BIZTONSÁGI VEZETŐK	biztonsági osztály munkatársa Adatvédelmi tisztviselő,
4.		KOCKÁZATOS	Kivizsgálás/ Reagálás	IBFSZ / Külső TÁMOGATÓ CSOPORTOK	reagáló erők és az Incidenskezelő team által meghatározott személyek
5.		KRITIKUS	Reagálás/ Kárenyhítés	MENEDZSMENT	gazdasági főigazgató, Médiaközpont vezető, Humánerőforrás igazgató, Informatikai igazgató
6.		SÚLYOS, KRITIKUS	Kárenyhítés/ Image kezelés	REKTOR	

A támogatási szintek megegyeznek az incidens során riasztandó személyek szintjével.

A szervezet számára fontos, hogy az incidens besorolások szerinti összesítő táblázat a 6. szint felé dinamikus csökkenést mutasson (lásd következő ábra).

A megfelelő incidens kezelés a minta szerinti kockázatossági és mennyiségi képet kell, hogy közöljön. Amennyiben a táblázat felvétele eltér, a következő mintától úgy az Incidenskezelési szabályzatot azonnal felül kell vizsgálni, valamint a szervezet biztonsági és kockázatossági mutatóit elkészítve gyors kiértékelés és intézkedési csomag szükséges. (a táblázat adatai éves adatvetítést mutatnak logaritmikus skálán).



XVI. INCIDENS TÍPUSOK

Az incidenseket azok iránya és tartalma szerint csoportokba soroljuk. A felsorolás alapján kell a tipizált incidenst bejelenteni és amennyiben lehetséges az elhárítást, kárenyhítést megkezdeni.

1.1 Informatikai Incidens

Informatikai incidensek körébe tartozik, ha a MATE rendszerében a következő eszközök-, elemek és berendezések ellen történik támadás-, vagy rendkívüli esemény.

Az Informatikai Incidensek csoportjai és jelentési irányok:

No	Esemény	Érintett Berendezés, Eszköz	Incidens szintje	Jelentési irány
1.	Rendszer leállás	számítógép, terminál, tablet	1. osztály	HelpDesk jelentés (telefon, fax, mobil sms)
2.	Vírus fertőzés (vírus és malware)	Vírusfertőzés vírusirtó jelzéssel	1. osztály	HelpDesk jelentés (telefon, fax, mobil sms)
3.	Alkalmazás leállás, elérhetetlenség	Informatikai elemek (számítógép, tablet, terminál, szerver, multifunkciós nyomtató)	1. osztály	HelpDesk jelentés (telefon, fax, mobil sms)
4.	Adatelérés részleges leállása	Hálózat leállás	2. osztály	HelpDesk jelentés (telefon, fax, mobil sms) és rendszer adminok
5.	Input, output eszközök elérhetetlensége	Informatikai elemek (számítógép, tablet, terminál, szerver, multifunkciós nyomtató)	2. osztály	HelpDesk jelentés (telefon, fax, mobil sms) és rendszer adminok
6.	Külső campus/telephely kapcsolat megszűnés	Hálózat, adatbázis, szerver, kliens	2. osztály	HelpDesk jelentés (telefon, fax, mobil sms) és rendszer adminok
7.	Zsaroló vírus fertőzés	Számítógép, tablet, terminál, szerver	3. osztály	HelpDesk jelentés (telefon, fax, mobil sms) és admin kérés
8.	Jogtalan hozzáférési kísérlet	Informatikai elemek (számítógép, tablet, terminál, szerver, multifunkciós nyomtató, adatbázis)	3. osztály	HelpDesk jelentés (telefon, fax, mobil sms) és admin kérés, Informatikai Igazgató, Adatvédelmi tisztviselő, Biztonsági osztályvezető
9.	Adatvesztés, adatszivárgás	Belső adatbázis és belső informatikai elemek	3. osztály	HelpDesk jelentés (telefon, fax, mobil sms) és admin kérés, Informatikai igazgató, Adatvédelmi tisztviselő, Biztonsági osztályvezető
10.	Nyomatatott dokumentum elvesztése	Számítógép, tablet, terminál, szerver, nyomtató	3. osztály	admin és biztonsági osztályvezető jelentés; Adatvédelmi tisztviselő (a nyomtatott dokumentum tartalma alapján eldöntendő)
11.	Illegális rendszer hozzáférés	Számítógép, tablet, terminál, szerver	4. osztály	Admin, biztonsági osztályvezető jelentés, adatvédelmi tisztviselő, informatikai igazgató
12.	Illegális eszköz megjelenése a hálózaton	Hálózat, szerver, adatbázis	4. osztály	Admin, biztonsági osztályvezető jelentés, adatvédelmi tisztviselő, informatikai igazgató
13.	Belső támadás, vagy belső rendszer összeomlás	Teljes belső hálózat leállás, Szerver és adatbázis elérés	5. osztály	Admin, biztonsági osztályvezető jelentés, adatvédelmi tisztviselő, informatikai igazgató
14.	Hálózati hozzáférés leállás, fogadási rendszer és kapcsolat megszakadás	Szerverek, hálózat, adatbázisok, Külső határvédelmi eszközök, Belső alkalmazások	5. osztály	Admin, biztonsági osztályvezető jelentés, adatvédelmi tisztviselő, informatikai igazgató, admin, Incidens kezelő team
15.	Internetes TÁMADÁS, szolgáltatás leállással, szervezeti IT infrastruktúra leállása	Teljes infrastruktúra, "B" site indítási probléma, Internetes hálózat leállás	6. osztály	Rektor irányításával, Incidens kezelő team

1.2 Adatkezelési Incidens

Adatkezelési incidensek és jelentés irányok:

No	Esemény	Érintett Berendezés, Eszköz	Incidens szintje	FELADAT
1.	Adatvesztés	Számítógép, tablet, terminál, szerver	4. osztály	admin és biztonsági osztályvezető jelentés
2.	Rendszeradatok és alkalmazás adatok kompromitállódása	Számítógép, tablet, terminál, szerver, nyomtató, levelezés, adathordozó	4. osztály	admin és biztonságiosztály vezető jelentés, Adatvédelmi tisztviselő kontroll
3.	Személyes adat vesztés	Számítógép, tablet, terminál, szerver	5. osztály	Admin, biztonsági osztályvezető jelentés, adatvédelmi tisztviselő, informatikai igazgató
4.	Személyes adat kompromittálódás	Számítógép, tablet, terminál, szerver	5. osztály	Biztonsági vezető, Informatikai vezető, Adatvédelmi tisztviselő
5.	Tömeges személyes adat kompromittálódása	Számítógép, tablet, terminál, szerver, nyomtató, levelezés, adthordozó	6. osztály	Első ellenőrzés: Admin, biztonsági osztályvezető jelentés, adatvédelmi tisztviselő, informatikai igazgató Döntés: Rektor

ÁLTALÁNOS INFORMÁCIÓ

a) Minden beérkező incidenst a HelpDeskes munkatársnak rögzítenie kell a HelpDesk rendszerben.
b) Az elektronikus információs rendszerek monitorozó rendszerei által, a kritikus rendszerek esetében kiadott kritikus szintű riasztásakor az ügyeletes rendszergazdának értesítenie kell a HelpDesk rendszert kezelő alkalmazottat.

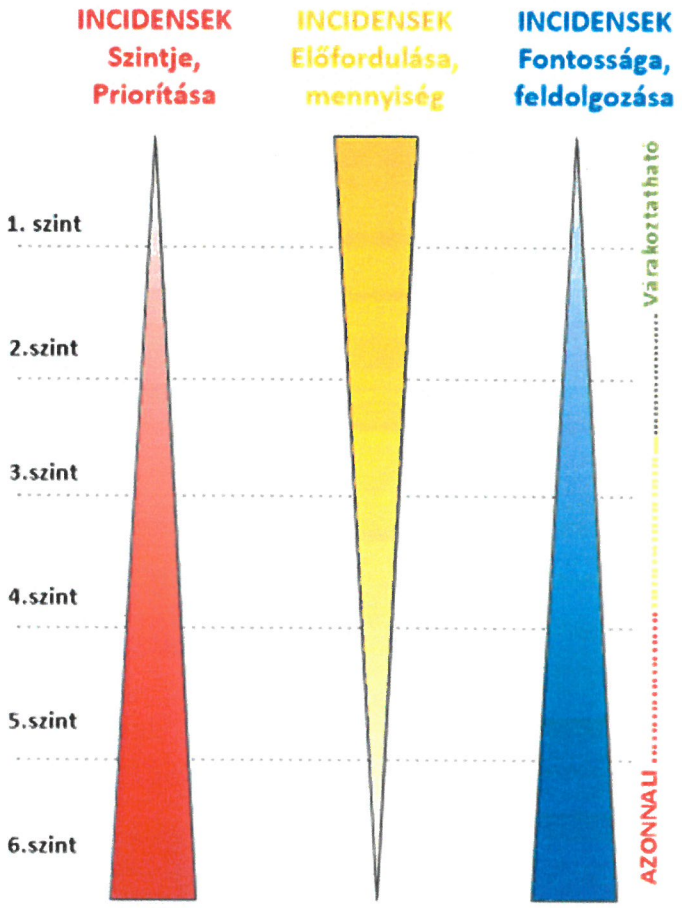
XVII. INCIDENSEK TÍPUS SZERINTI BESOROLÁSA

Szint	Típus, szint	Hatás	Érintettség	Eljárásrend	Válasz idő	Felelős
1.	Jelentéktelen	Jelentéktelen	kliens gép, internetes hozzáférés, vírusvédelmi riasztás, vagyoni kitettség alacsony, A Riasztás jelzés értékű	bejelentést követő távsegítség és helyreállítás, nyugtázás, iktatás	Gyors Helpdesk válasszal megoldható	Döntési szintekben
2.	Enyhe	alacsony, adat- és információ vesztés nem történt, rendszer és személy sérülés, vagyoni kár alacsony,	kliens gép, internetes hozzáférés, szerver, vagyontárgyak, bútorok, vírusvédelmi riasztás, vagyoni kitettség alacsony, A Riasztás jelzés értékű, Visszaellenőrzés és megerősítés már szükséges	bejelentést követő távsegítség és helyreállítás, nyugtázás, iktatás, Visszajelzés kérés, megfelelőségi kontrol futtatása. Őrszolgálati visszaellenőrzés	Gyors Helpdesk válasszal megoldható, Oktatási listára felvétel, helyszíni őrszolgálati ellenőrzés időszerű	Döntési szintekben
3.	Közepes	Adatvesztés, információvesztés kismértékű, nem kritikus élethelyzet, humán szolgáltatási igények megjelenhetnek (orvos, mentő hívás)	kliens gépek, számítógépek, terminálok, szerverek kisebb csoportja, A kár és kockázat anyagi vonzata felülvizsgálandó	A hálózati eszközökkel az érintet eszközök izolációja, mellet az őrszolgálati kivonulás kezdeményezése, a központi riasztás és felvétel indítása, az eszkalálódás elkerülése és rögzítése miatt	Az incidens felfedezését követően rövid határidővel történő megjelenés. Kockázat felmérés, helyszín biztosítás. Szükség esetén erősítés igénylése. Videós betekintés megfelelő	Döntési szintekben
4.	Kockázatos	Adatvesztés, információ szivárgás még nem történt meg, de az események folyamata ennek lehetőségét magában rejti Személy és vagyonbiztonság veszélyben. Gyors beavatkozás fontos	A Központi hálózat egyes elemei és illetve részei, Személyek, vagyontárgyak, személyes adatok, jelentős károkozássá fajulható környezet és esemény	Azonnali intézkedések végrehajtása központi irányítással, az ellentevékenység az elemzés után azonnali elkezdése, Az illetékesek bevonása, időleges hírzárlat elrendelése	Mielőtt még a szivárgás mértéke kritikussá válik. Gyors, határozott fellépés helyszínen és a központban. Vagyon és informatikai szakértők összedolgozása. Kompromisszum kötések átgondolása, hírzárlat és kommunikációs kontrol.	Döntési szintekben
5.	Súlyos (kritikus)	Komoly, adat és információ sérülések, személy és élet-veszélyes helyzet. Kockázatos nagymértékű vagyoni károkozás lehetősége	Az egész szervezetet (Központ hálózat, infrastruktúra), Területei kihatás lehetősége az egész szervezetre	Azonnali izolálás, a kompromittálódott rendszer rész lekapcsolása. Személyi beavatkozások azonnali elrendelése a helyszínen és a központban	Azonnali, késlekedés nem lehetséges. Előzetes forgatókönyv alapján megszervezett valós és virtuális ellenintézkedés. Hírzárlat a helyzet konszolidálódásáig	Döntési szintekben
6.	Súlyos (kritikus)	Komoly, adat és információ sérülések, szivárgások történnek. Személyek életveszélyben, vagyoni kár szervezeti mértékű	Az egész szervezetet (hálózat, infrastruktúra), Katasztrófa terveket átnézni, előkészíteni.	Azonnali izolálás, a klritikus részek zárása, Beavatkozó csaptok indítása, adatmentések és veszteségek ellenőrzése, személyi és vagyoni értékek mentése	Azonnali, késlekedés nem lehetséges, Hírzárlat. MATE felelősség és kontroll.	Döntési szintekben

1.1 Incidens Prioritások

a) Az incidensek prioritását az incidensek szintjei határozzák meg.
b) Minél magasabb az incidens szintje annál nagyobb a prioritása.

A sorban álló incidensek feldolgozásánál a magasabb prioritású, azaz a súlyosabb incidens a legelőször kezelendő, illetve leállítja vagy háttérbe állítja az alacsonyabb prioritású események kezelését.



a) Az incidenseket a saját csoportjaik (IV.1-5.) szerint kezeljük és adjuk meg a prioritási értékét.
b) Eltérő csoportba tartozó (IV. 1-5) kisebb prioritású események megoldása eltérő személyekhez kapcsolódik.
c) A magas prioritású események előfordulási gyakorisága okán azonos végrehajtói és kontrol személyekhez kötődik.
d) Az események feldolgozásában az egyedüli közös pont a média kommunikáció, melyet rektor által kijelölt egyedüli személy végezhet.
e) Az egységes kommunikáció és médiakezelés okán tilos a bekövetkezett események bemutatása, értékelése, megosztása külsős szervezetekkel a legfelső vezető jóváhagyása nélkül.
f) Az incidensek és kritikus események médiakommunikációja egy előre lekészített folyamat mentén kell, hogy zajlódjon. (Ettől eltérő információk zavarhatják a kárenyhítést és a kárelhárítást).

XVIII. AZ INCIDENSEK ÉRTÉKBEN KIFEJEZHETŐ ALAPELVEI

Az incidensek kezelése és kommunikációja céljából a következő alapelveket kell lefektetni.

Minden incidens a MATE számára költséggel jár:

a) Az incidensek költségei számíthatók az elhárításra fordított személyi juttatások költségeiből.
b) A veszteség költségeiből (az incidens lezárását követően határozható meg pontosan, addig becsült vagy tapasztalati összeg).
c) Az incidens értékét jelentő vagyoni, materiális és immateriális javak összességéből.
d) A helyreállításra fordítandó új eszköz, információ, adatbázis bekerülési költségeiből.
e) Az incidens okozta esetleges pénzügyi büntetések és gazdasági szankciók költségeiből.
f) A szervezet jó híréből és vásárlói visszaesés okozta bevétel kiesésekből.

A szervezet előzetes kommunikációjához és média bejelentéséhet a következő táblázatot kell kezelni.

CÉGES INCIDENSES VESZTESÉG KÖLTSÉGTÁBLA						
HATÁS TÍPUS	INCIDENSEK TÍPUSAI					
	1	2	3	4	5	6
Pénzügyi hatás	Kicsi	Kezelhető	Kezelhető	Jelentős	MATE működését fenyegető	MATE működését, hírnevét fenyegető
Jogi Következmény	Kicsi	Kezelhető	Jelentős	Jelentős	MATE működését fenyegető	MATE működését, és bizalmi jellegét fenyegető
Presztízsveszteség	Kicsi	Kezelhető	Jelentős	MATE működését fenyegető	MATE működését fenyegető	MATE működését, bizalmi szerepét fenyegető
SZÁMSZERŰSÍTETT (Ft)						

XIX. AZ ÉRINTETT FELELŐSÖK KÖRE

1.1 HelpDesk

a) Az incidens bejelentés alapvető egysége, amely az esetek nagy többségében autonóm módon alaptámogatást nyújt az incidensek megoldásában és a biztonsági helyzet helyreállításában.
b) Az 1. és 2. szintű incidensek kezelése a HelpDesk feladata. Az indulásként 1-2 szintű incidensek eszkalálódása esetén a HelpDesk feladata a magasabb szintre lépett incidensek tovább jelentése, átjelentése a megfelelő szintre.
c) A HelpDesk kötelessége a számára bejelentett incidensek nyomon követhetőségének biztosítása, tehát naplózása.
d) A HelpDesk naplózásának tartalmaznia kell:
    1. A bejelentés helyét.
    2. A bejelentés idejét.
    3. A bejelentő személyét.
    4. A fogadó HelpDesk ügyintéző nevét vagy azonosítóját.
    5. Az incidensben érintett személyt vagy technikai eszközt, területet.
    6. Az incidens kiterjedését.
    7. Az incidens induló besorolási szintjét.
    8. Az incidens elhárításának módját (vagy a besorolási szint változtatását).
    9. A szintemelés esetén a továbbadás módját és a fogadó személy megnevezését.
    10. Az incidens lezárásának idejét, és a lezáró személy azonosítóját vagy nevét.

A HelpDesk működtetését informatikai igazgatóság munkatársai biztosítják. Feladataik közé tartozik a HelpDesk tevékenység ellátása.

A HelpDesk elérhetőségeit a *14. számú melléklet* tartalmazza.

1.2 HelpDesk Vezetője

a) A HelpDesk vezetője felel az alá tartozó személyek tevékenységéért, és annak kontroljáért.
b) A HelpDesk vezetője kontrollálja az 5. biztonsági szinten létrehozott csapat munkáját, szükség esetén meghallgatja, vagy beavatkozik munkájukba.
c) A HelpDesk vezetője felel és irányítja a 6. szintbe tartozó incidensek elhárítását, a HelpDesk tevékenységének folytatására, korlátozására, vagy az incidensre adandó válasz kidolgozása létrehozott csoport tevékenységéért és az ekkor szükséges döntések meghozataláért.
d) A HelpDesk vezetője felel a szabályok és szabályzatok betartatásáért és az azok kontrolját ellátó személyek ellenőrzéséért.

1.3 Biztonsági Osztály Vezető

a) A szervezet Biztonsági osztályának Vezetője felel közvetlenül a szervezet biztonsági szabályzatainak betartatásáért
b) A biztonsági vezető az informatikai igazgató az őrszolgálati vezető és a gazdasági vezetővel együtt részt vesz a 4.-s 5.- szintű incidensek megoldásában a szervezet működésének helyreállításában.
c) A biztonsági osztály vezetője kontrolálja a 3. szintű incidensek végrehajtását és szakszerűségét. Szükség esetén, direkt módon beavatkozik az incidens elhárításba, az érintett terület vezetőjével együttműködve.

d) A Biztonsági vezető az Informatikai Igazgatóval együtt ellenőrzi a HELP DESK személyzetét, és működését.
e) A Biztonsági vezető kontrollálja a szervezet incidens kezelésének kialakítását és annak működését. Felel a szabályok betartásának és naprakészen létének állapotáért.
f) Kezdeményezéssel élhet a szervezet vezetője felé a szabályok, szabályzatok módosításáért és aktualizálásáért.
g) Az őrszolgálati vezetővel együtt kontrollálja a szervezet személyi és vagyonvédelmi rendszerének működését és részt veszt a problémák megoldásánál.
h) A Biztonsági vezető az osztályának személyzetével ellátja a szervezet biztonsági szabályzatában, incidens kezelési szabályzatában leírt korlátozások és biztonsági utasítások betartásának ellenőrzését.
i) A biztonsági vezető feladata a szabályzatok megsértése esetén a szankcionálási és korlátozó-, büntető javaslatok kidolgozása és beterjesztése a szervezet vezetője felé.
j) felel a szervezet fizikai biztonságának biztosításáért
k) a szervezet objektumait biztosító személyzetet (saját és szerződött partnereket)
l) kontrollálja a szervezet fizikai biztonságának betartását.

1.4 Gazdasági főigazgató

a) A pénzügyi és gazdasági vezető kontrolálja a 4. és 5 osztályba tartozó gazdasági és pénzügyi incidensek elhárítását.
b) Részt vesz az 5. típusú események elhárítására létrehozott stáb munkájában.
c) Kontrolálja a szervezet gazdasági tevékenységében bekövetkező anomáliák elhárítását.
d) Biztosítja a szervezet munkájához és biztonságához szükséges erőforrások elosztását.
e) Szükség esetén pénzügyi-, gazdasági támogatást nyújt más területen bekövetkező 4.-5. szintű incidensek mielőbbi felszámolására.
f) Biztosítja a szervezet biztonsági rendszerének működtetéséhez szükséges gazdasági és pénzügyi hátteret.
g) Saját hatáskörben felel a szervezet gazdasági és pénzügyi incidenseinek kivizsgálásában.
h) A gazdasági vezető a pénzügyi és gazdasági incidensek kivizsgálása esetén kéri vagy kérheti a biztonsági vezető és/vagy az informatikai igazgató támogatását és segítségét.

1.5 Médiaközpont vezető

a) Felel a szervezet vezetője által képviselt incidens és eseménykezelés kommunikációjában.
b) Amennyiben más kijelölés nem történik (a szervezet vezetője által) akkor, a média és nyilvánosság felé történő incidens ismertetés és kezelés a jelen szabályzat szerinti feladata.
c) A kereskedelmi és/vagy marketing, médiakommunikáció vezető felel a szervezet érintő incidensek szükség esetén elrendelendő hírzárlatáért.
d) A szervezet vezetőjének jóváhagyása nélkül a médiával és a nyilvánossággal önálló kommunikációt nem kezdeményez.
e) Az incidensek elhárításában nem, de azok megfigyelésében a kommunikációs részt vesz.
f) Hallgatólagos, de nem döntéshozó tagja a 4.5. szintű elhárítási stáb munkájának.

1.6 Informatikai Igazgató

a) Felel a szervezet informatikai rendszerének biztonságáért
b) Intézkedik az esetleges informatikai rendszer érintő problémák megoldásáról.
c) Az informatikai rendszer érintő incidensek esetén az informatikai igazgatósághoz tartozó személyek részvételével elhárítja a hibát, vagy támadást.
d) Az informatikai igazgató felel a 3.4. szintű informatikai incidensek kezeléséért.

e) Biztosítja a feltételeket a szervezet működőképességének és információáramlásának a fenntartásához.
f) Az informatikai igazgató irányításával és a biztonsági vezető közreműködésével (annak tudtával), illetve az incidens nagyobb kiterjedése esetén a gazdasági vezetővel és partnerkapcsolati vezetővel együtt részt vesz az 5. típusú incidensek elhárításában.
g) Az informatikát ért 4. szintű vagy magasabb támadásokról haladéktalanul értesíti a biztonsági vezetőt és az intézmény vezetőjét.
h) Amennyiben az incidens kiinduló pontja a szervezet fizikai területén belül van, úgy az azonnali intézkedésbe bevonja az őrszolgálat vezetőjét és a biztonsági vezetőt is.
i) Felügyeli a HelpDesk tevékenységét.
j) A biztonsági vezetővel együtt kontrollálja a HelpDesk munkájának pontosságát és szakszerűségét.
k) Időszakonként a HelpDesk ellenőrzésére a társ vezetők tájékoztatása mellett belső teszt incidenst generál.
l) Ellenőrzi a megfelelő adatkezelést és adatbiztonságot a szervezet központi rendszerében és output egységeinél.
m) Felügyeli a szervezetbe tartozó informatikusok munkáját és tevékenységét.
n) Felkérésre részt vesz más vezető által ellenőrzött vagy kezelt incidens kivizsgálásában.
o) Az informatikai incidensek kezelésénél az szervezet Információbiztonsági Szabályzatát (IBSZ) veszi alapul.
p) Kontrollálja az IBSZ és a kapcsolódó szabályzatok naprakész és aktualizált állapotát.
q) A Biztonsági Vezetővel együtt a szervezet vezetője felé a biztonsági szabályzatok és incidens kezelési szabályzat éves felülvizsgálatát kezdeményezi, szükség esetén módosítási javaslattételi jogával él.
r) A biztonsági vezetővel együtt kontrollálja a szervezetnél dolgozó személyes információbiztonsági tudatosságát, ellenőrzi az időszakos oktatások meglétét.
s) az 4.5. szintű incidensek kivizsgálásában és az incidens kezelő stáb munkájában aktívan részt vesz.

1.7 Információ Biztonsági Felelős

a) Az információbiztonsági vezető köteles az intézmény információ biztonsági szempontból történő működésének ellenőrzésére.
b) Köteles az adatkezelést és információbiztonságot érintő incidensek kivizsgálásában közreműködni, szükség esetén a törvény szerinti jelentést és módosítási javaslatot az intézmény vezetője felé megtenni.
c) Részt vesz a 3. szintűnél nagyobb incidensek kivizsgálásában és kontroljában.
d) Részt vesz a 4.5 szintű incidensek kivizsgáló stábjában.
e) Az intézményt ért támadások esetén jelentési kötelezettsége van a GOVCERT és NKI felé.
f) Az informatikai és biztonsági vezető mellett maga is kontrollálhatja a HelpDesk eseményeit, de nem a munkáját.

1.8 Adatvédelmi Tisztviselő (DPO)

a) A 2016. évi 679. EU rendelet szerinti feladatok ellátásának keretében ellenőrzi és kontrollálja az intézménynél kezelt személyes adatok rendszerét, folyamatát, és biztonságát.
b) A rendelet szerinti személyes adatvédelem betartásával kapcsolatban tett észrevételeit közvetlenül az intézmény vezetőjének jelenti.
c) Minden a rendelet szerinti személyes adatot érintő incidens, köteles jelenteni a NAIH (Nemzeti Adatvédelmi és Információszabadság Hatóság) részére.

d) Köteles minden személyes adatkezelési incidens kivizsgálni és arról jelentést készíteni.
e) Köteles elkészíteni és karban tartani az intézmény Adatkezelési szabályzatát.
f) A rendelet értelmében ellenőrzési joga van az intézmény minden személyi adattal kapcsolatban álló személye, csoportja vagy osztálya felett.
g) Köteles részt venni minden akár 1. szintű személyes adatot érintő incidens kezelésében függetlenül annak szervezeti egységhez, osztályhoz, szolgálathoz tartozásától.
h) Együtt kell működnie az intézmény Információbiztonsági Felelősével.

1.9 Tűzvédelmi Felelős

a) Köteles a szervezet tűzvédelmi szabályzatának és rendszerének karban tartását vagy karban tartatását elvégezni.
b) Köteles minden tűzvédelmi incidens kivizsgálásában részt venni.
c) Együttműködik a többi szervezeti vezetővel a tűzesetek és szervezeti kockázatok (adatvédelmi, információbiztonsági, fizikai biztonsági) összefonódása esetén a kivizsgálásban együttműködni.
d) Köteles minden tűzeset kivizsgálásakor a szabályzat kontrolját és szükség esetén módosítását kérni.
e) Köteles minden 1. szinttől induló tűz védelmi incidenst ellenőrizni.
f) Felel az intézményhez tartozó tűzvédelmi rendszerek és eszközök napra készen létéről. Az esetleges kockázatokat az intézmény vezetője felé azonnal jelenti.

1.10 Adatkezelő

a) Az adatkezelők mindazon személyek, akik az intézmény adatait, elektronikus és nyomatott információit kezelik, módosíthatják, a szervezet arra és személyükre, beosztásukra vonatkozó engedélyével.
b) Az adatkezelők kötelesek minden általuk tapasztalt az intézmény rendszereit, információit, eszközeit érintő anomáliákat, incidenseket jelenteni a HelpDesk felé.
c) Az adatkezelők kötelesek a maguk és az intézmény más tagjai által kezelt, használt adatok információk megőrzésében és védelmében mindent megtenni.
d) Az adatkezelők kötelesek a HelpDesk vagy a magasabb szintű incidens elhárításában részt vevők utasításait végrehajtani.
e) Az adatkezelők csak az általuk jogosan kezelt (részükre feldolgozásra átadott, munkavégzésükhöz szükséges) adatokhoz férhetnek hozzá. Minden más adathozzáférést vagy annak lehetőségét a HelpDesk felé jelenteni köteles.
f) Köteles az adatkezelés és az intézmény szabályzata és biztonsága szerint elvégezni és megakadályozni az illetéktelen hozzáférést.

1.11 Ügyintéző

a) Az ügyintézők a munkájukhoz szükséges körben, mennyiségben és minőségben szükséges adatokhoz, információk férhetnek hozzá.
b) Kötelesek az intézmény biztonsági intézkedéseit betartani.
c) Kötelezek az általuk észlelt minden az intézményt vagy a személyüket ért incidens, a HelpDesk felé bejelenteni.
d) Köteles az őrszolgálattal együttműködni.
e) Köteles a szervezet vagyon-, tűz-, adat-, információbiztonságát betartani
f) Köteles az adatkezelés és az intézmény szabályzata és biztonsága szerint elvégezni és megakadályozni az illetéktelen hozzáférést.

XX. INCIDENSKEZELÉSI FOLYAMATOK

1.1 Informatikai incidens

No	Esemény	Incidens szintje	FELADAT	VÉGREHAJTÁSI FÁZIS I	VÉGREHAJTÁSI FÁZIS II	VÉGREHAJTÁSI FÁZIS III	ESEMÉNY LEZÁRÁSA
1.	Rendszer leállás	1. osztály	HelpDesk jelentés (telefon, fax, mobil sms)	Visszahívás, Esemény részletes bekérése, leállás módja és formája (HW és SW hiba elkülönítés) kontrol lépések: Energia (230V) megléte, Monitor ki-bekapcsolás, Monitor és Táp kábelek megléte és csatlakozása, billentyűzet és/vagy egér csatlakozás ellenőrzés	Rendszer bootolás után, ha szükséges képernyőkép átvétellel admin jogosultsággal gép kontrol.		Működés visszaigazolás kontrol, HelpDesk naplóbejegyzés zárása, ok röviden
2.	Vírus fertőzés (vírus és malware)	1. osztály	HelpDesk jelentés (telefon, fax, mobil sms)	Jelzés utáni esemény kiolvasása a Vírusvédelmi rendszer naplóból. Szükség esetén rendkívüli vírusvédelmi ellenőrzés futtatás.			Működés visszaigazolás kontrol, HelpDesk naplóbejegyzés zárása, ok röviden
3.	Alkalmazás leállás, elérhetetlenség	1. osztály	HelpDesk jelentés (telefon, fax, mobil sms), adminok	Hálózati kapcsolat ellenőrzése, Felhasználói jogok lekérdezése, Alkalmazás terminál üzemmódban tesztelni			Működés visszaigazolás kontrol, HelpDesk naplóbejegyzés zárása, ok röviden
4.	Adatelérés részleges leállása	2. osztály	HelpDesk jelentés (telefon, fax, mobil sms) és rendszer adminok	Hálózati kapcsolat ellenőrzése, Felhasználói jogok lekérdezése, Alkalmazás terminál üzemmódban tesztelni			Működés visszaigazolás kontrol, HelpDesk naplóbejegyzés zárása, ok röviden
5.	Input, output eszközök	2. osztály	HelpDesk jelentés (telefon, fax, mobil sms) és rendszer	Hálózati kapcsolatok ellenőrzése. A jelzett eszköz státuszának lekérdezése (működőképesség, jogosultság,	Távoli terminál üzemmódban eszközelérés tesztelése		Működés visszaigazolás kontrol, HelpDesk naplóbejegyzés zárása, ok

	elérhetetlensége		adminok	hálózati kapcsolatok)			röviden
6.	Külső campus/telephely kapcsolat megszűnés	2. osztály	HelpDesk jelentés (telefon, fax, mobil sms) és rendszer adminok	Hálózati csatlakozás ellenőrzése, Internetes, Intranetes kapcsolat ellenőrzése, Jogok lekérdezése	Tűzfalak állapotának lekérdezése admin által.	Campus/telephelyi kapcsolat tesztelése.	Működés visszaigazolás kontrol, HelpDesk naplóbejegyzés zárása, ok röviden
7.	Zsaroló vírus fertőzés	3. osztály	HelpDesk jelentés (telefon, fax, mobil sms) és admin kérés	Gép hálózati leválasztatása, Gép és vírusvédelmi Admin kiküldése	Log elemzés, a fertőzés okának kivizsgálásáról, További megelőző intézkedések bevezetése	Mentésből helyreállítás, Jogosultságok visszaállítása, Mentési állományok vírusvédelmi ellenőrzése	Rendszer visszaállítás, gép visszaadás. Jelentések elkészítése, jegyzőkönyvi napló zárása. Biztonsági vezetői jelentés
8.	Jogtalan hozzáférési kísérlet	3. osztály	HelpDesk jelentés (telefon, fax, mobil sms) és admin kérés, Admin, biztonsági osztályvezető adatvédelmi tisztviselő, informatikai igazgató	Környezeti rendszer ellenőrzés. Adatbázis integritás ellenőrzés, Adatvesztés ellenőrzés, DPO értesítés, Biztonsági osztályvezető értesítés	Próbálkozások azonosítása (külső, belső), Logok elemzése, Jelszóváltoztatás elvégzése (kliens, admin),	DPO és Információbiztonsági Felelősi ellenőrzés, Szükség esetén szankciók bevezetése, Jelentés NKI és a NAIH felé, Személyi adatok sérülésének vizsgálata	Jelentések az esemény lezártjáról a NKI, MAIH felé. Új kontrollok bevezetése, szükség esetén szabályzat módosítása. Jegyzőkönyv zárása
9.	Adatvesztés, adatszivárgás	3. osztály	HelpDesk jelentés (telefon, fax, mobil sms) és admin kérés, Admin, biztonsági osztályvezető adatvédelmi tisztviselő, informatikai igazgató	Adatbázis vizsgálat kezdeményezése, DPO és Információbiztonsági Felelős vizsgálatának kezdeményezése. LOG elemzés indítása, Informatikai igazgató bevonása, szükség esetén Biztonsági osztályvezető és értesítése. A helyszín és a számítógép zárolása a hozzáférési adatok mentése.	Szükséges korlátozások bevezetése a DPO és INFOSEC Felelős által. Adatbázis helyreállítás megkezdése. Jelentésekhez szükséges adatok össze-gyűjtése, szükség szerint a helyzet eszkalálása egy szinttel feljebb.	Jelentések és szervezeti szabályzatok felülvizsgálata szükséges szankciók meghozatala. NAIH és NKI jelentések elkészítése, Szükség esetén GOVCERT értesítése.	Jelentések az esemény lezártjáról a NKI, MAIH felé. Új kontrollok bevezetése, szükség esetén szabályzat módosítása. Jegyzőkönyv zárása
10.	Nyomatatott dokumentum elvesztése	3. osztály	admin és biztonsági osztályvezető jelen-tés; Adatvédelmi tisztviselő (a	A nyomat tartalma szerinti ellenőrzés elindítása, Szükség esetén a nyomatatási kontrolok és szabályzatok módosítása. DPO és	Személyes adatok sérülése esetén a DPO irányítása szerinti eljárás lefolytatása	Szükséges szabályzatok módosítása, Személyes adat sérülése esetén incidens jelentés a NAIH	Jelentések az esemény lezártjáról a NKI, MAIH felé. Új kontrollok bevezetése, szükség esetén szabályzat

			nyomtatott dokumentum tartalma alapján eldöntendő)	INFOSEC felelős vizsgálata		felé.	módosítása. Jegyzőkönyv zárása
11.	Illegális rendszer hozzáférés	4. osztály	admin és biztonsági osztályvezető jelentés, DPO, informatikai igazgató	Azonnali admin, Informatikai igazgatói, biztonsági osztályvezető vezetői kivizsgálás kezdeményezése	Adatintegritás és szivárgás ellenőrzése. LOG fájlok olvasása és vizsgálata. Hozzáférési kísérlet céljának és tartalmának tisztázása. A kísérlet által okozott incidens miatti szabályok módosítása	Szankciók meghozása, Ha kell új ellenőrzések bevezetése. Ha szükséges (adatszivárgás okon) jelentés a NAIH és NKI felé.	Szabályzat módosítási javaslat benyújtása, Jegyzőkönyv lezárása. Szankciók bevezetése. Szükség esetén a BTK alkalmazása.
12.	Illegális eszköz megjelenése a hálózaton	4. osztály	admin és biztonsági osztályvezető jelentés, adatvédelmi tisztviselő, informatikai igazgató	Informatikai igazgatói és Biztonsági osztályvezetői kivizsgálás indítása. Jelentés az incidenskezelő team felé. Őrszolgálati kontrol erősítése. Őrszolgálati szabályzat átvizsgálása, módosítása.	Eszköz leválasztása, eszköz által gyűjtött információk elemzése, LOG elemzés elvégzése. Hálózati analízisek elvégzése	Hálózatbiztonsági szabályok módosítása (IBSZ módosítása). Szabályok felülvizsgálata, szükség esetén módosítása. Adatszivárgás esetén annak típusától függően jelentés a NEI vagy NAIH felé	Szabályzat módosítási javaslat benyújtása, Jegyzőkönyv lezárása. Szankciók bevezetése. Szükség esetén a BTK alkalmazása.
13.	Belső támadás, vagy belső rendszer összeomlás	5. osztály	admin és biztonsági osztályvezető jelentés, adatvédelmi tisztviselő, informatikai igazgató	Azonnali admin értesítés, Támadás irányának és céljának felderítése. Lehetőség szerint az őrszolgálattal a támadás lokalizálása és kiiktatása (Belső támadás). Külső támadás esetén annak formája és módja szerint ellentevékenység megkezdése. Szükség esetén a GOVCERT bevonása.	Adatvesztés és adatszivárgás kivizsgálása, Az incidenskezelési team közös tevékenységének indítása. Kontrollok és elkerülő utak, lehetőségek keresése. Rendszerek zárása, esetleg HonayPot-ok elhelyezése.	Károk felmérése, Adatvesztés kontrolja. Szükséges veszteségi értékek számítása. Szabálymódosítások elvégzése.	Szabályzat módosítási javaslat benyújtása, Jegyzőkönyv lezárása. Szankciók bevezetése. Szükség esetén a BTK alkalmazása. Média kommunikáció meghatározása.

14.	Hálózati hozzáférés leállás, fogadási rendszer és kapcsolat megszakadás	5. osztály	Biztonsági osztályvezető, Informatikai igazgató, Adatvédelmi tisztviselő, informatikai igazgatóság érintett munkatársai, Incidens kezelő team	Azonnali Incidenskezelői team összehívása, admin és biztonsági osztályvezető a kivizsgálást közben elkezdik.	Működés helyreállításának kísérlete ("B" site). Támadás vagy belső hiba meghatározása.	Biztonsági kontrollok és szabályok felülvizsgálata. További hasonló incidens elkerülésére hozandó szabályok bevezetése.	Szabályzat módosítási javaslat benyújtása, Jegyzőkönyv lezárása. Szankciók bevezetése. Szükség esetén a BTK alkalmazása. Média kommunikáció meghatározása.
15.	Internetes TÁMADÁS, szolgáltatás leállással, szervezeti IT infra-struktúra leállása	6. osztály	Szervezet vezetőjének irányításával, Incidens kezelő team	Portok lezárása, Kommunikáció a GOVCERT-el. Szervezet vezetői döntés megszerzése	Az incidens kezelési csoport vezetői utasítás szerinti munkavégzése	Inciden okozta károk felszámolás, Értékvesztés és kárérték meghatározása	A vezetői döntések végrehajtása. Jelenntések és média kommunikácó indítása.

1.2 Adatkezelési Incidens

No	Esemény	Incidens szintje	FELADAT	VÉGREHAJTÁSI FÁZIS I	VÉGREHAJTÁSI FÁZIS II	VÉGREHAJTÁSI FÁZIS III	ESEMÉNY LEZÁRÁSA
1.	Adatvesztés Adatmódosítás	4. osztály	admin és biztonsági osztályvezető jelentés	Adatbázis vizsgálat kezdeményezése, DPO és Információbiztonsági Felelős vizsgálatának kezdeményezése. LOG elemzés indítása, Informatikai igazgató bevonása, szükség esetén Biztonsági osztályvezető értesítése. A helyszín és a számítógép zárolása a hozzáférési adatok mentése.	Szükséges korlátozások bevezetése a DPO és INFOSEC Felelős által. Adatbázis helyreállítás megkezdése. Jelentésekhez szükséges adatok összegyűjtése, szükség szerint a helyzet eszkalálása egy szinttel feljebb.	Jelentések és szervezeti szabályzatok felülvizsgálata szükséges szankciók meghozatala. NAIH és NKI jelentések elkészítése, Szükség esetén GOVCERT értesítése.	Jelentések az esemény lezártáról a NKI, MAIH felé. Új kontrollok bevezetése, szükség esetén szabályzat módosítása. Jegyzőkönyv zárása
2.	Rendszeradatok és alkalmazás adatok kompromittálódása	4. osztály	admin és biztonsági osztályvezető jelentés, Adatvédelmi tisztviselő kontroll	Informatikai igazgató irányításával az Incidenskezelő team összeállítja az azonnali beavatkozási módszerek és intézkedések sorrendjét.	Az adminok megkezdik a LOG elemzéseket. Azonnali jelszóváltoztatás elrendelése, szükség esetén rendszer leválasztás és teljes körű zárlat elrendelése.	Adatvesztés és kompromittálódás mértékének meghatározása, Szabályzatok módosítása és szankciók meghozatala.	Jelentések a szervezet vezetője felé. Média kommunikáció egyeztetése. A veszteségi költségek meghatározása.
3.	Személyes adat vesztés adatmódosítás	5. osztály	Biztonsági vezető, Informatikai vezető, Adatvédelmi tisztviselő	DPO által kezdeményezett eljárás indítása. DPO vezetésével indul az Incidenskezelő team munkája.	Vesztett adatok mértékének meghatározása. Érintettek tájékoztatása. Szabályok módosítása. NAIH jelentés előkészítése. Szükség esetén PTK szerinti eljárás indítása.	Szabályzatok átvizsgálása. Új biztonsági intézkedések bevezetetése. Esemény történetének, a károkozás mértékének feldolgozása.	Incidensben érintettekkel egyeztetés, NAIH jelentés, Szabály módosítás, Média kommunikáció egyeztetés
4.	Személyes adat kompromittálódás	5. osztály	Biztonsági vezető, Informatikai vezető, Adatvédelmi tisztviselő	DPO által kezdeményezett eljárás indítása. DPO vezetésével indul az Incidenskezelő team munkája.	Vesztett adatok mértékének meghatározása. Érintettek tájékoztatása. Szabályok módosítása. NAIH jelentés előkészítése. Szükség esetén PTK szerinti eljárás indítása.	Szabályzatok átvizsgálása. Új biztonsági intézkedések bevezetetése. Esemény történetének és a károkozás mértékének feldolgozása.	Incidensben érintettekkel egyeztetés, NAIH jelentés, Szabály módosítás, Média kommunikáció egyeztetés

A biztonsági incidensek kategóriájába az alábbi események tartoznak:

a) Információs vagyon (eszköz, szoftver, adat, stb.) elvesztése, módosítása, eltulajdonítása, vagy megrongálódása.
b) Jogosulatlan hozzáférés (informatikai eszközhöz, alkalmazáshoz, adathoz, biztonsági zónához)
c) Határincidensek, vírusfertőzések,
d) A mentési feladatok végrehajtásának akadályoztatása,
e) Működési rendellenességek (információ biztonságot veszélyeztető eszköz hiba, program hiba, információ rendelkezésre állásának elvesztése, hibás adatok, stb.),
f) Az IBSZ-ben hivatkozott törvények, szabályzatok és előírások, vagy az IBSZ szabályzatának megsértésére utaló cselekmények.

Incidensek priorizálása

MAGAS PRIORITÁSÚ INCIDENSEK (4,5,6 OSZTÁLY): Az incidensek kivizsgálását és elhárítását azonnal meg kell kezdeni.

a) Információs vagyon (eszköz, szoftver, adat, stb.) elvesztése, módosítása, eltulajdonítása, vagy megrongálódása.
b) Határsértés, és illegális tevékenység észlelése (behatolás).
c) Jogosulatlan hozzáférés (informatikai eszközhöz, alkalmazáshoz, adathoz, biztonsági zónához)
d) Vírus-vészhelyzet (tömeges fertőzés), vagy központi vírusvédelmi eszköz kiesése.
e) Adminisztrátori jogosultságok sérülése.
f) Kritikus rendszer, vagy rendszer elemek kiesése.
g) „Titkos" információk bizalmasságának, sértetlenségének elvesztése.

KÖZEPES PRIORITÁSÚ INCIDENSEK (3,4 OSZTÁLY): Az incidensek kivizsgálását azonnal meg kell kezdeni, ha az egy magas prioritású incidens elhárítása nem akadályozza.

a) Ismétlődő vírusfertőzés, vagy vírusdefiníciós állomány nem frissülése.
b) Felhasználói jogosultságok sérülése.
c) Kiemelten fontos rendszer, vagy rendszer elemek kiesése.
d) „Bizalmas" információk bizalmasságának, sértetlenségének elvesztése.

ALACSONY PRIORITÁSÚ INCIDENSEK (1,2 OSZTÁLY): Az incidensek feldolgozását két órán belül meg kell kezdeni, ha az egy magasabb prioritású incidens elhárítása nem akadályozza.

a) Egyszeri vírusfertőzés, vagy helyi vírusvédelmi eszköz kiesése. (Amennyiben a vírusvédelmi rendszerrel az eszköz kiesése a felhasználó részéről automatikusan megoldható, nem szükséges további intézkedés.)
b) Fontos rendszer, vagy rendszer elem kiesése.
c) Kisebb jogosultsági incidensek (felhasználó elfelejtette a jelszavát, vagy az lejárt, stb.).
d) Vírusvédelmi menedzsment eszközök kiesése.

EGYÉB INCIDENSEK: Az incidensek kivizsgálását lehetőleg még a bejelentés vagy az észlelés napján, a folyamatban levő magasabb prioritású incidensektől függően kell megkezdeni.

a) Nem fontos rendszer, vagy rendszer elem kiesése.
b) Munkaállomás működésével kapcsolatos működési hibák.
c) Szabály-, és eljárássértések.
d) Felhasználói hibák.

Biztonsági incidensek kezelésének folyamata

A MATE informatikai rendszerét használója köteles értesíteni az Informatikai Igazgatóság munkatársait lokális probléma esetén vagy az adatvédelmi tisztviselőt kiterjedt probléma esetén az általa észlelt biztonsági incidensekről.

Incidens bejelentés bármely MATE informatikai eszközt használó, vagy üzemeltető MATE munkatársától érkezhet.

Az incidenseket a HelpDesk rendszeren keresztül kell bejelenteni.

Az incidensek kezeléséért felelős személyek az alábbiak:

a) Kisebb incidensek: informatikai igazgatóság munkatársa
b) Vírusvédelmi incidensek: informatikai igazgatóság munkatársa
c) Határvédelmi incidensek: informatikai igazgatóság munkatársa, adatvédelmi tisztviselő, információvédelmi felelős
d) Jogosultsági incidensek: adatgazda, informatikai igazgatóság munkatársa, információvédelmi felelős
e) Rendelkezésre állási incidensek: adott rendszer/eszköz rendszergazdája,
f) Törvény-, szabály-, és eljárássértések: Rektor, adatvédelmi tisztviselő

A biztonsági incidensek kezelése:

a) A bejelentett incidensről szükséges minden rendelkezésre álló információt elkérni a felhasználótól/bejelentőtől. Minden vonatkozó információt rögzíteni kell. A bejelentéseket (pl. e-mail vagy telefon) minden esetben, a prioritásától függően minél hamarabb vissza kell igazolni.
b) Amennyiben az informatikai igazgatóság munkatársa saját hatáskörben meg tudja oldani a bejelentett incidenst, és a megoldott incidenssel kapcsolatban a bejelentő 2 napon belül nem jelzett vissza, az incidens megoldottnak tekinthető. A megoldott incidensről a felhasználót/bejelentőt értesíteni kell.
c) Amennyiben az informatikai igazgatóság munkatársa saját hatáskörben nem tudja megoldani a bejelentett incidenst, prioritástól függően azonnal értesíteni kell az információvédelmi felelős és a felettesét. Ebben az esetben a probléma megoldására az információ biztonsági felelős az informatikai igazgatóság munkatársával együttműködve, megpróbálja a megfelelő megoldást kidolgozni.
d) Amennyiben a probléma továbbra sem oldódik meg, a probléma szélesebb eszkalálása szükséges. Ebben az esetben a probléma további megoldására az információ biztonsági felelős az informatikai igazgatóság munkatársával együttműködve, külső szakértő vagy a rendszer szállítójának bevonásával megpróbálja a megfelelő megoldást kidolgozni.
e) Ha eddig a pontig eljutva sem sikerül megoldást találni a problémára, akkor az információ biztonsági felelős az informatikai igazgatóság munkatársával az alábbi döntés előkészítő javaslatokat teszi a MATE informatikai igazgatója részére.
f) A probléma súlyosságát mérlegelve vészhelyzetet kell elrendelni és a vészhelyzeti terveknek megfelelően a normál működésre történő visszaállítást végrehajtani.
g) A probléma súlyosságát mérlegelve fejlesztések, vagy beszerzések elindítása.
h) Az incidens okozta kockázatokat csak a rektor és az informatikai igazgató vállalhatják fel az információ biztonsági felelős javaslata alapján.

Az incidensek elhárítására, az informatikai igazgatóság munkatársa hatáskörén kívül tett intézkedéseket az adatvédelmi tisztviselőnek jelenteni kell, aki a szükséges információkat dokumentálja.

A konkrét vészhelyzeti tervek és operatív tennivalók a tervezés során meghatározott helyen, formanyomtatványon vannak meghatározva. A vészhelyzethez tartozó általános adatok a *11. számú mellékletben* vannak felsorolva.

Problémakezelés

A problémakezelés célja az elhárított incidensek okának feltárása, és a kiváltó ok megszüntetése ezen incidensek előfordulásának csökkentése, vagy megszüntetése érdekében. A keletkezett és lezárt incidensek hiba okának felderítése a kezelésében résztvevő kollegák feladata.

Eredménye lehet:

a) hiba okának definiálása a hozzá tartozó megoldással,
b) hiba okának definiálása megoldás nélkül,
c) incidens vizsgálat folyamatossá tétele a kellő információ hiányában.

Amennyiben sikerült feltárni a hiba okát, azt rögzíteni kell a „tudásbázisban" illetve meg kell osztani a teljes informatikai szervezet körében. A hiba okát ismerve intézkedéseket kell tenni a kiváltó ok végleges megszüntetésére, illetve az általa okozott probléma előfordulási gyakoriságának csökkentésére.

XXI. ADATVÉDELMI ELJÁRÁSOK MENEDZSMENTJE

1.1 A határvédelem megvalósítása

A MATE informatikai rendszere és az internet között határvédelmi technikai megoldások biztosítják a biztonság megfelelő szinten tartását. A biztonsági szint fenntartása érdekében az alább felsorolt előírások szükségesek.

A MATE egységes és homogén határvédelmi eszközök alkalmazására törekszik (tűzfal, vírusvédelmi gateway-ek, appliance stb.). A határvédelmi eszköz felülvizsgálatát évente kell elvégezni és szükség esetén fejlesztéseket kell végrehajtani (cseréje, upgrade-je, újra licencezése stb.).

Az életcikluson belül a határvédelmi eszközök biztonsági frissítéseit rendszeresen, folyamatosan el kell végezni. A firmware frissítéseket legalább évente szükséges ellenőrizni illetve végrehajtani. A szignatúra-frissítéseket, amennyiben automatikusan beállítható az eszközön, napi rendszerességgel kell ütemezni; amennyiben manuális beavatkozást igényel, hetente kell elvégezni.

Biztosítani kell, hogy a határvédelmi eszközökhöz csak kiemelt felhasználók (erre a célra kijelölt és kiképzett rendszergazdák) férjenek hozzá. A MATE egységes határvédelmi eszközein minden tevékenységet naplózni kell, a beállításokat minden változtatás előtt és azt követően menteni szükséges.

Az egységes határvédelmi eszközöket rendszeresen monitorozni kell. Célszerű központi loggyűjtő és monitoring rendszer használata. A monitorozás eredményét minden esetben vissza kell csatolni, ha szükséges fejlesztést, vagy szabályozást kell végrehajtani, bevezetni. Az egységes és homogén határvédelem dokumentációját úgy kell tárolni, hogy az indokolatlan hozzáférés, illetve az illetéktelen kezekbe jutásuk elkerülhető legyen.

Amennyiben lehetséges a tűzfalak naplóit központi loggyűjtő szerveren kell tárolni

Vírusvédelem

A vírusvédelem irányelvei:

A MATE vírusvédelmi rendszere korszerű vírusvédelmi technológiák, összehangolt folyamatok és szabályok összessége, melyek alkalmazásának irányelvei az alábbiak:

a) ***Megelőzés:*** a MATE a rosszindulatú programkódok elleni védekezésben a megelőző folyamatokra koncentrál.
b) ***Folyamatosság:*** a vírusvédelmi kockázatok csökkentése, valamint a fertőzések megelőzése érdekében a vírusvédelmi rendszert folyamatosan, ebben a szabályzatban megfogalmazott módon kell működtetni.
c) ***Reagálás:*** A világban folyamatosan változó, vírusvédelemmel kapcsolatos kihívásokra a MATE igyekszik rugalmasan, gyorsan, és hatékonyan reagálni.
d) ***Tudatosság:*** A vírusvédelmi rendszer hatékony ága jelentős mértékben növelhető, ha a vírusvédelemben résztvevő személyek (informatikai dolgozók, felhasználók), felkészültsége, motivációja, illetve tudatos felelősségvállalása biztosított.

A MATE-nál a vírusvédelem központilag irányított folyamat. A részletes vírusvédelmi előírásokat a MATE Vírusvédelmi szabályzata tartalmazza.

A jogosultsági rendszer megvalósítása

Az adatok bizalmasságának és sértetlenségének biztosítása érdekében a MATE-nál egységes jogosultság kezelő és nyilvántartó rendszer működik, amely alapja az LDAP/AD rendszer.

A jogosultsági rendszer a felhasználói csoportokon és ezek hierarchikus rendszerén keresztül biztosítja az adatok adatosztályozási szintjeinek megfelelő bizalmassági és sértetlenségi követelményeknek való megfelelést.

A jogosultságokkal és azok kezelésével kapcsolatos előírásokat a ***XXXI. számú fejezet*** tartalmazza.

Mentés, archiválás, visszatöltés

Az adatok rendelkezésre állásának biztosítása érdekében a MATE-nál egységes biztonsági alapokon nyugvó mentési, archiválási, illetve visszatöltési rendszert kell kialakítani, működtetni.

A mentési, archiválási, illetve visszatöltési rendszernek biztosítania kell az adatok adatosztályozási szintjének megfelelő rendelkezésre állási követelményeknek való megfelelést.

A mentési, archiválási, illetve visszatöltési rendszer eljárásait, előírásait, és a rendszer üzemeltetésével kapcsolatos feladatokat a ***XXXI. számú fejezet*** tartalmazza.

XXII. INFORMATIKAI SZOLGÁLTATÁSOK BIZTONSÁGA

1.1 Alkalmazás-, és szoftvereszközök használatának szabályozása

A MATE minden munkatársa számára biztosítja a munkavégzéshez szükséges jogtiszta szoftvert. A személyhez kötött munkaállomásokra, nyilvánosan elhelyezett, közös használatú munkaállomásokra illetve az otthoni munkavégzéshez biztosított, MATE tulajdonban lévő munkaállomásokra csak azok az alkalmazások, és szoftver eszközök telepíthetők, amelyre az alkalmazottnak a munkájához szüksége van, és az adott alkalmazással a távoli elérés engedélyezett. A szoftverek telepítése a rendszergazdák feladata.

Az elektronikus adatok és a levelezés biztonságának irányelvei

A MATE informatikai rendszerében kezelt (továbbított, tárolt) elektronikus adatok, így az elektronikus levelek is - a levelek feladójától, címzettjétől, tartalmától függetlenül-, a MATE tulajdonát képezik.

A felhasználók a MATE rendszereit és erőforrásait csak az engedélyezett módon és mértékben használhatják. A MATE rendszerein, ily módon elhelyezett adatokért a felhasználót terhel minden jogi felelősség. A használatot a MATE kijelölt szakemberei ellenőrizhetik, illetve korlátozhatják.

Súlyos adatvédelmi incidensnek minősül és tilos a levelek külső szolgáltató felé történő átirányítása!

Az internet elérés biztonságának irányelvei

A MATE az internet elérést a MATE kutatási és ügyviteli folyamataihoz, és az azokat támogató folyamatok fenntartásához ahol ez technikailag lehetséges az KIFÜ hálózatán keresztül biztosítja.

Az internetelérés során biztosítani szükséges, hogy a kártékony tartalmak ne juthassanak el a MATE rendszereibe.

Fájlkezelés

A MATE informatikai rendszerében kezelt (továbbított, tárolt) elektronikus adatok így a fájlok is a MATE tulajdonát képezik. A fájlok kezelése során törekedni kell, hogy a tároló rendszerben az adott fájlnak minél kevesebb példánya tárolódjon. Dokumentumok közzététele esetén célszerű a fájlt egy helyre letárolni, és a címzetteknek a fájl elérési útvonalát tartalmazó, a fájlra mutató linket megküldeni.

A felhasználók a fájljaikat a központilag kialakított helyen kötelesek tárolni (központi adattárolók, felhőszolgáltatás, campus/telephelyen kialakított adattárolók). Nyilvános mappában tilos elhelyezni „Bizalmas", vagy ennél magasabb minősítésű dokumentumot. A felhasználóknak tilos megosztani az egyéni mappájukat, valamint saját helyi tárolójukon tárolni munkával összefüggő fájlokat.

XXIII. A BIZTONSÁGI SZINT MÉRÉSE, MONITOROZÁSA

1.1 A biztonsági szint mérésének feltételei

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

a) A mérés függetlenségének biztosítása:

1. A méréseket a mérésben érintettek előzetes értesítése nélkül kell végrehajtani, hogy ne tudjanak felkészülni, illetve ne tudják befolyásolni a mérés eredményét.
2. Az informatikai rendszer biztonsági szintjének mérése a rektor által megbízott külső megbízott feladata. A méréseket a felhasználóktól, az üzemeltetési területtől független személy végzi.

b) A mérés hitelességének biztosítása:

1. Az informatikai rendszer elemeinek idő szinkronizálása szükséges a naplófájlok megbízható kiértékeléséhez
2. A biztonsági szint mérésével megbízott személy rendelkezzen naplófájlok eléréséhez szükséges felhatalmazással.
3. Biztosítani kell a naplófájlok sértetlenségét. A naplófájlokhoz csak olyan személyeknek legyen hozzáférése, akiknek a munkájához feltétlen szükséges

A biztonsági szint mérésének eszközei és módszerei

Technikai szintű auditok. A biztonság szintjének mérésének egyik leghatásosabb módszere a technikai audit jellegű felmérések, amelyek lehetnek:

a) Az informatikai rendszer Internet felöli sérülékenységeinek vizsgálata.
b) Az informatikai rendszer Intranet felöli sérülékenységeinek vizsgálata.

Technikai szintű auditot a MATE-nál kétévente, a fenyegetettségek felmérésével egy időben kell elvégezni.

Személyi biztonság szintjének mérése

A személyi biztonság szintjének mérését a MATE-nál kétévente, a fenyegetettségek felmérésével egy időben kell elvégezni. A vizsgálat célja feltárni a felhasználók magatartásában, szokásaiban, tudatosságában rejlő alapvető biztonsági hiányosságokat.

A vizsgálat az alábbi területekre terjed ki:

a) A felhasználók adat-tárolási szokásaira
b) A felhasználók levelezési szokásaira
c) A felhasználók Internetezési szokásaira

Az informatikai rendszer monitorozása

Az informatikai rendszer kritikus elemeit, illetve biztonsági eszközeit folyamatosan kell monitorozni.

A monitorozásnak minimálisan az alábbi témákra terjed ki:

a) Határvédelmi incidensek, és hálózati illegális tevékenység
b) Vírusvédelmi incidensek
c) Jogosultság kezelési incidensek (pl.: 6-nál többszöri sikertelen belépések száma)
d) Mentési feladatok sikeres/sikertelen végrehajtása
e) Védett adatok hozzáférésének naplózása
f) Hiba jellegű incidensek
g) Külső vagy távoli felhasználók tevékenységei, távoli elérések naplózása
h) Rendszergazdák tevékenységei
i) Rendszer konfigurációjának megváltoztatása
j) Biztonsági riasztórendszerek naplózása (UPS, Tűzvédelem, Behatolás/betörés védelem, stb.)

A mérési adatok feldolgozása, visszacsatolása

Az információbiztonság szempontjából kritikus pontokon mérési és ellenőrzési rendszert kell bevezetni. A mérések eredményéről az **adatvédelmi tisztviselő** évente írásban számol be az **MATE rektorának.**

A mérési rendszer kontroll pontjait összefoglaló táblázat a *12. számú mellékletben* található.

Ellenőrzési irányelvek

Az információ biztonság szinten tartása érdekében megfelelő kontrollokat kell kialakítani. A kontrollok kialakításánál elsődlegesen azt kell figyelembe venni, hogy azok által az információbiztonság szintje mérhető legyen. Ennek érdekében meg kell határozni az ellenőrzések területeit, és minden területhez külön- külön meg kell fogalmazni az ellenőrzési célkitűzéseket.

Az ellenőrzési célkitűzések ismeretében meg kell jelölni az ellenőrzés eszközeit (dokumentumok, naplók, szoftverek, adatok, amelyek a biztonsági rendszerről hiteles képet tudnak adni), azok tartalmi követelményeit.

Az ellenőrzés eredménye minden esetben kiértékelésre kerül, amelyből a megfelelő következtetések levonhatók, így a kapott eredmények visszacsatolhatóak a biztonsági folyamatra. Vagy szükség esetén felelősségre vonási eljárást is kezdeményezhető.

Az ellenőrzéseket dokumentumok, dokumentációk, személyes beszámoltatás és helyszíni szemlék alapján lehet végrehajtani.

Az információ biztonsággal kapcsolatos ellenőrzések területei az alábbiak lehetnek:

a) ***Megfelelőségi vizsgálat.*** Célja felderíteni, hogy a MATE szervezeti egységei, és Intézetei rendelkeznek-e a törvényi előírásokban meghatározott személyi, eljárási, tárgyi feltételekkel, és azok megfelelően dokumentáltak-e.
b) ***Az információ biztonság szintjére vonatkozó vizsgálat***. Célja felderíteni, hogy a MATE szervezeti egységeinél és Intézeteinél az információ biztonság szintje megfelel-e a meghatározott védelmi szintnek.
c) ***Az információ biztonsági szabályok betartásának ellenőrzése.*** Célja felderíteni, hogy a MATE információ biztonsági szabályait az illetékes személyek ismerik-e, illetve betartják-e. Ez az ellenőrzés az információ biztonság egy-egy területére is leszűkíthető.

Az ellenőrzések során elsősorban az alábbiakat kell vizsgálni:

a) Az információbiztonsági rendszer működése megfelel-e a törvényi előírásoknak.
b) Az információbiztonsági rendszer felépítése, tartalma megfelel-e az ISO 27001 szabványnak.
c) Az információbiztonsági szabályok érvényesítve vannak-e a folyamatokban.
d) Az információbiztonsági rendszer előírt dokumentumai léteznek-e, illetve naprakészek-e.
e) Az információszemélyzet, illetve a felhasználók rendelkeznek-e a megfelel információbiztonsági ismeretekkel.
f) Az adatokra és rendszerekre vonatkozó kezelési szabályok betartását.
g) A naplózási rendszer megfelelő alkalmazását. A biztonsági események kezelésének, a szükséges mértékű felelősségre vonás gyakorlatát.
h) A mentési rendszer megfelelő alkalmazását.
i) Az informatikai rendszert üzemeltetők, és felhasználók információ biztonsággal kapcsolatos ismereteit.
j) A hozzáférési jogosultságok nyilvántartásának naprakészségét, a kiadott jogosultságok szükségességét.
k) A dokumentációk pontosságát - naprakészségét, változás követését, megfelelő kezelését/nyilvántartását.
l) Az alkalmazott szoftverek jogtisztaságát.
m) A szerződések megfelelőségét.
n) A fizikai biztonsági előírások betartását.

Az információbiztonsági rendszer, illetve annak egyes elemeit rendszeresen felülvizsgálatra kerülnek. A biztonsági rendszerek felülvizsgálati idejét összefoglaló táblázat a *12. számú mellékletben* található.

XXIV. A SZERVERTEREM KIALAKÍTÁSÁNAK KÖVETELMÉNYEI

1.1 A szerverterem elhelyezésének szempontjai

Az szerverterem elhelyezésének biztonsági szempontjai az alábbiak:

a) A belmagasságot is figyelembe véve biztosítsa az egyes szerverek, vagy egyéb aktív eszközök számára szükséges levegő térfogatot.
b) A helyiség aljzatának megfelelő statikai terhelhetősége az elhelyezett eszközök tömegét, és fizikai méretét figyelembe véve.
c) A helyiség ajtajának mérete biztosítsa az elhelyezésre kerülő eszközök akadálytalan ki- és beszállítását.
d) A helyiséghez vezető folyósok, lépcsők, liftek alkalmasak legyenek az elhelyezésre kerülő eszközök ki-, és beszállítására.
e) A helyiség határoló falai és nyílászárói alkalmasak legyenek a fizikai betörések megakadályozására.

   A helyiség elhelyezését úgy kell megválasztani, hogy a felette elhelyezkedő helyiségekben ne legyen vizes blokk (mosdó, WC, konyha, stb.). Ellenkező esetben a födém vízzárásának kialakítása szükséges.

f) Ha a szerverszoba szintjén vízkár veszélye forog fenn (árvíz, belvíz, csőtörés, stb.), akkor az alábbi védőmechanizmusok bevezetése szükséges:

   1. Alpadló, a berendezések mennyezetről való táplálása.
   2. Falak, nyílászárók vízbehatolás elleni védelme.
   3. Ún. védőtálcák alkalmazása a berendezések elhelyezésére.

g) Azokon a campus/telephelyeken ahol nincs kialakított szerverterem, hálózati feladatokat ellátó eszközöket zárható rack szekrényben kell tárolni melynek elhelyezésénél lehetőség szerint figyelembe kell venni a szerverszoba kialakítására vonatkozó szabályokat.

A szerverterem behatolás védelme

A bizalmas adatok tárolását végző szerverek esetében a szerverterem behatolás-védelmének biztosítása érdekében az alábbi szempontokat kell érvényesíteni:

a) Belépést regisztráló rendszer kialakítása (a munka befejezését is célszerű rögzíteni).
b) Automatán záródó ajtó, mely kifelé kézzel nyitható (a menekülés biztosítása érdekében).
c) Betörés-riasztó rendszer alkalmazása.

A szerverterem tűzvédelem

A szerverterem tűzvédelmének biztosítása érdekében az alábbi szempontok figyelembe vétele szükséges:

a) A tűz-, vagy füstriasztó rendszer alkalmazása.
b) Kézi tűzoltó-berendezések elhelyezése a bejárat közvetlen közelében.

A szerverterem áramellátása

A szerverterem illetve a szervertermen kívüli zárt rack-szekrényben elhelyezett hálózati aktív eszközök áramellátásának biztosítását az alábbi szempontok szerint kell végrehajtani:

a) A teljes épület villámvédelmének biztosítása.
b) A szerverterem független betáplálásának biztosítása.
c) A szerverteremben illetve az azon kívül zárt rack-szekrényben üzemeltetett eszközök túlfeszültség elleni biztosítása.
d) A főkapcsolók biztonságos helyen való elhelyezése (lehetőleg a bejárat közelében). A főkapcsolók legyenek védve illetéktelen beavatkozás ellen.
e) Az eszközök szünetmentes tápellátása (központi UPS vagy helyi UPS-ek).
f) A helyiség betáplálásának terhelés elosztása fázisonként.
g) Az UPS-ek betáplálásának elosztása fázisonként.
h) A szerverteremben illetve az azon kívül zárt rack-szekrényben elhelyezett eszközök részére minimálisan 30 perc tartási időre méretezett UPS-t kell alkalmazni.
i) Az UPS-ek akkumulátorait legalább évente egyszer (pl. a tervszerű megelőző karbantartás alkalmával) tesztelni kell és szükség esetén gondoskodni kell azok haladéktalan cseréjéről).
j) Érintésvédelem kialakítása, rendszeres felülvizsgálata.

A szerverterem klimatizálása

A szerverterem üzemi hőmérsékletének szabályozásának érdekében az alábbi szempontok figyelembe vétele szükséges:

a) A szerverteremben klíma-berendezéseket kell üzemeltetni, a megfelelő üzemi hőmérséklet szabályozására.
b) A klímarendszer független legyen az épület egyéb klíma rendszereitől.
c) A klíma berendezések darabszámát, típusát, teljesítményét úgy kell tervezni, hogy a szerverteremben elhelyezett eszközök hődisszipációs mutatói mellett, még egy klímaberendezés meghibásodása esetén is biztosítani tudják a megfelelő szabályozást.
d) A klíma-berendezések automatikus újraindítását biztosítani kell az esetleges áramszünet megszűnése esetén.
e) A csapadékos évszakokban, különösen alagsori helységek esetén a megnövekedett pára kártékony hatása ellen páramentesítő alkalmazása célszerű.

Zavarvédelem

A szerverterem zavaráló képességének biztosítására az alábbiakat kell megfontolni: gépészeti eszközök (víz-, gáz-, fűtés vezetékek, stb.) eltávolítása javasolt.

XXV. A SZERVERTEREM HOZZÁFÉRÉSI KÖVETELMÉNYEI

1.1 A szerverterem nyitásának, és zárásának szabályai

A szervertermet folyamatosan zárva kell tartani még akkor is, amikor a helyiségben éppen munkavégzés folyik. Amennyiben a fenti követelmény valamilyen ok miatt nem követhető (pl.: meghibásodás, vagy beszállítás) a szerverterem bejáratának felügyeletét meg kell oldani.

A szerverterembe történő belépés, kilépés rendje

Kerülni kell a szerverteremben indokolatlan belépést. Azokat az üzemeltetési feladatokat, amelyek távoli eléréssel elvégezhetők, távoli menedzsment alkalmazásával kell elvégezni. A szerverterembe csak az arra felhatalmazott személyek léphetnek be. A MATE-nál a szerverterembe a következő személyek belépése engedélyezett:

a) informatikai igazgató,
b) munkaköri leírása alapján arra jogosult munkatársak,
c) az adatvédelmi tisztviselő,
d) információ biztonsági felelős,
e) a fentiek valamelyikének jelenlétében megbízott vagy felkért auditor,
f) a fentiek valamelyikének jelenlétében és felügyelete alatt telepítést, karbantartást végző külső munkatárs.

A szerverterembe történő belépéseket dokumentálni kell. A dokumentáció tartalmazza:

a) a belépő nevét,
b) a belépés célját, külső munkatárs esetén a küldő partner nevét,
c) a belépés idejét,
d) a kilépés idejét.

A szerverteremben történő munkavégzés rendje

A szerverteremben csak a folyamatban lévő munkavégzéshez szükséges eszközöket, szerszámokat szabad tartani. A helyiségben tartózkodás ideje alatt az elrendelt munkavégzéstől eltérő tevékenységet folytatni (evés, ivás, stb.) tilos.

A szerverterem más irányú hasznosítása (pl. raktározás, stb.) tilos. Ha olyan tevékenységet kell a szerverteremben végezni, amely veszélyeztetheti az egyes eszközök rendelkezésre állását, akkor a feladat végrehajtását az informatikai igazgatónak engedélyeznie kell.

Az elvégzett tevékenységet (telepítés, konfigurálás, javítás, karbantartás, stb.) minden esetben dokumentálni kell. A dokumentáció tartalmazza:

a) A feladatot végző személy(ek) nevét,
b) A tevékenység leírását,
c) A tevékenység időtartamát.

A dokumentáció lehet azonos a szervernaplóval.

XXVI. A BESZERZÉSI FOLYAMATRA VONATKOZÓ BIZTONSÁGI ELŐÍRÁSOK

1.1 Eszközök beszerzése

A beszerzésekre vonatkozó felhasználói és egyéb rendszerbővítési igényeket az informatikai igazgató specifikálja, melynek során figyelembe veszi:

a) A MATE intézményeire vonatkozó közbeszerzési eljárás lefolytatására vonatkozó előírásokat.
b) A MATE intézményei által alkalmazható speciális szoftverlicencezési lehetőségeket.
c) A MATE teljes informatikai rendszerére vonatkozó informatikai fejlesztési és bővítési terveket, a homogén rendszer kialakítására és megtartására irányuló előírásokat és standardokat valamint az információbiztonsági követelményeket.
d) Az adott piaci kínálatot.

Az eszközök (hardver, szoftver) kiválasztásánál a fentiekben részletezett általános és gazdasági tényezők mellett figyelembe kell venni az adott eszköz által nyújtott biztonsági funkciókat, megoldásokat is.

A hardver eszközök beszerzéséhez még az alábbi tényezők figyelembevétele szükséges:

a) A hardver funkcionalitása, erőforrásai
b) A hardver várható rendelkezésre állása (megbízhatóság)
c) A hardver garanciális feltételei (garancia idő, tartalom)
d) A hardver szakértői és technikai támogatottsága (tanácsadás, alkatrész biztosítás)
e) Támogatja-e a hardver a MATE homogenitási és standardizálási törekvéseit

A szoftver megoldásoknál még az alábbi tényezők figyelembevétele szükséges:

a) A szoftver funkcionalitása
b) Illeszkedés a platform szabványokhoz (kompatibilitás)
c) Támogatja-e a szoftver a MATE homogenitási és standardizálási törekvéseit
d) A szoftver biztonsági megoldásai (jogosultság kezelés, titkosítás, LDAP/AD integrálhatóság, stb.)
e) A szoftver menedzselhetősége
f) A szoftverhez biztosított szupport és rendelkezésre állás
g) az életciklus alatti biztonsági frissítések elérhetősége (ha nem frissíthető, nem üzemeltethető)

A teljes beszerzési folyamatot, feladatokat, és felelősségeket a ***MATE Gazdálkodási Szabályzata*** rögzíti.

1.2 Az eszközök átvételével kapcsolatos előírások

A beszerzett eszközöket a beszállítás után ellenőrizni kell, hogy mennyiségre és minőségre azonos-e a megrendelésen szereplő tételekkel, illetve meg kell győződni arról, hogy a beszállított eszközök sértetlenek-e (nincs-e a szállításból adódó fizikai sérülés).

A szállítólevelet vagy az átadás-átvételi dokumentumot csak akkor szabad aláírni, ha a fenti ellenőrzés során nem merült fel mennyiségi, minőségi vagy más kifogás.

Szolgáltatások minőségének ellenőrzése

A szolgáltatások minőségének ellenőrzésére szolgáltatásonként kontrollokat kell felállítani. Minimális kontrollok az alábbiak:

a) Szolgáltatás minőségére vonatkozó kontrollok:

   1. A szolgáltatás rendelkezésre állása (PL: Internet esetén kiesett órák száma, vagy a hiba elhárításának megkezdése stb.).
   2. A szolgáltatás minősége (Pl.. Internet esetén sávszélesség, vagy a hiba gyors és szakszerű elhárítása stb.).

b) A szolgáltató megbízhatóságára vonatkozó kontrollok:

   1. A szolgáltató rendelkezésre állása.
   2. A szolgáltató együttműködési készsége.
   3. A szolgáltató szakmai kompetenciája.

A szolgáltatások minőségének ellenőrzését az informatikai igazgatóság munkatársa végzi.

Szerződésekre, dokumentumokra vonatkozó előírások

A beszállítói szerződésekre vonatkozó előírások

A beszállító szerződésekben az alábbiak szerint kell érvényesíteni a biztonsági szabályokat:

a) A beszállítónak titoktartási nyilatkozatot kell tennie a szerződésben, vagy különálló dokumentumban, amelyben a beszállító felelősséget vállal arra, hogy az általa szállított megoldásokról, illetve a MATE-ról tudomására jutott egyéb információkról nem ad tájékoztatást harmadik félnek.
b) A beszállítói szerződésekben meg kell határozni a garancia és a szupport pontos tartalmát, és idejét. Szükség esetén ki kell térni a szellemi tulajdonjogok tisztázására.

A szolgáltatói szerződésekre vonatkozó előírások

A szolgáltatói szerződésekben az alábbiak szerint kell érvényesíteni a biztonsági szabályokat:

A beszállítónak kollektív titoktartási nyilatkozatot kell tennie a szerződésben, vagy különálló dokumentumban, amelyben a beszállító felelősséget vállal arra, hogy az általa szállított megoldásokról, illetve a MATE-ről tudomására jutott egyéb információkról nem ad tájékoztatást harmadik félnek.

Igény esetén a szolgáltatói szerződésekben meg kell határozni a hozzáférések követelményeit, valamint a szolgáltató részére bocsátott erőforrások körét. Ebben az esetben a külső szolgáltatókra vonatkozó biztonsági szabályokat a munka megkezdése előtt meg kell ismertetni a szolgáltatóval.

Meg kell határozni az incidensek bejelentésével, kezelésével kapcsolatos elvárásokat

A szolgáltatói szerződésekben meg kell határozni a szolgáltatói fél rendelkezésre állásának követelményeit, illetve a szolgáltatás tárgyát képező eszközökkel kapcsolatos rendelkezésre állási követelményeket.

A szolgáltatásokkal kapcsolatos rendelkezésre állási előírásoknak követnie kell a MATE teljes informatikai rendszerére vonatkozó, az egységes üzemvitel kialakítására és megtartására irányuló előírásokat és standardokat valamint az információbiztonsági követelményeket.

A dokumentumokkal kapcsolatos követelmények

A beszerzések során, az alábbi dokumentációk átadását kell a beszállítóktól, illetve a szolgáltatóktól megkövetelni:

a) Titoktartási nyilatkozat: a beszállítást, illetve szolgáltatást végző alkalmazottaktól
b) A beszállítás tárgyát képező eszköz eredeti gyártói specifikációkat és licenceket, felhasználói segédleteit, üzemeltetési és üzembe helyezési (installációs) dokumentumokat.
c) A szolgáltatással kapcsolatos elvégzett feladatokról (javítás, karbantartás stb.) munkalap.

XXVII. AZ ÜZEMELTETÉSHEZ KAPCSOLÓDÓ VÉDELMI INTÉZKEDÉSEK

1.1 Az üzemeltetési folyamathoz tartozó biztonsági előírások

Az üzemeltetési folyamatokhoz ki kell alakítani a tevékenység-felelősség mátrixot, amelyben az alábbi felelősségeket kell megállapítani:

a) Döntési felelősség
b) Koordinálási / felügyeleti felelősség
c) Végrehajtási felelősség
d) Ellenőrzési felelősség

A feladatkörök leosztásánál lehetőség szerint biztosítani kell, hogy az adott feladat végrehajtását, és ellenőrzését ne végezze ugyanaz a személy.

Az informatikai rendszer, vagy rendszerelemek változása (verzióváltás, frissítések) csak előzetesen sikeres tesztelés után történhet meg. Abban az esetben, amikor tartalékeszköz nem áll rendelkezésre, a visszaállíthatóság érdekében gondoskodni kell a mentésről. Több, azonos funkciót ellátó eszköz vagy eszközcsoport esetében (pl. számítógépes labor) előbb egy tesztcsoporton kell a változtatásokat végrehajtani és csak pozitív teszteredmények esetén szabad csak a változtatásokat a rendszer többi elemén is végrehajtani.

Kritikus eszközöknek tekintjük azokat a kiszolgáló, illetve hálózati aktív eszközöket, amelyek segítségével illetve melyeken keresztül a MATE kifejti informatikát igénybe vevő, normál ügyviteli, oktatási, kutatási és egyéb feladataihoz kötődő folyamatait.

A kritikus eszközökön történő változás esetén, amely veszélyeztetheti az eszköz rendelkezésre állását, a változás előtt mentést kell végrehajtani a visszaállíthatóság érdekében. A javítási, karbantartási és szolgáltatási szerződésekben az eszközök által kezelt adatok rendelkezésre állási követelményeihez igazodó rendelkezésre állási időket kell érvényesíteni.

Az informatikai rendszert folyamatosan monitorozni kell. A monitorozás eredményéből, valamint az incidensek kezeléséből származó információkból statisztikákat, kimutatásokat kell készíteni, hogy a rendszerek megbízhatósága, rendelkezésre állása mérhető legyen.

XXVIII. INFRAS81.oTRUKTURÁLIS RENDSZERFEJLESZTÉSEKKEL KAPCSOLATOS KÖVETELMÉNYEK

1.1 Szakmai követelmények meghatározása

A MATE-on belül egységes fejlesztési tervet kell kidolgozni, amely meghatározza az egységes és homogén infrastruktúra kialakításának alapelveit és standardizálja az alkalmazott hardver és szoftver eszközök körét, típusait és ezek jellemző paramétereit. Az egységes fejlesztési terv kidolgozásáról a MATE Informatikai Bizottsága (IB) dönt.

Az infrastrukturális rendszerfejlesztések tervezésekor az alábbi szempontokat kell figyelembe venni:

a) A rendszerek egységesítése, funkcionalitása, platformfüggősége, illetve annak homogenitása.
b) A rendszer teljesítmény, és kapacitás adatai.
c) A rendszer biztonsági megoldásai (pl.: jogosultság kezelés, titkosítás, stb.).
d) Alkalmazott szabványok, interfészek.
e) A rendszer (központi) menedzselhetősége.
f) A rendszerhez nyújtott garanciák, és szupport tevékenységek.
g) A megoldást szállító cég referenciái.

A rendszer tervezésének és bevezetésének folyamatát az adatvédelmi tisztviselőnek végig kell kísérni. A fejlesztéssel kapcsolatos szerződéseket az adatvédelmi tisztviselőnek véleményezni szükséges.

Infrastrukturális fejlesztéssel kapcsolatos szerződések tartalmi követelményei

Az infrastrukturális rendszerfejlesztésekkel kapcsolatos szerződések tartalmazzák az alábbi követelményeket:

a) A vállalkozóval szemben támasztott titoktartási követelményeket.
b) A rendszerrel kapcsolatos garanciális-, és szupport-megegyezéseket.
c) Az rendszerrel átadandó dokumentumok listáját, és azok tartalmával kapcsolatos esetleges követelményeket.

XXIX. DOKUMENTÁCIÓVAL KAPCSOLATOS KÖVETELMÉNYEK

Az infrastrukturális rendszerfejlesztések alkalmával az üzembeállítás előtt az alábbi dokumentációkat kell elkészíteni:

a) **Rendszerterv**, amely tartalmazza:

1. A bevezetésre kerülő rendszer leírását, funkcióit.
2. A bevezetésre kerülő rendszer logikai, és fizikai moduljainak funkcionális felépítését, leírását.
3. A bevezetésre kerülő rendszer illeszkedését a jelenlegi rendszerhez, az alkalmazott interfészek, szabványok leírását.

b) **Üzemeltetési és karbantartási utasítás**, amely tartalmazza:

1. A rendszer elhelyezésével kapcsolatos követelményeket.
2. A rendszer üzemelési paramétereinek leírását (áramellátás, hőmérséklet stb.).
3. A rendszer installálásával kapcsolatos instrukciókat.

4. A rendszer karbantartásával kapcsolatos követelményeket.
5. Hibajelzési és javítási alapinstrukciókat.

XXX. A NEM KÍVÁNT PROGRAMOK (VÍRUS, SPAM, SPYWARE, STB.) ELLENI VÉDELEM

1.1 Rosszindulatú programok elleni védekezés alapjai

Vírusvédelmi események

A fertőzés nagyságától függően az alábbi területeket különböztetjük meg:

a) **Elszigetelt:** ha a MATE területén, 24 órán belül legfeljebb 2-3, egy intézményben legfeljebb 12 fertőzés fordul elő, és egy védendő eszközön sem ismétlődött meg a fertőzés.
b) **Ismétlődő:** ha egy bizonyos eszköz egy nap többször, vagy több egymás utáni napon, hasonló módon megfertőződik.
c) **Sorozatos:** ha 24 órán belül a MATE területén 10-20, egy intézményen belül 5-10 fertőzés történt.
d) **Tömeges:** fentieknél nagyobb 24 órán belüli fertőzésszám.
e) Fertőzés az is, amit nem a vírusvédelmi eszközök jeleznek, hanem ami a felhasználók és rendszergazdák jelzései alapján valószínűsíthető.

Események szintjei:

1. **szintű vírusvédelmi eseménynek** minősül, ha a víruskereső elszigetelt fertőzést észlelt, és az előírt vírusmentesítést elvégezte.
2. **szintű vírusvédelmi eseménynek** minősülnek a következők:
   a) A vírusvédelem elszigetelt fertőzést észlel, de nem tudja a vírusmentesítést elvégezni.
   b) A vírusvédelem sorozatos vagy ismétlődő vírust észlelt, és a vírusmentesítést elvégezte.
   c) A vírusvédelmi menedzsment alkalmazás azt észleli, hogy valamelyik kiemelt eszközön nem fut a vírusvédelem.
   d) A vírusvédelmi menedzsment alkalmazás azt észleli, hogy valamelyik munkaállomáson 2 napja nem fut a vírusvédelem.
   e) A vírusvédelmi eszköz jelzi, hogy egy számítógépen 5 napnál régebbi a szignatúra. Kivételt képez az az eset, amikor a menedzsmentfelület a saját adatbázisa alapján azért mutat régi szignatúrákat, mert az adott számítógép több napja nincs bekapcsolva vagy nem elérhető, illetve már nem a hálózat része.
   f) A központi vírusvédelmi eszközök valamelyikének 1 napnál hosszabb üzemképtelensége.
   g) Itt fel nem sorolt egyéb esetek, amikor a vírusvédelmi rendszerbe bármi okból illetéktelenül beavatkoznak.
3. **szintű vírusvédelmi eseménynek** (vírusriadó) minősül:
   a) Tömeges vírusfertőzés
   b) Sikertelen vírusmentesítés sorozatos vagy ismétlődő fertőzés esetén.

A valós idejű védelem kialakítása

A MATE-nél a védendő eszközök hatékony védelmének érdekében valós idejű védelmet kell kialakítani.

A szervereken és munkaállomásokon a valós idejű védelemnek folyamatosan bekapcsolva kell lennie, hogy biztosítsa a felhasználói munka során igénybe vett állományok (adatok, programok) használat előtti vírusellenőrzését. Olyan központi kliens szerver megoldáson alapuló megoldást kell alkalmazni, mely automatikusan ellenőrzi:

a) A teljes lokális és távoli fájlrendszert.
b) A hálózati (vezetékes és vezeték nélküli) kapcsolatokat.
c) Az adatbeviteli perifériákat (floppy, USB tárolók, CD és DVD meghajtók).
d) Levelezési rendszer.

Biztosítani kell, hogy a munkaállomásokon a valós idejű védelmet a felhasználók ne tudják kikapcsolni.

Amennyiben a valós idejű védelem a detektált vírus eltávolítására nem képes, a vírusvédelmi rendszer automatikus értesítést küld a felhasználó és az informatikai igazgatóság munkatársa számára, és a fertőzés gyanús állományt a rendszer automatikusan karanténba helyezi.

A vírusfertőzésről vagy annak gyanújáról a felhasználó köteles értesíteni a helyi rendszergazdát.

Manuálisan indított / időzített teljes fájlrendszer átvizsgálása

A védendő kiszolgáló eszközökön a teljes állományrendszer vírusellenőrzését legalább heti egy alkalommal végre kell hajtani. A vírusellenőrzést ütemezve minden szerveren el kell indítani.

A helyi vírusvédelmi eszközöknél biztosítani kell, hogy a felhasználók a távolról indított vagy ütemezett feladatokat ne tudják leállítani vagy megváltoztatni.

A munkaállomásokon talált vírusgyanú esetén a teljes fájlrendszer ellenőrzésének elindítása kötelező. A teljes fájlrendszer átvizsgálásának manuális elindítása az informatikai igazgatóság munkatársa feladata.

Szükség esetén a manuális átvizsgálás történhet a telepített vírusvédelmi eszközöktől független, hiteles forrásból származó, jogtiszta vírusvédelmi keresőprogramok segítségével is).

A vírusveszély csökkentésének hardveres és szoftveres lehetőségei

Egyéb hálózati eszközök alkalmazása a vírusvédelemben

A MATE-nál a vírusfertőzés veszélyének csökkentése érdekében ki kell használni azokat a rendelkezésre álló technikai eszközöket, amelyek nem vírusvédelmi feladatokat látnak el, de egyes funkcióik alkalmas a vírusok elleni védekezésre, mint például:

a) A hálózati aktív eszközök nem használt – fizikai és szoftveres – portok letiltása.
b) A tartalomszűrő eszközökkel letöltések vagy levélben való küldésének blokkolása (vírusok jellemző karakter sorozatainak kiszűrése, veszélyes fájltípusok tiltása: .exe, .bat, .com stb.).
c) Amennyiben a hálózati eszköz műszakilag alkalmas ott hálózat vezérelt hozzáférést kell alkalmazni minden más esetben határvédelmi tűzfalakon a nem használt illetve nem támogatott protokollok és szoftver portok letiltása.
d) Szervereken a nem használt applikációk és szervizek leállítása, eltávolítása.
e) Szervereken kizárólag a működésükhöz és üzemeltetésükhöz szükséges programok telepítése.

Korlátozások operációs rendszer szinten

A vírusvédelmi kockázatok csökkentése érdekében lehetőség szerint az operációs rendszerek szintjén korlátozásokat kell bevezetni. A korlátozások terjedjenek ki az alábbiakra:

a) A munkaállomásokon és szervereken meg kell akadályozni a nem használt távdiagnosztikai portok, távoli hozzáférést biztosító szolgáltatások elérését.
b) A munkaállomásokon és szervereken meg kell akadályozni a nem használt szervizek, beépített alkalmazások hozzáférését.

A korlátozásokat a telepítő image-ben, illetve a csoportos és helyi házirendben is alkalmazni kell.

Szoftverek biztonsági frissítése

A vírusfertőzések kockázatainak csökkentése érdekében a MATE-nál központilag menedzselt szervert kell üzemeltetni a Microsoft rendszerek automatikus biztonsági frissítésére. Továbbá biztosítani kell a többi alkalmazott szoftver folyamatos biztonsági frissítését is. A frissítéseket úgy kell ütemezni, hogy egy sérülékenység nyilvánosságra hozatala és a biztonsági frissítése között a legkevesebb idő teljen el.

A szoftverek beszerzése esetében kötött szerződésekben ki kell térni a szoftver biztonsági frissítéseiről szóló utógondozási feladatokra.

Vírusvédelmi szignatúrák frissítése

A vírusvédelmi eszközök vírusadatbázis (szignatúra) elosztása három szinten, automatikusan történik:

Felső szint: központi CMS (Central Manager System)

A vírusvédelmi eszközök műszaki dokumentációjában rögzített időpontokban (de legalább naponta) Internetről frissíti a vírusadatbázist a szoftver gyártója által leírt módon, elérhetővé teszi azokat más számítógépek számára és/vagy átmásolja a másodlagos vírusvédelmi szerverekre.

Második szint: Területi CMS (Central Manager System)

A szignatúra frissítésével kapcsolatos hálózati terhelés csökkentését szolgálják. A lokális vírusvédelmi szerverek az elsődleges központi vírusvédelmi szerverről frissítik az adatbázisukat. A frissítés az eszközök műszaki dokumentációjában rögzített időpontokban (de legalább naponta) történik.

Alsó szint: a védendő eszközök, ezek lehetnek munkaállomások és szerverek

A MATE munkaállomásai, szerverei, amelyeken vírusvédelmi szoftver üzemel. A lokális vírusvédelmi szerverről frissítik az adatbázisukat.

Előírások felhasználók részére a vírusveszély csökkentésére

Általános előírások

A felhasználóknak tilos a munkaállomásukon, hordozható számítógépükön alkalmazott vírusvédelmi szoftver aktív védelmének kikapcsolás, vagy a védelmi beállításának megváltoztatása. A szerverekhez tilos nem MATE tulajdonú perifériát csatlakoztatni.

A vírusvédelem humán kockázatainak csökkentése érdekében a felhasználóknak a jogviszony létrejöttekor meg kell ismernie a MATE vírusvédelmi szabályait, ennek tudomásul vételét dokumentálni kell.

Internet használata

Tilos az ügyvitellel és az oktatási, kutatási feladatokkal össze nem függő fájlok megnyitása, letöltése az Internetről.

1.5.3 Adathordozók kezelése

A szerverek és munkaállomások adatmeghajtó eszközeibe illetve csatlakozó felületeihez tilos ismeretlen eredetű vagy nem biztonságos adathordozót behelyezni (CD, DVD) vagy csatlakoztatni (pendrive, memóriakártya olvasó).

Vírusvédelmi incidensek jelentése

A felhasználóknak jelenteniük kell a rendszergazdának a normális működéstől eltérő eseményeket. Vírusvédelmi incidens esetén a felhasználónak az informatikai igazgatóság munkatársa útmutatásai szerint kell eljárnia.

A vírusvédelemi felelősségek, feladatok

A MATE-nál a vírusvédelmet egységesen kell kezelni. A vírusvédelmi feladatok végrehajtása kétszintű:

Felső szint: informatikai igazgatóság

Háttérfeladatok

a) Rendszeresen felülvizsgálja jelen vírusvédelmi folyamatot, szükség esetén módosítja azt.
b) Elkészíti a vírusvédelmi rendszer műszaki dokumentációját, szükség esetén elvégzi a szükséges módosításokat.
c) Részt vesz a vírusvédelmi eszközök kiválasztásában, felügyeli azok rendszeresítését, és telepítését.
d) Részt vesz a vírusvédelemmel kapcsolatos oktatási és tudatosítási feladatok szervezésében, és lebonyolításában.

Védelmi feladatok

a) Folyamatosan ellenőrzi a vírusvédelmi folyamatok betartását, szükség esetén javaslatot tesz a hiányosságok megszüntetésére, vagy felelősségre vonás kezdeményezésére.
b) Jóváhagyja a vírusvédelmi eszközök Vírusvédelmi szakértő által meghatározott beállításait.
c) Rendszeresen értékeli a vírusvédelmi események emlékeztetőit, szükség esetén javaslatot tesz fegyelmi vizsgálat lefolytatására.
d) Felügyeli a vírusvédelmi eszközök működőképességét.

Feladatok sorozatos vagy tömeges vírusfertőzés esetén

a) Információkat gyűjt a vírusfertőzés főbb jellemzőiről (fertőzés módja, mértéke, stb.).
b) Meghatározza a vírusmentesítéshez szükséges mentesítési eljárásokat, megbecsüli azok erőforrásigényét, idejét.
c) Felügyeli a vírusmentesítés folyamatát, szükség esetén kapcsolatot tart fenn a vírusvédelmi cégek tanácsadóival.
d) Folyamatosan tájékoztatja a szervezeti egységek vezetőit.
e) Felügyeli a visszaállítás folyamatát.
f) Kivizsgálja a fertőzés okait, szükség esetén javaslatokat tesz a vírusvédelmi rendszer módosításaira, illetve a fegyelmi eljárások végrehajtására.

Technikai szint: informatikai igazgatóság munkatársa

Háttérfeladatok

a) Folyamatosan tájékozódik az újabb vírusfenyegetettségekről, és vírusvédelmi eszközökről.
b) Rendszeresen felülvizsgálja a vírusvédelmi eszközök beállításait, szükség esetén javaslatokat tesz azok módosítására.
c) Elvégzi a vírusvédelmi eszközök rezidens keresési, időzített keresési, frissítési, és riasztási beállításait.
d) Végrehajtja a vírusvédelmi eszközök telepítését, végrehajtja a jóváhagyott és standardizált beállításokat.
e) Tájékoztatás vagy oktatás tart a felhasználóknak a vírusvédelemről.
f) Tartja a szakmai kapcsolatot a vírusvédelmi szoftverek szállítójával. Ha indokoltnak látja, tanfolyam elvégzését javasolja a vírusvédelemben résztvevő szereplőknek.
g) Tervezi és nyomon követi vírusvédelmi eszközök optimális életciklusát, szükség esetén javaslatokat tesz az eszközök fejlesztésére, cseréjére.

Védelmi feladatok

a) Megoldja a vírusvédelemben előforduló váratlan vagy tisztázatlan technikai problémákat. Együttműködik az adatvédelmi tisztviselővel azoknak a vírusforrások minimalizálására, amelyek többször is fertőzést okoztak, vagy okozhatnak.
b) Szükség esetén az Internetről előírt rendszerességgel letölti a vírusszignatúrákat a kijelölt tároló helyre.
c) 2. szintű vírusvédelmi eseménykor indokolt esetben, 3. szintű eseménykor minden esetben végrehajtja a vírusmentesítést.
d) Rendszeresen, de legalább hetente minden védendő eszközön ellenőrzi vírusvédelem működőképességét, illetve a vírusszignatúrák frissességék.
e) 1. szintű eseménynél kivizsgálja a vírus eredetét, és amennyiben lehetséges, akkor végrehajtja a vírusmentesítést. Amennyiben a fertőzést emberi mulasztás okozta, vagy a jelenséget trójai vagy kémprogram okozta, azt jelenti az adatvédelmi tisztviselőnek.
f) A 2. vagy magasabb szintű eseményekről emlékeztetőt készít, mely tartalmazza
    1. az esemény fajtáját,
    2. az elhárítással foglalkozók nevét,
    3. az érintett eszközöket,
    4. az esemény észlelésének és az elhárítás befejezésének az idejét,
    5. az esemény valószínű okát.

Feladatok sorozatos vagy tömeges vírusfertőzés esetén

a) Végzi a vírus szignatúrák soron kívüli frissítését.
b) Végzi a fertőzött rendszerek vírusmentesítését.
c) Közreműködik a visszaállításánál.
d) A visszaállítás után a kivizsgálja a fertőzés okát, lokalizálja annak forrását, majd jelenti az adatvédelmi tisztviselőnek.

A vírusvédelemi eszközök üzemeltetése

A vírusvédelmi eszközök üzemeltetéséért a MATE informatikai igazgatóság, illetve informatikai igazgatóság munkatársai a felelősök. Az üzemeltetési feladatokat a következő pontok figyelembe vételével kell végrehajtani a MATE vírusvédelmi szabályzata szerint.

A vírusvédelmi eszközök javítása

Meghibásodott központi vírusvédelmi eszközök javítása idejére, a rendelkezésre álló tartalék vagy a javítást végző szakszerviz által biztosított egyéb vírusvédelmi eszközzel meg kell oldani a helyettesítést. Ellenkező esetben az adott szolgáltatást (Internet, E-mail) a javítás idejére szüneteltetni kell.

A vírusvédelmi eszközök karbantartása

A vírusvédelmi eszközök karbantartását (pl.: frissítések), amennyiben lehetséges úgy kell elvégezni, hogy a vírusvédelmi eszköz működőképessége biztosítható legyen. A verzióváltásokat munkaidőn kívül célszerű végrehajtani.

A vírusvédelmi eszközök mentése

A vírusvédelmi eszközöket rendszeresen menteni kell annak érdekében, hogy:

a) Szükség esetén a vírusvédelmi képesség visszaállítható legyen,
b) A vírusvédelmi eszközök által jelentett vírusvédelmi incidensek visszakereshetők legyenek.

Ellenőrzés

Minden három hónapban az informatikai igazgatóság kijelölt munkatársa kötelessége vírus statisztikákat elkészíteni és az informatikai igazgató részére eljuttatni. Az informatikai Igazgató kötelessége, hogy háromhavonta feldolgozza a kapott statisztikát meghatározva:

a) a vírusvédelmi eszközök által felismert és sikeresen elhárított vírustámadásokat,
b) a vírusvédelmi eszközök által felismert és sikeresen elhárított, de további emberi beavatkozást kívánó vírustámadásokat,
c) a vírusvédelmi eszközök által felismert, de el nem hárított támadásokat,
d) a vírusadatbázis frissítésekkel kapcsolatos riasztásokat szerverenként, a vírustámadások eloszlását, campus/telephelyek, vírusfajták szerint.

XXXI. A JOGOSULTSÁGI RENDSZER ELŐÍRÁSAI

1.1 A hozzáférési rendszer kialakítása

A hozzáférés követelményrendszere

A MATE-nál a hozzáférési jogosultságok kialakítását szabályozó követelmények a következők:

A hozzáférési jogosultságokat az adatcsoportok osztályozásával összhangban kell megállapítani.

a) A MATE informatikai rendszereit csak authentikációs és authorizációs címtáron keresztül lehet elérni.
b) Az optimális hozzáférési rendszer kialakításához minél kevesebb, a feladathoz kapcsolódóan minimális jogokkal rendelkező felhasználói csoport kialakítása szükséges. A csoportok kialakítását a MATE szervezeti felépítéshez és kutatási tevékenységéhez igazodva kell elvégezni. A csoportokhoz rendelt jogosultságoknak összhangban kell lenniük a csoport tagjai által kezelt adatok osztályozásával.
c) A felhasználói csoportok jogosultsági körét az általuk végzett feladatokhoz képest úgy kell minimalizálni, hogy a felhasználónak csak a munkaköri feladataik elvégzéséhez szükséges minimális hozzáférési jogok álljanak rendelkezésre.
d) A felhasználókat minden általuk használt rendszerben egyedileg azonosítani kell, és informálni kell őket az illető rendszerben fennálló korlátozásokról.
e) A felhasználók azonosítását egyedi, titkos információval kell hitelesíteni (felhasználói azonosító és jelszó).
f) A jogosultsági rendszer kialakításánál figyelembe kell venni a védelemre vonatkozó szerződésszerű kötelezettségeket, melyben az adatokhoz, vagy alkalmazásukhoz való hozzáférésről esik szó.
g) Egyedi, személyre szóló hozzáférési jogokat kell alkalmazni, a felhasználói azonosítókat nem lehet megosztani a felhasználók között.
h) Ideiglenes jogok meghatározása külső személyek számára csak a tevékenységükhöz szükséges mértékben történhet, kizárólag korlátozott időtartamig aktiválható, a szerződésükben meghatározott rendszerekhez. Ennek hiányában külső személynek hozzáférés nem adható a MATE informatikai rendszereihez. A munkajogviszony megszűnését követően vagy a munkavégzés alóli mentesítés kezdetétől, amennyiben a munkáltatós és a közalkalmazott úgy állapodnak meg, hogy a mentesítési idő egy időtartamban és nem megosztva kerül kiadásra, vagy az előre meghatározott időtartam lejárta után a jogokat inaktiválni kell.

A követelményrendszert évente felül kell vizsgálni, és javított formában az informatikai igazgatóság munkatársa számára át kell adni. A felülvizsgálatot az adatvédelmi tisztviselő végzi.

A hozzáférési rendszer kialakításának részfeladatai

A hozzáférési jogosultságok kialakításának részfeladatai a következők:

a) a tárolt adatok különböző szervereken és ezeken belül különböző megosztásokba való csoportosítása,
b) a tárolt adatok besorolása biztonsági szempontból,
c) felhasználói csoportok definiálása,
d) az egyes megosztások és az azokon belül található almappákhoz és adatokhoz történő csoportok és azok jogosultságainak hozzárendelése,

e) az informatikai igazgatóság munkatársak feladat megosztási rendszerének és az ennek megfelelő hozzáférési jogainak kidolgozása,
f) a hozzáférés nyilvántartásának kialakítása és folyamatos karbantartása.

Felhasználói csoportok létrehozása

A MATE egyes szervezeti egységeinél használatos munkakörök (felhasználói csoportok) kialakítása:

a) Az adott alkalmazás vagy szervezeti egység adatgazdája meghatározza az adott alkalmazást, illetve központi erőforrást használók általános és speciális felhasználói csoportjait.
b) A MATE adott szervezete nyilvántartja, és az informatikai igazgatóság számára átadja az aktuális felhasználói csoport listát.

Jogosultságok felhasználói csoporthoz rendelése

A MATE egyes szervezeti egységeinél használatos informatikai alkalmazások által létrehozott, illetve kezelt biztonsági szempontok szerint besorolt és rendszerekhez hozzárendelt adatok felhasználói csoporthoz rendelése.

a) A hozzárendelés során egy adathoz több felhasználói csoport is rendelhető.
b) A hozzárendelés során egy felhasználói csoporthoz több jogosultság is rendelhető.

Hozzáférési jogosultságok nyilvántartása

A MATE dolgozói számára a rendszerhez való hozzáférési jogosultságot elektronikus vagy papír alapon, a MATE iktatási és dokumentumkezelő rendszerében rögzítetten, munkáltatói jóváhagyás mellett kell igényelni.

A központi jogosultságigénylés menete a következő:

1. A központi rendszerekhez jogosultságot az Intraneten **elérhető Jogosultságigénylő lapon** lehet igényelni. A munkavállaló részére a közvetlen felettese igényli a hozzáférést, az érintett rendszer adatgazdájától. A különböző rendszerek adatgazdái, illetve az ő elérhetőségeik szintén az Intraneten tekinthetőek meg. Az igény elbírálása (szükség szerint a jogosultsági szint módosítása) után a jóváhagyott igénylést az adatgazda továbbítja beállításra az informatikai igazgatóság munkatársához.
2. A jogosultságokat úgy kell meghatározni, hogy a felhasználó minden, a munkájához szükséges, és csak a szükséges adatokhoz, funkciókhoz férjen hozzá.
3. **Nem a szabályozott csatornán és formában érkező igényeket az informatikai igazgatóság nem hajthatja végre.**

Az intézeti üzemeltetésben lévő szolgáltatásokhoz jogosultságok igénylése az érintett intézet igazgatón keresztül történik.

Felhasználói jogosultságok aktiválása, inaktiválása

a) Új munkatárs hozzáférési rendszerbe való illesztését, vagy jogosultsággal rendelkező munkatárs jogosultság változási igényét a ***„Jogosultságigénylő lap"*** űrlap kitöltésével és elküldésével, az adott szervezeti egység vezetője írásban (elektronikusan vagy hagyományos módon) igényeli az adott rendszer adatgazdájának való megküldésével. A MATE informatikai rendszeréhez kizárólag olyan munkatárs kaphat hozzáférést, akinek adatai a munkaügyi rendszerében rögzítésre kerültek, emellett a MATE-kal érvényes munkaviszonnyal rendelkezik.

A jóváhagyott ***Jogosultságigénylő lapot*** a Humánpolitikai Osztály HelpDesken keresztül megküldi az informatikai igazgatóság részére és ez alapján a jogosultság aktiválása megtörténik.
Az applikációkban a jogosultság kiosztásáról az adatgazdának kell értesíteni az adott applikáció alkalmazásgazdáját.

b) Minden felhasználó definiálásánál biztosítani kell az 1 természetes személy = 1 felhasználói azonosító, egy-egy értelmű megfeleltetést, azaz nem lehet közösen használt felhasználói azonosító.

c) Az alkalmazotti jogviszony megszűnésének, megszüntetésének esetében a felhasználói hozzáférés zárolása automatikusan történik az alkalmazott kilépésekor. Ennek biztosítására:

   1. Azonnali felmondás esetén, illetve ha a kilépő alkalmazott vezetője úgy ítéli meg, a jogosultság azonnal visszavonásra kerül. A kilépő alkalmazott vezetője ebben az esetben értesíti a HelpDesket. A telefonos vagy szóbeli értesítést írott formában (e-mail vagy papír) is meg kell erősíteni. Az applikációkban a jogosultság megszüntetéséről az adatgazdának kell értesíteni az adott applikáció alkalmazásgazdáját.
   2. Munkaviszony megszűnése esetén a jogosultság visszavonása a **Leszámolási lapon** jelzett dátummal történik meg. Ehhez az informatikai igazgatóságot tájékoztatni kell a munkaviszony megszűnéséről, ezt a Humánpolitikai Osztály a HelpDesken keresztül teszi meg. Az applikációkban a jogosultság megszüntetéséről az adatgazdának kell értesíteni az adott applikáció alkalmazásgazdáját.

d) Alkalmazott esetében az adatvédelmi tisztviselő köteles rendelkezni a felhasználó adatairól, dokumentumairól (archiválás, törlés, 3. személy általi hozzáférhetőség). A felhasználói fiók törlésére az adatok sorsának rendezése után kerülhet sor. A szervezeti egység vezetőjének a szóban forgó adatokkal kapcsolatban rendelkeznie kell arról, hogy az adatokhoz a továbbiakban ki férhet hozzá, illetve archiválni, törölni kell-e az adatokat.

Amennyiben a felhasználó jogviszonyában változások következnek be, de a munkáltatói jogviszony (áthelyezés más osztályra, munkakör vagy munkaköri leírás megváltozása) továbbra is a MATE-hoz köti, a felhasználót a felhasználói és hozzáférési jogosultságokat az új jogviszony szerint (az új jogviszonyhoz tartozó vezető kérelmének megfelelően) kell beállítani.

1.2 JESZÓKEZELÉS

A jelszavas védelem felépítése, fajtái

A MATE informatikai rendszereinek elérésére használható hozzáférés szintjei:

1. **Névre szóló** informatikai igazgatóság munkatársának **hozzáférés** esetén, a jogosítványt az informatikai igazgatóság munkatársa a saját nevére szóló, kizárólagosan általa használt, megfelelő jogkörrel felruházott felhasználói azonosító segítségével lehet használni.
2. **A beépített** (root, administrator, rendszergazda stb.) rendszergazdai accountokat biztonsági okokból el kell távolítani a rendszerből. Bármilyen operációhoz használni ezeket tilos. (Abban a rendszerben, ahol ez nem távolítható el, ott le kell tiltani.) Minden informatikai igazgatóság munkatársnak rendelkeznie kell felhasználói hozzáféréssel is, amelyet egyébként használ.
3. **Speciális esetek** számára (pl., vészhozzáférés) létre lehet hozni a kétemberes szabály alkalmazásával egy rendszergazdai jogosítványt. Egyéb esetben amennyire technikai és egyéb szempontok lehetővé teszik, a csoportos rendszergazdai hozzáférést használni **tilos.**

4. **Névre szóló felhasználói** hozzáférés keretében a felhasználó külön, saját névre szóló, más által nem használt, kizárólag a munkája ellátása miatt elengedhetetlen jogosítványokkal rendelkezik az informatikai és telekommunikációs rendszerekhez és azok erőforrásaihoz, az üzleti folyamatok ellátásához kapcsolódó feladatok elvégzéséhez.
5. **Csoportos felhasználói hozzáférés** keretében több felhasználó azonos, a munkája ellátása miatt elengedhetetlen felhasználói hozzáférést használ az informatikai és telekommunikációs rendszerekhez és azok erőforrásaihoz, az üzleti folyamatok ellátásához kapcsolódó feladatok elvégzéséhez. Amennyire technikai és egyéb szempontok lehetővé teszik, a csoportos felhasználói hozzáférést csak a védelmet nem igénylő adatokat tartalmazó rendszerek esetén szabad alkalmazni, minden más esetben **tilos.** A csoportos felhasználói hozzáférést csak igen különleges és indokolt esetekben szabad csak alkalmazni.

Illetéktelen hozzáférés elleni védelem

Jelszómenedzsment

A kliens gépeken a jogosultság kezelésben a adminisztrátori és kliens jogosultságot szét kell választani, illetve a hozzá tartozó jelszavakat is el kell különíteni.

Tilos a rendszerben a kliens és admin jogosultság összevonása.

Felhasználói hozzáférések

Azon informatikai rendszerek esetén, melyek rendelkeznek a megfelelő technikai feltételekkel, a hitelesítéshez használt felhasználói hozzáféréshez rendelt jelszavaknak az alábbi kritériumoknak kell megfelelni:

a) Az utolsó 3 jelszót nem lehet újra használni.
b) A felhasználói jelszavak minimális hossza 8 karakter, de javasolt a jelszó mondat használata.
c) A felhasználóknak be kell jelentkezni a jelszó megváltoztatásához.
d) A felhasználóknak meg kell változtatniuk a jelszavukat, amikor első alkalommal használják felhasználói azonosítójukat.
e) A rendszer tagadja meg a hozzáférést 6 hibás jelszó megadása után.
f) A hibás próbálkozásokat követően a rendszer 15 percre blokkolja az accountot.
g) Mind a sikeres, mind a sikertelen belépési és kilépési kísérleteket naplózni kell.
h) Hálózatba kötött, vagy bizalmas adatok tárolására használt informatikai eszközök esetében félévente a jelszó változtatása kötelező.
i) Tilos a jelszavak kiírása, kiragasztása a számítógépre vagy környezetében.

A fenti követelményekről minden felhasználót tájékoztatni kell, munkájának megkezdése előtt.

Informatikai igazgatóság munkatársi, alkalmazásgazdai hozzáférések

Azon informatikai rendszerek esetén, melyek rendelkeznek megfelelő technikai megoldásokkal, az azonosításhoz használt **rendszergazdai** hozzáféréshez rendelt jelszavaknak az alábbi kritériumoknak kell megfelelni:

a) A rendszergazdai jelszavak minimális hossza 8 karakter.
b) Az utolsó 4 jelszót nem lehet újra használni.
c) A rendszergazdának be kell jelentkezni a jelszó megváltoztatásához.
d) Szabályozni és szűrő segítségével biztosítani kell a jelszavak összetettségét: szükséges nagybetűk, kisbetűk, számok és speciális karakterek, vagy jelszó mondat használata.
e) Mind a sikeres, mind a sikertelen belépési és kilépési kísérleteket naplózni kell.

f) Vészhozzáférések: a rendszergazdai hozzáféréseket a rendszerüzemeltetés számára nem ismert tartalommal, kinyomtatott formában, zárt borítékban el kell helyezni a MATE adott szervezetének vezetője által használt tűzálló páncélszekrényben.
g) Félévente a jelszó változtatása kötelező.

A **bejelentkező** névhez tartozó jelszót meg kell változtatni,

a) a felhasználói név rendszerbe történt felvételét követő első bejelentkezéskor,
b) ha a jelszó illetéktelen személy tudomására jutott, vagy bármilyen módon nyilvánosságra került.

A vészhozzáférést biztosító jelszavakat tartalmazó borítékok felbontását a központilag a rektor vagy megbízottja, valamint az informatikai igazgató, intézeti szinten az intézetigazgató/adatvédelmi tisztviselő rendelheti el. A felbontásnál meg kell határozni a felbontás elrendelésének okát, és a felbontás bekövetkeztéről írásos feljegyzést kell készíteni, és értesíteni kell az adatvédelmi tisztviselőt. Az informatikai igazgatóság munkatársa gondoskodik a vészhozzáférést biztosító jelszavak megváltoztatásáról és a zárt boríték páncélszekrénybe történt elhelyezéséről.

Az alkalmazói rendszerekben a jelszavak biztonságos tárolásánál az operációs rendszerek jelszó tárolási elvét kell alapul venni. A felhasználó rendszerek biztonságos jelszó tárolási mechanizmusát, módszerét az informatikai igazgatóság munkatársa ellenőrzi.

Alkalmazotti munkaállomásokra vonatkozó előírások

A munkaállomások monitorait úgy kell elhelyezni, hogy a monitorokon megjelenésre kerülő adatokat illetéktelen személyek ne tudják leolvasni.

„Üres asztal – tiszta képernyő" szabály:

a) A papíranyagokat és adathordozókat zárható szekrényben kell őrizni/tárolni, amikor éppen nincsenek használatban, főként a munkaidőn kívüli időszakban.
b) Amennyiben sajátos az itt meghatározottnál szigorúbb információbiztonsági előírások vannak érvényben egy szervezeti egységnél, akkor a dokumentumokat azon előírások alapján kell tárolni.
c) Munkaállomást csak abban az esetben szabad felügyelet nélkül hagyni, ha a munkaállomáson jelszó védelemmel rendelkező képernyő-védőt alkalmaznak, vagy a munkaállomást zárolják.

„Rendszergazda" jogosultságú felhasználóval csak az ilyen jogosultságú feladat elvégzésének idejére szabad bejelentkezni a munkaállomásra, ezután ki kell vele jelentkezni. A feladat elvégzése alatt a munkaállomást felügyelet nélkül hagyni, vagy a munkaállomáson egyéb tevékenységet folytatni szigorúan tilos.

Jelszókezelés

Minden jelszót úgy kell kialakítani, hogy a magyar 44 betűs ÁBC kis és nagy betűiből álló (legalább egy nagybetűt tartalmazó) esetleg, de nem kötelezően „. ; , : ; –; !; ?; „(pont, vessző, kettőspont; pontos vessző; elválasztó jel, felkiáltó jel, kérdő jel) magába foglaló minimálisan 8 karakterből (space, üres karakterrel együtt) álló jelszót kell megadni.

A beírt jelszó lehet név, vers, film-, könyv cím, dalrészlet stb.), Támogatott a jelszó mondat használata.

A kódszámítás alapja mely indokolja a jelenlegi megoldást

Azonosító	ALAPKÓD készlet		alapjel készlet	KARAKTEREK SZÁMA (Jelszó Hossza)			
				8	9	10	11
			db	Variációk száma			
1	CSAK kis vagy NAGY betű	"1x44"	44	14 048 223 625 216	618 121 839 509 504	27 197 360 938 418 200	1 196 683 881 290 400 000
2	KIS és NAGY BETŰ	"(2x44)"	88	3 596 345 248 055 300	316 478 381 828 866 000	27 850 097 600 940 200 000	2 450 808 588 882 740 000 000
3	KIS és NAGY BETŰ plusz ?,!.	"(2x44)+4"	92	5 132 188 731 375 620	472 161 363 286 557 000	43 438 845 422 363 200 000	3 996 373 778 857 420 000 000
4	kis és Nagy betű plusz decimális számok, plus 15 spec karakter	"(2x44)+10+15"	124	55 895 067 029 733 400	6 930 988 311 686 940 000	859 442 550 649 180 000 000	106 570 876 280 498 000 000 000
	4-azonosítóhoz (8-s hossz) viszonyított 2			4 nyert	2 nyert	JAVASOLTA min 2-s, megfelelő a 3-s	

CSAK eset PÉLDÁK	Ej, mi a kő, tyúkanyó kend	19 betű + 7=26	26
	Dr Nagy szám 517012	19 betű +4=25	25
	Armageddon	10 betű=10	10
	Kedves Mama	10 betű +1=11	11
	Párizsban a Mirabó híd alatt fut a Szajna árja	37 betű +7=44	44
	Hazádnak rendületlenül légy híve, óh, magyar	39 betű +7=46	46
	iU6Wy9zc15	10 vegyes=10	10

Nem javasolt jelszavak példái

A táblázat csak példákat tartalmaz a teljesség igénye nélkül, segédletként a jelszavak képzéséhez!!!

No	Tiltott kód	Jelszó hossz	No	Tiltott kód	Jelszó hossz
1.	123456789	9	14.	Jelszó123	9
2.	9876543210	10	15.	Jelszavam	9
3.	Abcd12345	9	16.	Jelszavaim	10
4.	Abcdefghijkl	12	17.	password1	9
5.	Oiuztrewq	9	18.	000001234	9
6.	Lkjhgfdsa	9	19.	MATE	14
7.	Asdfghjklé	10	20.	Pénzügy12	9
8.	Qwertzuiop	10	21.	Adóosztály	10
9.	Íyxcvbnm,	9	22.	Gazdaságiosztály	16

10.	Mnbvcxy01	9	**23.**	Billentyű	9
11.	Számítógép1	11	**24.**	MATE1234	12
12.	Notebook1	9	**25.**	Linux1234	9
13.	Fecebook1	9	**26.**	MATE12	9
14.	Microsoft	9	**27.**	Jelszó12	9
VALAMINT TILOS:			**Település neve / munkavállalói Családnév és/vagy keresztnév / BELÉPÉSI AZONOSÍTÓ jelszó használata**		

Javasolt (előírt) jelszókezelés

A MATE informatikai rendszereihez való illetéktelen logikai hozzáférés megakadályozására jelszavas védelmet kell alkalmazni.

A MATE informatikai hálózatába, illetve az alkalmazások rendszerébe bejelentkezési névvel (accounttal) rendelkező felhasználó köteles a bejelentkező nevéhez tartozó jelszó megőrzésére. A saját bejelentkező névhez tartozó jelszót elárulni, mások által is elérhető módon feljegyezni tilos.

Bejelentkező névhez tartozó jelszó beállításának megtörténtét és a jelszót a jogosultság kezelő rendszergazda telefonon közölheti abban az esetben, ha

a) új felhasználó felvétele, vagy egyéb ok (pl. elfelejtés) miatt a felhasználó előtt még ismeretlen új belépési jelszót definiált,
b) a beszélgető partner azonosítására az elvárható gondossággal járt el, és
c) figyelmezteti a felhasználót arra, hogy a beszélgetést követő első bejelentkezésekor a rendszer a közölt jelszó megváltoztatására fogja kényszeríteni.

Valamennyi informatikai rendszer esetén a hozzáférésekhez rendelt jelszavaknak, a hozzáférés szintjétől függetlenül az alábbi alapkritériumoknak feleljenek meg:

A jelszókezelés kapcsán előírt a jelszómondat használata.

a) A jelszómondat nem lehet a felhasználó vagy családtagjának a neve.
b) A jelszómondat nem lehet a MATE azonosítója vagy címe.
c) A jelszó mondat minimum 3 (három) szóból kell, hogy álljon.

Javasolt jelszó kialakításra példák:

a) Luke én vagyok az apád
    1. Luke4én4vagyok4az4apád (a bővített számot is tartalmazó verzió. Bármely szám lehet a space helyén)
    2. Luke4én4vagyok4az4apád? (bővített és írásjelet is tartalmazó változat példa)
b) Egyszer volt, hol nem volt. (írásjeleket is tartalmazó jelszó mondat)

Kötelező biztonságos jelszót választani. A jelszó cserénél az új jelszó nem állhat a régivel azonos szavakból. A jelszó mondatok esetében javasolt az ékezetes karakterek használata (magyar ÁBC)

A jelszókezelésben tilos:

a) A jelszavakat a rendszerrel illetve a böngészővel megjegyeztetni (Tilos az alkalmazások, böngészők általi jelszó megjegyzési ajánlatát elfogadni. Kivételt képeznek a már beléptetett rendszerek kommunikációs jelszavait a NISZ, MÁK adatszolgáltató rendszere felé)
b) A jelszavakat a számítógép környeztében, felírva tárolni (monitoron, billentyűzeten, könyöklőn, jegyzetfüzeten, post-it stb.)
c) A jelszavakat elektronikus levélben (e-mail), faxon, levélben, sms-ben elküldeni.
d) A jelszavakat és jelszavas beléptetéseket megkerülni, letiltani (amennyiben erre lehetőség lenne)
e) A jelszavakat másokkal megosztani. (Amennyiben valamilyen okból mégis szükséges lenne és ilyen eseményre elkerülhetetlenül sor kerül, úgy a következő belépésnél a jelszót módosítani kell.)
f) A tiltó táblázatban szereplő kombinációk használata, valamint ezek kiegészített (karakter bővítéssel) felhasználása.
g) A külső (internet felőli) bejelentkezésre használt jelszóval azonos jelszót használni a számítógépre való bejelentkezésre.

A jelszókezelésben kötelező

a) Félévente jelszót változtatni, oly módon hogy az előzővel nem lehet azonos az új jelszó
b) Jelszó kód esetében a minimális 8 karterből 6 karakter cserélendő (pl. nem lehet a Karcsika1 helyett Karcsika2)
c) Jelszó mondat esetében kötelezően cserélendő az első 3 szó (pl. medvecukor gyártó kisiparos helyett nem használható a gumicukor készítő kisiparos, de lehet áfonyalekvár készítő kisiparos, vagy áfonya gyűjtő medve stb.)
d) A képernyővédelmet be kell kapcsolni, ha a felhasználó elhagyja a munkahelyét, a képernyővédelemből való visszatérés esetén a rendszer jelszó használat beállítása kötelező.
e) A számítógéptől való távozás (bekapcsoltan történő otthagyás) esetén a rendszerből történő kijelentkezés.
f) A beállított jelszavakat egy lezárt aláírt borítékban a szervezeti egység vezetőnknél letétbe kell helyezni.
g) A jelszó cserék esetében a korábbi jelszavat tartalmazó borítékot felbontás nélkül a szervezeti egység vezetője papírdarálóban (iratmegsemmisítőben) ledarálja. Az új jelszavakat tartalmazó borítékot biztonságosan elzárja.
h) Minden gyanús jelszó és hozzáférés jogosultság változást vagy eltérést az információbiztonsági felelősnél be kell jelenteni.
i) Négy érvénytelen kísérlet után a rendszer a kísérletezőt 15 percre kizárja a további próbálkozásokból, és írásos jelentést generál az MATE informatikai igazgatóság munkatársa felé.

Felhasználók bejelentkezése

A MATE számítógépes hálózatába és rendszereibe bejelentkezni csak a rendszerben definiált bejelentkező név és a hozzátartozó jelszó ismeretében lehet.

A több felhasználós informatikai rendszerek elérésénél a felhasználók megkülönböztetésére, illetve a bizalmasság és sértetlenség megőrzésére bejelentkezési és kijelentkezési eljárásokat kell definiálni. A bejelentkezési eljárások definiálásánál az alábbi biztonsági követelményeket kell figyelembe venni:

a) Egyéni felhasználói azonosítók használata, amely felhasználóhoz köthető és az ő műveleteiért felelős.

b) Ellenőrizni kell, hogy a felhasználónak van-e engedélye az informatikai rendszer, vagy alkalmazás használatára.
c) A felhasználó a hozzáférési jogairól, annak változásairól kapjon írásos értesítést.
d) A hozzáférés igénylés jóváhagyásáig nem lehet ideiglenes hozzáférést biztosítani.
e) Listát kell tudni készíteni az alkalmazásokat használó regisztrált személyekről (vagy az alkalmazás menüjéből lekérdezhető módon, vagy külön vezetett lista segítségével).
f) Biztosítani kell, hogy a feleslegessé vált felhasználói azonosítók minél hamarabb törlésre kerüljenek, és ne kerüljenek ismét felhasználásra.

Felhasználók logikai hozzáféréssel kapcsolatos kötelességei, felelősségei

A **felhasználóknak** ismerniük kell a jelszavak, illetve a felhasználó kezelésében lévő berendezések használatára vonatkozó előírásokat.

A MATE informatikai rendszerének használatával kapcsolatos felhasználói feladatok:

a) A felhasználói jelszavak titkosan kezelendők.
b) A jelszó elfelejtése esetén a felhasználó az informatikai igazgatóság munkatársától vagy a jogosultság kezelő alkalmazásgazdától igényelhet új jelszót. Az új jelszót az első bejelentkezés alkalmával kötelező megváltoztatni.
c) A jelszó megválasztására vonatkozó szabályokat jelen szabályzat tartalmazza.
d) A jelszót a felhasználó semmilyen körülmények között nem jelenítheti meg a különböző adathordozókon, képernyőn, papíron stb.

Szándékos jogosulatlan hozzáférés kísérlete esetén – a sikerességre vagy sikertelenségre való tekintet nélkül – a felhasználót felelősségre vonás terheli. Minden, az informatikai rendszerek hozzáférésével kapcsolatos visszaélési kísérletet jelenteni kell az adatvédelmi tisztviselőnek.

Felügyelet nélkül hagyott alkalmazotti munkaállomások

Ha a felhasználó szünetelteti a munkaállomáson végzett tevékenységét, ki kell jelentkeznie, *vagy* zárolnia kell a számítógépet, *vagy* automatikus képernyővédőt kell alkalmazni. A rendszernek ez után újra kell indítania az azonosítási és a jogosultság ellenőrzési folyamatot, a felhasználó csak az újbóli bejelentkezés, illetve jelszó megadás után folytathatja a munkát.

A megnyitott alkalmazásokat, a használatot követően a felhasználónak be kell zárnia.

A felügyelet nélkül hagyott felhasználói munkaállomások védelme érdekében a munkaállomások beállításait az informatikai igazgatóság munkatársai végzik. A felhasználóknak tilos az informatikai igazgatóság munkatársa által beállított paraméterek törlése, megváltoztatása.

Belépési kísérletek korlátozása

A felhasználók és rendszergazdák pontos azonosításának megőrzésének érdekében, a felhasználói jelszavak bizalmasságát biztosítani kell. Az azonosításra fennálló 30 perces időtartam túllépése esetén a folyamatot, lehetőség szerint, le kell állítani. Amennyiben technikailag lehetséges, biztosítani kell, hogy felhasználói azonosító hat egymást követő sikertelen bejelentkezési kísérlet után felfüggesztésre kerüljön. A felfüggesztést automatikus módon, 30 perc elteltével a rendszer is visszaállíthatja, illetve az informatikai igazgatóság munkatársai állíthatják vissza a felhasználó személyes kérésére

Az operációs rendszerhez, illetve az alkalmazói rendszerekhez való hozzáférés esetén, ahol lehet, az utolsó sikeresen bejelentkezett felhasználói azonosítónak rejtve kell maradnia.

A hozzáférés ellenőrzése

A MATE jogosultsági rendszerét meghatározott időközönként, de legalább évente felül kell vizsgálni, melynek felelőse az adatvédelmi tisztviselő.

Az ellenőrzések megkezdése előtt információkat kell gyűjteni:

a) az egyes alkalmazások személyes biztonsági követelményeiről,
b) az alkalmazások ki és bemenő adatairól,
c) az adatok bizalmassági/sértetlenségi szintbe sorolásáról, az adott bizalmassági/sértetlenségi szinten meghatározott adatkezelésről,
d) a különböző rendszerek és hálózatok összefüggéseiről,
e) a vonatkozó törvényi, hatósági és szervezeti szabályozásokról, stb.

Az ellenőrzés során felmerülő feladatok:

a) Felülvizsgálni a felhasználók jogosultságait, illetve jogosultság változást előidéző eseményekkor (pl.: a felhasználó kilépésekor, áthelyezésekor, új munkatárs felvételekor). A vizsgálat során figyelni kell arra, hogy a felhasználónak csak olyan alkalmazásokhoz, rendszerekhez legyen hozzáférési joga, amiket valójában használ.
b) Szúrópróbaszerűen ellenőrzi, hogy a jogosultságok adminisztrációja a szabályzatban foglaltak szerint történik-e, a rendszerek felhasználására és az adatok meghatározott mértékű elérésére csak a dokumentációban rögzített személyek jogosultak.
c) A vizsgálat során ki kell térni különös tekintettel a páncélszekrényben tárolt rendszergazdai jelszavak vizsgálatára is. A vizsgálatot végző ellenőr a páncélszekrényben található borítékok felbontása után meggyőződik, hogy az ott tárolt jelszavak használhatóak, valamint gondoskodik arról, hogy a vizsgálat után a rendszergazdai jelszóval rendelkező munkatárs megváltoztassa, és leellenőrzi, hogy ez nem egyezik a vizsgálat elején a borítékban talált jelszóval. A felbontott borítékokat és tartalmukat, a vizsgálatot követően meg kell semmisíteni, és gondoskodnia kell arról, hogy az új jelszó elhelyezésre kerüljön a páncélszekrényben.
d) A feltárt hiányosságokról Megbízókönyvet kell készíteni, és a megfelelő eljárásokról saját hatáskörében intézkedni, valamint szükség esetén hatáskörét meghaladó eljárások megindítását kezdeményezi.

Mentés, archiválás, és visszatöltés

A dokumentum célja, hogy meghatározza a MATE informatikai rendszerén elektronikusan tárolt adatok mentési és archiválási rend alapelveit.

Minden mentésnek a MATE központi vagy campus/telephelyi adathordozóra kell történnie, lokál meghajtóra tilos menteni!

A mentési rend alapelveinek célja, hogy kialakítsa azokat az eljárásokat, feladatokat és felelősségeket, amelyekkel biztosítani lehet az üzleti szempontból „fontos", vagy annál magasabb adatosztályba sorolt adatok előírt rendelkezésre állását.

Felelősségek

Az adatvédelmi tisztviselő elektronikusan tárolt adatok mentésével kapcsolatos feladatai és felelőssége:

a) Felelős a MATE központi, campus/telephelyi illetve az adott intézetének mentési, archiválási rendjének kidolgozásáért.

b) Felelős a mentési, archiválási rend rendszeres ellenőrzéséért.
c) Felelős a mentési rendet érintő változások követéséért, illetve a mentési rendről szóló dokumentációk felülvizsgálatáért.
d) Felelős a mentési feladatokkal megbízott informatikai igazgatóság munkatársa által jelentett incidensek kezelésére vonatkozó intézkedések foganatosításáért, illetve szükség esetén a kezeléshez szükséges erőforrások biztosításáért.
e) Felelős a helyi mentések visszatöltéssel történő ellenőrzéséért.
f) Felelős a helyi archívumban elhelyezett médiák rendszeres ellenőrzéséért.
g) Felelős a helyi mentéssel, archiválással, illetve visszatöltéssel kapcsolatos dokumentálások ellenőrzéséért.

A mentésért felelős informatikai igazgatóság munkatársának felelőssége:

a) Felelős a kezelésére bízott informatikai rendszerben tárolt elektronikus adatok mentésének, archiválásának rendszeres, előírásszerű végrehajtásáért.
b) Felelős a mentések, archiválások végrehajtása során feltárt incidensek jelentéséért, illetve ebben a dokumentumban meghatározott követelmények alapján az incidensek kezeléséért.
c) Felelős a mentések visszatöltéssel történő ellenőrzések végrehajtásáért.
d) Felelős az archívumban elhelyezett médiák rendszeres ellenőrzéséért, időszakonként történő átcsévéléséért, vagy átmásolásáért.
e) Felelős a mentéssel, archiválással, illetve visszatöltéssel kapcsolatos dokumentálások elvégzéséért.

Mentés irányelvei

A mentések megtervezésekor az alábbi szempontokat kell figyelembe venni:

a) Minden olyan adat mentésre kerüljön, amely az adatosztályozás során „fontos", vagy annál magasabb besorolást kapott.
b) Minden mentésnek biztosítani kell az adatok kezeléséhez szükséges szoftverkörnyezet következetes helyreállíthatóságát (operációs rendszer, adatbázis-kezelő, stb.).
c) Minden olyan adat mentésre kerüljön, amely az auditálás, ellenőrzés eszköze lehet (naplófájlok, riportok, stb.).
d) Minden olyan eszköz konfigurációja mentésre kerüljön, amely részt vesz „fontos", vagy annál magasabb besorolású adat kezelésében (tárolásában, továbbításában, stb. pl.: hálózati aktív eszközök).
e) Minden mentés alkalmas legyen olyan környezet helyreállítására, mely lehetővé teszi valamely igazolható állapothoz való visszatérést.
f) A kritikus rendszerek mentése legalább két példányban készüljön, a két példányt elkülönítetten kell tárolni

A mentések tartalma

Szerverek mentése

A szerverek mentését a mentendő eszközök listáját, a mentési eljárást (mentés gyakorisága, típusa) a mentendő állományok specifikációját (image, tároló területek, fájlok, adatbázisok, konfigurációs fájlok, rendszer területek, jelszó fájlok, profil fájlok, stb.) a mentések időpontját és gyakoriságát a ***"Mentési Rend"*** tartalmazza melyet az adatgazda és az informatikai igazgatóság munkatársa közösen készít el.

Adatkommunikációs eszközök mentése

Az adatkommunikációs eszközök mentését az alábbi esetekben kell elvégezni:

a) Új eszköz rendszerbeállítása esetén,
b) Az adatkommunikációs eszközök konfigurációjában történő bármilyen változás esetén.

Félévente egy alkalommal Mentendő állományok: Router, Tűzfal, Switch esetében: az NVRAM-ban található startup-config file.

Az adatkommunikációs eszközök konfigurációit a kijelölt szerveren a rendszergazdai könyvtárba kell lementeni, valamint a lementett konfigurációs fájlok archiválását legalább 6 havonta, a gyors visszaállíthatóság érdekében külső adathordozóra is kell elvégezni.

Az archiválások rendje

Archiválásnak nevezik azt, amikor a rendszerből az adatok kikerülnek és csak az adathordozón léteznek tovább.

Kiszolgálók archiválásának rendje

Archiválást kell biztosítani az alábbi állományikra:

a) Fájlszerveren tárolt fájlok dokumentumok, melyeket régóta nem használnak, jelentős tárterületet foglalnak és a felhasználó, vagy az adatgazda kéri az archiválást.
b) A felhasználók postaládájában található régi levelek, amelyek a méretkorlátozások miatt akadályozzák a kommunikációt, és a felhasználó kéri az archiválást.

Az archiválások által keletkezett adathordozók tárolását jelen szabályzatnak megfelelően kell tárolni, illetve dokumentálni.

Az egyéni archiválások igénylésének rendje

Ha az információk rendelkezésre állási követelményei miatt szükséges, vagy a központi archiválási eljárásban nem szerepel, a felhasználó kérheti adatainak renden kívüli archiválását.

Az archiválási igényeket az informatikai igazgatónak kell benyújtani. A mentésre adatokat tartalmazó média tárolásáról, megőrzéséről a felhasználó gondoskodik.

Amennyiben a felhasználó jogosan igényel, vagy eleve rendelkezik archiválási eszközzel saját munkaállomásán, úgy a helyi informatikai szervezet segítséget nyújt a helyes archiválási eszköz kiválasztásához, elvégzi annak installálását és segíti a felhasználót az archiválás elsajátításában.

A mentések visszatöltése

A mentések visszatöltése ellenőrzési céllal

A mentési médiákat a mentési eljárás sikeres lefutásától függetlenül a ***"Mentési rend"***-ben előre meghatározott terv alapján szúrópróba-szerűen minimum félévente minden mentési feladat esetén, és évente az archív mentések esetében ellenőrizni kell. Az ellenőrzés lefolytatása az alábbi feladatok végrehajtását jelentik:

a) Média kiválasztása (véletlenszerűen)
b) Visszatöltés teszt-célú rendszerbe átmeneti helyre
c) A sikeresség ellenőrzése mintavételezéses eljárással

d) Média visszahelyezése, teszt elvégzésének dokumentálása

Az ellenőrzések lefolytatását, dokumentálását a mentésért felelős informatikai igazgatóság munkatársa hajtja végre. Az adatvédelmi tisztviselő évente egy alkalommal ellenőrzi a visszatöltések dokumentáltságát.

Mentések visszatöltése visszaállítási céllal

Az adatok visszatöltési idejét az adatok rendelkezésre állása szerinti osztályba sorolásnak védelmi követelményei alapján kell meghatározni.

Az adatok visszatöltését a katasztrófa vagy más létező vészhelyzeti tervek aktualizálása esetén, az abban foglaltak szerint kell végrehajtani.

Egyéb esetben adatok visszatöltését az illetékes munkahelyi vezető kérheti az informatikai igazgatótól.

A visszaállítás tényét a visszatöltést végző rendszergazdának dokumentálni kell.

Mentési médiák kezelése

Cserélhető mentési médiák használatba vétele

Az adathordozót használatba vétel előtt külsőleg is fel kell címkézni. A címkén kötelező jelleggel szerepelnie kell – választott ciklikus mentési rendnek megfelelő – a sorozat és napi azonosítónak. A mentési folyamatokban a szalag belső elektronikus azonosítója használható.

Mentési médiák tárolása

Munkapéldányok tárolása

A napi és heti mentések egyes számú példányait a gépteremben az adathordóra vonatkozó szabályok szerint kell tárolni, hogy szükség esetén a hozzáférés azonnal biztosítható legyen.

Biztonsági másolatok tárolása

A biztonsági mentési kazettákat a jelen szabályzatban előírt módon, biztonsági besorolásától függően az adathordóra vonatkozó szabályok szerint kell tárolni. A másolat elhelyezéséért a mentésért az informatikai igazgatóság munkatárs a felelős.

Archív mentések tárolása

A biztonsági mentési kazettákat a jelen szabályzatban előírt módon, biztonsági besorolásától függően az adathordóra vonatkozó szabályok szerint kell tárolni. Az archívum elhelyezéséért az archiválást kérő szervezeti egység adatgazdája a felelős. A hozzáférésükről naplót kell vezetni.

Mentések, archiválások dokumentálása

A mentések végrehajtását mentési naplóban (automatikusan készül, vagy egyedileg vezetett) kell rögzíteni. Ha külön szabályozás nincsen a mentési rendre, akkor a naplónak a következőket kell tartalmaznia:

a) Szervezeti egység megnevezése
b) Rendszer megnevezése
c) Mentés azonosítója
d) Mentés ideje

e) Mentés tartalma
f) Mentés végrehajtója és aláírása
g) Mentés státusza (sikeres, sikertelen)

A mentési napló ellenőrzését az adatvédelmi tisztviselő végzi.

A mentési médiák rotálására, selejtezésére illetve megsemmisítésére vonatkozó táblázatokat a *13. számú melléklet* tartalmazza.

XXXII. VÉDELMI INTÉZKEDÉSEK

1.1 Hardver eszközök fizikai hozzáférése

Szerverek fizikai hozzáférése

A MATE szervereit az erre a célra kialakított szerverszobákban kell elhelyezni. A szerverszoba kialakítási, és hozzáférési követelményeiről jelen szabályzat ***XIV. fejezete*** rendelkezik.

Munkaállomások fizikai hozzáférése

A munkaállomások elhelyezési követelményeiről, fizikai védelméről jelen szabályzat rendelkezik.

Felhasználóknak tilos a munkaállomás hardver konfigurációját megváltoztatni, a hardver eszköz belsejébe bármilyen okból belenyúlni, burkolatukat megbontani. A csatlakozó külső perifériák csatlakozását megszüntetni.

A munkaállomásokat az üzembe helyezés alkalmával zárjeggyel lehet ellátni annak érdekében, hogy meg lehessen állapítani, ha a hardver eszköz konfigurációját valaki megbontotta.

Az irodán belül a munkaállomást úgy kell elhelyezni, hogy a normál munkavégzés során biztosítva legyen, hogy a munkaállomás képernyőjét csak annak használója láthassa.

Nyomtatók fizikai hozzáférése

A MATE nyomtatóit úgy kell elhelyezni, hogy a kinyomtatott anyagok illetéktelen kezekbe ne kerülhessenek.

Ennek érdekében:

a) A megosztott nyomtatókat úgy kell elhelyezni, hogy az állandó felügyelet, vagy a hozzáférés egyedisége és naplózása biztosított legyen. Elszeparált „nyomtatóhelység" használata tilos!
b) A megosztott nyomtatókon „Belső használatra"vagy „Bizalmas", illetve annál magasabb minősítésű információt csak abban az esetben szabad nyomtatni, ha a nyomtatóhoz hozzáférő valamennyi személynek az ilyen információkba betekintési joga van.
c) Azokat a nyomtatókat, amelyeken „Titkos" anyagok nyomtatása történik, névhez kell kötni, és a munkaállomás közvetlen környezetében, ahhoz közvetlen módon csatlakoztatva (soros, párhuzamos vagy USB port) kell elhelyezni.

Hálózati eszközök fizikai hozzáférése

A hálózati eszközöket úgy kell elhelyezni, hogy az illegális tevékenységből adódó kockázatok minimálisak legyenek.

Ennek érdekében az alábbi elhelyezési körülmények közül kell választani:

a) Központi rendezés esetén a szerverszobában.
b) Osztott rendezés esetén zárható, vagy felügyelhető helyiségben, illetve zárt rack-szekrényben.

Hardver eszközök fizikai biztonsága

A hardver eszközök fizikai biztonságának biztosítása érdekében minimálisan az alábbi védelmeket kell kialakítani:

a) **Tűzvédelem:** A tűzvédelmi szabályzatban kell kitérni az egyes biztonsági zónák tűzvédelmi minősítéséről, és tűzvédelmi megoldásairól.
b) **Villámvédelem:** A MATE épületeit villámvédelemmel kell ellátni, melyeket rendszeresen felül kell vizsgáltatni.
c) **Túlfeszültség-védelem:** Túlfeszültség-védelmet kell telepíteni azoknak az eszközöknek a betáplálásához, amelyek kritikusak a meghibásodás szempontjából (szerverek, aktív eszközök stb.)

A fentieken túl biztosítani kell, hogy a hardver eszközök közelében ne folyjon olyan tevékenység, amely veszélyeztetheti az eszköz működőképességét. Tilos az alábbi tevékenységek folytatása:

a) A hardver eszközökön tilos tárolni olyan anyagokat, amelyek veszélyeztethetik a hardver eszközt (virág, élelmiszer, ital, mágneses tárgyak, stb.).
b) Tilos a hardver eszközök közvetlen környezetében étkezni, és bármilyen italt fogyasztani.

Hardver eszközök üzemeltetési környezetének paraméterei

A hardver eszközök üzemeltetése során figyelembe kell venni a hardver gyártójának üzemeltetésre vonatkozó előírásait.

Általában az alábbi környezeti feltételeket kell biztosítani a hardver eszközök számára:

a) A munkaállomások üzemeltetési hőmérséklet tartomány 15 Celsius foktól 35 Celsius fokig terjedjen. Szerverek esetében ez az érték 21 Celsius környékén stabilizált (klíma). Kerülni kell a hirtelen hőmérsékletváltozást, ügyelni kell a fokozatosságra.
b) A hardver eszközöket óvni kell a fröccsenő víztől, illetve a levegő magas portartalmától.
c) A hardver eszközöket óvni kell az erős mágneses, vagy elektromágneses tértől.
d) A hardver eszközök számára biztosítani kell a gyári specifikációban előírt betáplálást. Ez hazánkban 230 V / 50 Hz.

A fenti követelményeknek való megfelelésért a szerverszobában elhelyezett eszközök esetén az eszközök üzembe helyezéséért felelős rendszergazda, munkaállomások esetében a felhasználó felelősek.

Hardver eszközök teljesítmény-, és kapacitásmenedzsmentje

A hardver eszközök előírt rendelkezésre állási követelményeknek való megfelelősége érdekében a kiszolgáló hardver eszközök teljesítményét, és egyéb kapacitását (pl.: tároló kapacitás, memória kapacitás, processzor teljesítmény, nyomtató kapacitás, stb.) rendszeresen monitorozni kell.

A tapasztalatok alapján eszközönként meg kell határozni azokat a teljesítmény és kapacitás korlátokat, amelyek elérése esetén a hardver eszközök fejlesztése szükséges.

A kapacitástervezésnél figyelembe kell venni azokat az időkorlátokat is, amelyek az eszközök fejlesztéséhez szükséges beszerzésekhez szükséges.

A kapacitás menedzsment végrehajtásáért az adott hardver eszköz üzemeltetését végző rendszergazda felelős.

Hardver eszközök rendeltetésszerű használata

A munkaállomások rendeltetésszerű használatához az alábbiakat kell figyelembe venni:

a) A munkaállomás be-, és kikapcsolásához a hardver eszköz erre a célra kialakított kapcsolóját kell használni. Lehetőség szerint a kikapcsolásra az operációs rendszer kikapcsolás funkcióját kell használni.
b) Az adatvesztés elkerülése érdekében a munkaállomás kikapcsolását kerülni kell, amikor az, lemezműveletet végez (munkaállomás indítása, fájlhozzáférés, stb.)
c) Ha a munkaállomás a művelet végzése közben „lefagy" elsősorban az újraindítással kell próbálkozni (Ctrl+Alt+Del többszöri próbálkozása), kikapcsolás akkor kell kezdeményezni, ha az újraindítás sikertelen volt.
d) A perifériákat (billentyűzet, egér, nyomtató, stb.) csak kikapcsolt állapotban szabad a munkaállomáshoz csatlakoztatni, vagy onnan leválasztani (kivéve USB eszközök).
e) A munkaállomás adatbeviteli egységeibe csak szabványos a munkaállomáshoz illeszkedő adathordozókat szabad behelyezni.

Hardver eszközök kezelési rendjével kapcsolatos óvintézkedések

Hardver eszközök üzembe helyezése

A hardver eszközök üzembe helyezését csak az informatikai üzemeltetés munkatársai végezhetik. A felhasználóknak tilos az üzembe helyezéssel kapcsolatos bármilyen tevékenységet (telepítés, installálás) folytatni.

Az informatikai eszközöket az üzembe helyezés során aláírással ellátott zárcímkével lehet ellátni. A felhasználóknak a zárcímkét tilos eltávolítani, vagy megrongálni.

Hardver eszközök cseréje, módosítása

A felhasználóknak tilos a hardver eszközök konfigurációjának megváltoztatása. Erre csak az informatikai üzemeltetés kijelölt munkatársai jogosultak.

A felhasználók nem csatlakoztathatnak idegen, vagy magántulajdonú perifériákat a munkaállomásaikhoz.

Hardver eszközök javítása, karbantartása

A hardver eszközök rendelkezésre állási követelményeinek való megfelelés érdekében ***„Karbantartási tervben"*** tervszerű megelőző karbantartási, valamint javítási eljárást kell kialakítani.

A hardver eszközök karbantartására évente ***„Karbantartási tervet"*** kell készíteni. A tervben szerepeltetni kell minden eszközt (vagy eszközcsoportot), amelynek karbantartásával számolni kell.

A karbantartási tervben minimálisan szerepelnie kell az alábbi eszközcsoportoknak:

a) Szerverszoba klíma berendezései
b) Szerverek
c) Hálózati aktív és passzív eszközök
d) UPS-ek
e) Központi nyomtatók

A hardver eszközök javításával, karbantartásával kapcsolatos szerződésekben szerepeltetni kell azokat a rendelkezésre állási követelményeket, amelyek az eszköz által kezelt adatok minősítési osztálya megkövetel.

A rendelkezésre állási követelményeknek ki kell térnie:

a) A cég szakembereinek rendelkezésre állásának meghatározására
b) A karbantartás, vagy javítás tárgyát képező eszközök rendelkezésre állási követelményeinek meghatározására

A karbantartási, javítási szerződésekben ki kell térni a titoktartás felelősségekre, vagy a már meglévő szerződéseket ún. „Titoktartási nyilatkozatot" kell kiegészíteni.

A fenti karbantartási, javítási feladatok végrehajtásáért a helyi informatikai igazgató a felelős.

A felhasználók szükség esetén az alábbi karbantartásokat végezhetik:

a) Monitor képernyőjének tisztítása arra alkalmas tisztító eszközökkel.
b) A billentyűzet tisztítása, portalanítása alkalmas tisztító eszközökkel.
c) Az egér tisztítása alkalmas tisztító eszközökkel.

Hardver eszközök tárolása

A használaton kívüli hardver eszközöket raktáron kell tárolni. A raktári tárolás közben is biztosítani kell a gyári specifikációban előírt tárolási környezeti paramétereket. A szerverhelységeket tilos raktárként használni.

A raktári eszközök esetén biztosítani kell az eszközök fizikai védelmét.

Hardver eszközök szállítása

A hardverek eszközök szállítása közben biztosítani kell:

a) A munkavédelmi törvények betartását
b) A hardverek fizikai védelmét
c) A káros környezeti hatásoktól való védelmet (hősugárzás, erős sztatikus kisülés, mágneses tér, folyadék, stb.)

A hardver eszközök szállítása közben biztosítani kell a folyamatos felügyeletet.

Hardver eszközök selejtezése, megsemmisítése, továbbértékesítése

A hardver eszközök selejtezése, megsemmisítése, vagy továbbértékesítése előtt a hardver eszköz adathordozóját visszaállíthatatlanul törölni kell.

A törlési eljárás kiválasztásáról és végrehajtásáról a rendszergazda gondoskodik. Minden más tevékenységet a jelen szabályzatban megfogalmazottak, illetve az érvényben levő selejtezési eljárás szerint kell lefolytatni.

Hardver eszközök nyilvántartása

A törvényben előírt analitikus nyilvántartáson (Leltár) kívül a hardver eszközök nyilvántartására az alábbi nyilvántartást kell vezetni:

a) Szerverek legalább domain béli névvel való azonosítása
b) Hálózati eszközök legalább nevével való azonosítása

c) Raktárnyilvántartások
d) Eszközkiadási bizonylatok
e) Szállítólevél

A szerverhelységekben és rack-szekrényekben elhelyezett szervereket és hálózati aktív eszközöket, az azonosítás megkönnyítése végett fel kell címkézni. A címkéken minimálisan a következő információkat kell feltüntetni:

a) Szerverek esetében domain név
b) Hálózati eszközök esetében az IP-cím

XXXIII. A MOBIL ESZKÖZÖK KEZELÉSI RENDJE

1.1 Mobil eszközök kezelése

A hordozható eszközök használatba adása-vétele

A hordozható számítógépek (notebook), szoftvereit, operációs rendszerét az informatikai igazgatóság üzemeltetésért felelős munkatársai telepítik az előre kidolgozott szabványos eljárás és paraméterezés szerint.

Ugyancsak az üzemeltetésért felelős informatikai igazgatóság munkatársa jogosult az alkalmazói szoftverek telepítésére, verziófrissítésre, a beállítások megváltoztatására.

A többi mobil eszközön csak a gyártó által telepített rendszerszoftver használható, ennek frissítéséről köteles az eszköz használója gondoskodni.

Használatba adás előtt az alábbi védelmi eszközöket kell telepíteni, konfigurálni:

a) Helyi biztonsági házirend
b) Az eszközhöz illeszthető vírusvédelmi szoftver
c) Az eszközhöz illeszthető tűzfal
d) Szükség esetén titkosító szoftvert és/vagy hardver megoldás

A felhasználónak a használatba vétel során ellenőrizni kell:

a) A mobil eszköz és tartozékainak meglétét.
b) A telepített védelmi eszközök meglétét (vírusvédelmi eszköz, személyi tűzfal)

Az átadás-átvétel tényét dokumentálni kell.

A hordozható eszközök használata

A hordozható eszközök konfigurációjának, beállításainak, paramétereinek megváltoztatására kizárólag az üzemeltetésért felelős informatikai igazgatóság munkatársa jogosult.

Amennyiben az eszköz hosszabb ideig (1-2 hét) nem csatlakozik a helyi hálózathoz, a vírusvédelmi szoftver szignatúrájának frissítését a felhasználónak kell megoldani. Ehhez szakmai segítséget a HelpDesk munkatársaitól kaphat.

A felhasználó köteles a hordozható eszközt a munkával kapcsolatos feladatokra, rendeltetésszerűen használni.

A mobil eszközön tilos a „Titkos" minősítésű, valamint magánjellegű adatok tárolása, feldolgozása.

A szükséges frissítések, illetve konfigurációs változtatások végrehajtására, legalább havi rendszerességgel, az üzemeltetésért felelős informatikai igazgatóság munkatársának kérésére a felhasználó köteles a hordozható eszközt a beavatkozás idejére biztosítani.

Az eszköz tárolása

A MATE-ben hordozható eszközöket használaton kívül zárható szekrényben kell tárolni, amelyhez a mobil eszköz használójának kizárólagos joga van.

A hordozható személyi számítógépek épületéből való kivitele

A hordozható eszközök az arra jogosultak mobilitását szolgálják, így az épületből való kivitelhez külön engedély nem szükséges.

Mobil eszközök védelmi előírásai

Mobil eszközök fizikai védelme

A hordozható eszközök mobilitásuknál fogva fokozott veszélynek vannak kitéve a fizikai biztonságukkal kapcsolatos fenyegetettségekkel szemben. A hordozható eszközök fizikai biztonsága érdekében az alábbi szabályokat kell betartani:

A mobil eszközöket csak az arra rendszeresített vízlepergetős, bélelt táskában szabad szállítani. A szállítás során biztosítani kell, hogy az eszköz ne legyen kitéve erős rázásnak, vagy ütésnek. A mobil eszközt tilos felügyelet nélkül hagyni.

Repülőn, autóbuszon, vagy vasúton történő szállítás esetén a hordozható eszközöket kézipoggyászként kell szállítani. A folyamatos felügyeletet ez alatt is biztosítani kell.

A hordozható eszközöket általában tilos kitenni:

a) Erős fizikai behatásnak
b) Sugárzó hőnek
c) Erős mágneses, vagy elektromágneses térnek
d) Fröccsenő víznek
e) Poros környezetnek

A perifériákba csak szabványos adathordozók használhatók.

A megjelenítő eszköz fokozottan érzékeny a fizikai behatásoknak, ezért annak tisztítását csak erre a célra alkalmas törlőkendőkkel, és tisztítóanyagokkal szabad elvégezni.

Mobil eszközökön tárolt adatok védelme

Titkosítás

A hordozható eszközökön külön engedéllyel tárolt a „Titkos" minősítésű adatok védelmére hardveres és/vagy szoftveres titkosító eszközök használata szükséges.

Ebben az esetben a titkosító kulcsokat külső eszközön kell tárolni (PEN drive, SmartCard, Security Key, stb.). A titkosító kulcsokat tartalmazó eszközt a hordozható eszköztől külön kell kezelni (tárolni, szállítani, stb.).

Teendő, ha a számítógépet eltulajdonították

Amennyiben a számítógépet eltulajdonították, az alábbiakat kell tenni:

a) Értesíteni kell a rendőrséget, aki kiállítja a bejelentésről szóló Megbízókönyvet. Értesíteni kell az adatvédelmi tisztviselőt, illetve az informatikai igazgatóságot, aki intézkedik a felhasználó jelszavának megváltoztatására.
b) Az adatvédelmi tisztviselő illetve az informatikai igazgatóság intézkedik az esemény kivizsgálására annak érdekében, hogy megállapítható legyen a felhasználó esetleges felelőssége.

c) Ha a rendőrségi nyomozás nem jut eredményre a nyomozás befejezéséről szóló Megbízókönyvet, és a bejelentésről szóló Megbízókönyvet át kell adni az adott szervezet gazdasági vezetőjének.

Távoli hozzáférések, távmunka

Hozzáférések szabályozása

A távoli hozzáféréseket illetve távmunkával kapcsolatos jogosultság kezelését a jelen szabályzatban leírt módon kell végrehajtani.

Eszközök hálózatra csatlakoztatása

Távoli hozzáférés a MATE hálózatához, informatikai eszközeihez, kizárólag csak a MATE Internet kapcsolatain keresztül üzemeltetett biztonságos virtuális magánhálózat kialakításával (VPN) lehetséges.

A VPN kliensek telepítését a MATE eszközeire az üzemeltetésért felelős informatikai igazgatóság munkatársa végezheti.

Távoli munkavégzésre (Home Office) a felhasználó saját tulajdonú informatikai eszközt csak különleges helyzetben a MATE vezetője írásbeli elrendelése esetén lehet használni. A VPN kliens feltelepítését saját magának kell elvégeznie melyhez segítséget a HelpDesken keresztül kérhet. VPN klienst HelpDesken keresztül az otthoni munkavégzést engedélyező dokumentum csatolásával lehet igényelni. A VPN használatának technikai megoldását az üzemeltetéssel kapcsolatos szabályzatban kell definiálni.

A hallgatók saját eszközeikkel a MATE hálózatára csak az Eduroam hálózaton keresztül a „Hallgatói Felhasználói Szabályzatban" valamint az eduroam.hu oldalon megtalálható szabályzatban meghatározottak szerint csatlakozhatnak.

A kifejezetten belső használatra konfigurált hordozható eszközök nem csatlakoztathatók idegen hálózatra.

A távoli munkavégzés szabályai

A távoli elérés csak működő személyi tűzfal, illetve vírusvédelmi szoftver mellett kezdeményezhető.

A távoli elérés alatt tilos más - nem az aktuális munkával kapcsolatos - tevékenységek folytatása.

A távoli elérés alatt használt erőforrásokat csak szükséges időtartamra szabad foglalni. A nem használt hozzáféréseket be kell zárni.

Mobil eszközök vezeték nélküli hozzáférése

A belső ügyviteli hálózatra kapcsolódó vezeték nélküli hozzáféréséhez a MATE szabványos (wifi) vezeték nélküli hozzáférést biztosít kizárólag alkalmazottai számára, MATE tulajdonban levő mobil eszközökhöz. Vezeték nélküli kapcsolódás esetén gondoskodni kell az illetéktelen használat, megelőzéséről az alábbi előírások egyidejű betartásával:

a) WPA Enterprise (vagy ennél erősebb, illetve hatékonyabb) titkosítással,
b) A MATE hallgatói saját eszközükkel csak az Eduroam hálózatra az eduroram szabályzatában meghatározottak figyelembevételével valamint a „Hallgatói Felhasználói Szabályzatban" meghatározottak szerint csatlakozhatnak.
c) A MATE WIFI hálózatát csak azonosított felhasználók használhatják.

d) Kivételt képez konkrét eseményhez (pl. konferencia) kötötten az informatikai igazgató engedélyével. Ebben az esetben az informatikai igazgatóság kérésre külön WIFI hálózatot biztosít. A rendezvény szervezője köteles gondoskodni arról, hogy a részvevők megfelelő tájékoztatást kapjanak a WIFI használat szabályairól.

Ellenőrzések

A mobil eszközök használata szabályainak betartását az informatikai igazgatóság munkatársai rendszeresen ellenőrzik.

Amennyiben az ellenőrzés során olyan megállapításra jutnak, hogy az eszköz használata veszélyezteti a MATE informatikai hálózatát, eszközeit, kötelesek letiltani az adott eszköz csatlakozását.

A távoli hozzáféréseket naplózni kell, a log-állományokat rendszeresen elemezni, és kiértékelni szükséges.

XXXIV. A SZOFTVEREKHEZ KAPCSOLÓDÓ VÉDELMI INTÉZKEDÉSEKNEK

1.1 Szoftverek erőforráskönyvtárainak védelme

A MATE-nál használt szoftverek védelmének érdekében a szoftverek erőforráskönyvtárait védeni kell az illetéktelen hozzáférésektől az illetéktelen installációtól és az abban található fájlok nem rendeltetésből adódó megváltoztatásától.

Szoftverek nem használt funkcióinak tiltása

A MATE-nál használt szoftverek védelmének érdekében a szoftverek (különösen az operációs rendszer) nem használt funkcióit, szolgáltatásait (szervizeit) le kell tiltani.

Az operációs rendszerek nem használt távdiagnosztikai portjait szintén le kell tiltani, hogy csökkentsük a távoli elérésből származó kockázatokat.

Szoftverek biztonsági frissítése

Az informatikai igazgatóság munkatársainak figyelni kell a megjelenő sérülékenységekről szóló jelentéseket

Ki kell dolgozni a MATE-ban használt szoftverek biztonsági frissítésével kapcsolatos:

a) Letöltési folyamatokat
b) Disztribúciós folyamatokat
c) Tesztelési folyamatokat
d) Implementációs folyamatokat

A biztonsági frissítéseket, a megjelenésüket követően a lehető legrövidebb idő alatt kell telepíteni.

„Dobozos" szoftverek tárolása

A „dobozos" szoftvereket a helyi informatikai rendszer üzemeltetéséért felelős szervezeti egység, központi helyen kell tárolni.

Szoftverek nyilvántartása

A MATE-nál használt szoftverekre és szoftver licencekre nyilvántartást - a tárgyi eszköz nyilvántartásától függetlenül - kell vezetni. A nyilvántartások vezetéséért az informatikai igazgató felelős. A nyilvántartás tartalmazza:

a) A szoftver pontos megnevezését
b) A szoftver verziószámát
c) Nyelvi verzióját
d) A szoftver regisztrációs kódját (nem azonos az installációs kóddal)
e) A szoftverhez tartozó licence szerződés számát
f) A licenc jellegét vagy típusát
g) A szoftver licence hány telepítésre ad lehetőséget (felhasználó szám)
h) A beszerzés idejét
i) A szállító nevét

A szoftverek informatikai nyilvántartásánál figyelembe kell venni a mindenkor érvényben lévő számviteli törvény előírásait, a BSA (Business Software Alliance) ajánlásait. Az informatikai szoftver nyilvántartásának összhangban kell lennie az ügyviteli rendszerek (tárgyi eszköz) nyilvántartásával.

XXXV. A KOMMUNIKÁCIÓHOZ KAPCSOLÓDÓ VÉDELMI INTÉZKEDÉSEK

1.1 Az elektronikus levelezés biztonsága

Az elektronikus levelezés biztonsági követelményei

Az elektronikus levelezés a MATE informatikai rendszerében az egyik fő fenyegetettség forrása. Az elektronikus levelezés biztonsága érdekében az alábbi előírásokat kell betartani:

Az elektronikus levelezéssel kapcsolatos tiltórendelkezések az alábbiak:

a) Szigorúan tilos a közízlést, a MATE jó hírnevét veszélyeztető, erkölcstelen, vagy politikai tartalmú e-mail elküldése.
b) Tilos a levelező rendszert „Titkos" minősítésű fájlok, dokumentumok kijuttatására használni.
c) Tilos a MATE Központos ügyeket nem a Központos, MATE vagy intézetei által biztosított levélcímen intézni. Tilos olyan levelek továbbítása a MATE levelező rendszerében, amelyek bármilyen nyelven arra szólítanak fel, hogy a levelet minél több címre kell továbbítani (lánclevél).
d) Tilos feliratkozni nem szakmai jellegű illetve nem az ügyviteli vagy oktatási munkát segítő hírlevél küldő szolgáltatásra.
e) Tilos válaszolni olyan levelekre, amelyek arra szólítanak fel, hogy a MATE biztonsági rendszeréről, vagy a felhasználó saját hozzáférési adatairól (felhasználónév, jelszó) adjon tájékoztatást. Ilyen esetekben azonnal értesíteni kell az informatikai igazgatóság munkatársait, akik a szükséges védelmi intézkedéseket megteszik.
f) Tilos az elektronikus levelező rendszeren „Titkos", információt titkosítás nélkül továbbítani.
g) A levélszűrésen fennakadt levelekről automatikus üzenet csak a MATE alkalmazottjának küldhető. Ezzel kapcsolatos automatikus üzenet küldése a MATE-n kívülre tilos.
h) Tilos a kéretlen levelek (spam gyanús) megnyitása, melléleteinek megnyitása, és a levélben elhelyezett linkek megnyitása.
i) Tilos a levelezés átirányítása külső levelező szolgáltatóhoz.

Az elektronikus levelezés korlátozásai

Az elektronikus levelezés biztonsága érdekében az alábbi korlátozások vannak érvényben:

A fogadható és küldhető levelek maximális megengedett mérete általában 50 MB.

Ennél nagyobb méretű állomány küldésére kizárólag csak a MATE által biztosított alkalmazás vehető igénybe.

Elektronikus levelezés magáncélú használata

Mivel minden levelezést a MATE tulajdonát képező infrastruktúra és erőforrások biztosítanak, ezért a magán célú levelezésre a MATE által biztosított postafiók nem használható. A fentieken túl kerülni kell az Interneten található ingyenes levelezési portálok belülről történő használatát.

Elektronikus levelezés jogosultsága

A MATE valamennyi aktív jogviszonnyal rendelkező alkalmazottja, hallgatója hozzáférést kap az elektronikus levelezési rendszerhez.

Elektronikus levelezés ellenőrzése

A MATE fenntartja a jogot a levelezés méretének, gyakoriságának, korlátozására a levelező szerver és az Internet csatlakozás kapacitásának hatékonyabb kihasználása, valamint a MATE informatikai rendszerének biztonsága érdekében.

Az internet biztonsága

Az Internet hozzáférés biztonsági előírásai

Az Internet hozzáférés a MATE informatikai rendszerében az egyik fő fenyegetettség forrása. Az Internet hozzáférés biztonsága érdekében az alábbi előírásokat kell betartani:

Az Internet hozzáférést csak a kutatási, az ügyviteli folyamatokkal, illetve azok támogatásával kapcsolatos ügyintézésre, szabad használni.

Az Internet böngészőknél törekedni kell a legmagasabb biztonsági szint beállítására.

Az Internetezés közben el kell utasítani azokat a felbukkanó párbeszéd ablakokat, amelyek segédprogramok telepítésére, vagy egyes funkciók kikapcsolására ösztönöznek.

Tilos az Internetes web helyek eléréshez szükséges jelszavakat úgy megválasztani, hogy abból a MATE-nál használt jelszóra következtetni lehessen. Erről a felhasználót tájékoztatni kell.

Korlátozások az Internet használatában

Tiltott Internetes alkalmazások

A MATE-nál csak a rendszeresített Internetes alkalmazások használhatók.

A MATE-nál a felhasználóknak szigorúan tilos olyan internetes alkalmazások használata:

a) Melyekkel a MATE, vagy más személyek információinak, alkalmazásainak, bizalmasságának, sértetlenségének, rendelkezésre állásának megsértésére irányul.
b) Melyekkel a MATE erőforrásainak illegális megosztására irányul.
c) Melyek licenc szerződéseivel a MATE nem rendelkezik.

Tiltott Web helyek

Szigorúan tilos a MATE érdekeit sértő, erkölcstelen oldalak látogatása, bővebb szabályozást a MATE Informatikai Szabályzat tartalmaz, amely hivatkozik a KIFÜ Program Felhasználói Szabályzatára (HTTP://WWW.KIFU.GOV.HU).

Tiltott Internetes tevékenységek

Internet használata során be kötelező tartani a törvényes rendelkezéseket.

Szigorúan tilos minden, a közízlést sértő, erkölcstelenállomány letöltése. Bővebb szabályozást a MATE szabályzatai tartalmaznak, mely hivatkozik a KIFÜ szabályzatára (HTTP://WWW.KIFU.GOV.HU)

A MATE fenntartja a jogot, hogy biztonsági okokból technikai szűréseket és korlátozások rendeljen el az informatikai igazgató által.

Az Internet hozzáférések ellenőrzése

A MATE fenntartja a jogot az Internetezés gyakoriságának, és ha szükséges tartalmának ellenőrzésére, korlátozására az Internet csatlakozás kapacitásának hatékonyabb kihasználása, valamint a MATE informatikai rendszerének biztonsága érdekében.

A KIFÜ előírásai

a) A MATE informatikai rendszere több ponton kapacsolódik a KIFÜ tagintézmények és felhasználók számára üzemeltetett hálózati infrastruktúrához és szolgáltatásainak egy részét ezen keresztül biztosítja. Ebből következően minden MATE felhasználó egyben KIFÜ felhasználó is. így minden MATE felhasználó köteles betartani a Nemzeti Információs Infrastruktúra Fejlesztési Programról szóló 5/2011. (II.3.) Korm. rendeletben meghatározott, a Fejlesztési Program keretében működtetett számítógép-hálózat használati szabályait.

Az KIFÜ hálózat használati szabályzat teljes szövege megtalálható az Informatikai és Hírközlési Közlönyben illetve az IHM és a KIFÜ (HTTP://WWW.KIFU.GOV.HU) internetes honlapján. Kivonatolt formájában a MATE Informatikai Szabályzatban olvasható.

ZÁRÓ RENDELKEZÉSEK

A szabályzat által hivatkozott biztonsági dokumentumokat a hatálybalépéstől számított folyamatosan kell kidolgozni és a folyamatokba beilleszteni.

Gödöllő, 2021.11.05.

Prof. Dr. Gyuricza Csaba
rektor

Magyar Agrár- és Élettudományi Egyetem
4.

1 számú melléklet - Helyettesítő mátrix

sorszám	Szerepkör	Név	Helyettesítő sorszáma	ELÉRHETŐSÉG E-mail Vezetékes telefon; Mobil telefon
1.	Rektor			
2.	Rektor-helyettes			
3.	Gazdasági Főigazgató			
4.	Koordinációs Főigazgató			
5.	Humánerőforrás Igazgató			
6.	Informatikai Igazgató			
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				

Jelen táblázatnak minden esetben aktualizáltnak és könnyen elérhetőnek kell lenni.

Gödöllő, ...

2 számú melléklet - az informatikai biztonsággal kapcsolatos feladatkiadásra, teljesítésigazolásra és kapcsolattartásra jogosultak szerepkörei, elérhetőségei

Beosztás	Név	Mobil elérhetőség	Vezetékes telefon	Cím
Adatvédelmi Tisztségviselő				
Informatikai Igazgató				
Információ Biztonsági Felelős				
IT Biztonsági Felelős				

3 számú melléklet – Információ Biztonsági Felelős elérhetőségei

Információ Biztonsági Felelős				
Neve	**Minősítése (GOVCERT, NKI)**	**Végzettsége a 2013. évi L szerint**	**Elérhetősége**	**NKI és GOVCERT elfogadottsága**

4 számú melléklet – Az üzemeltetésért / támogatásért felelős szervezeti egység vezetőjének megnevezése és elérhetősége

Beosztás	Név	Mobil elérhetőség	Vezetékes telefon	Cím
Informatikai Igazgató	Madarász Miklós	06704911350		2100 Gödöllő, Páter Károly utca 1.

5 számú melléklet – Beszállítói Alapminősítő Lap, Partner / Beszállítói Elégedettség Mérés

BESZÁLLÍTÓI ALAPMINŐSÍTŐ LAP (BAM)						
Beszállító megnevezése:				Címe:		
Cégbírósági adatok állapota:	**RENDEZETT**			**RENDEZETLEN**		**NEM VIZSGÁLT**
Elismertsége az informatikai piacon	**Pont**	**Nemzetközileg elismert**		**Országosan elismert**	**Szakmai körökben elismert**	**Nem elismert**
	Adható	3 pont		2 pont	2 pont	0 pont
	Adott					
Elismertsége az MATE-n belül	**Pont**	**Nagyon elismert**		**Elismert**	**Kevésbé elismert**	**Nem elismert**
	Adható	3 pont		2 pont	1 pont	0 pont
	Adott					
Szállított termék (áru, szolgáltatás) minősége, megbízhatósága	**Pont**	**Kiváló**		**Megfelelő**	**Elfogadható**	**Gyenge**
	Adható	3 pont		2 pont	1 pont	0 pont
	Adott					
Szállítási határidő betartása	**Pont**	**Mindig pontos**		**Néha előfordul késés**	**Gyakran fordul elő késés**	**Kiszámíthatatlan**
	Adható	3 pont		2 pont	1 pont	0 pont
	Adott					
Emberi kapcsolatok	**Pont**	**Kiváló**		**Megfelelő**	**Gyenge**	**Együttműködésre alkalmatlan**
	Adható	3 pont		2 pont	1 pont	0 pont
	Adott					
MINŐSÍTÉS EREDMÉNYE						
Besorolási kategória	**Elért érték**	**Kategória**	„A"	„B"	„C"	„D"
			Kiváló,	(Megfelelő	(Korlátozottan igénybe vehető,	(Alkalmatlan,
			14-15 pont	9-13 pont)	6-8 pont)	0-5 pont)
JAVASLOM	**NEM JAVASLOM**		MEGJEGYZÉS:			
Informatikai vezető neve:			Aláírás:		Dátum:	
KÖVETŐ MINŐSÍTÉS						
Munkaszám:	**Szállított termék minősége**		**Szállítási határidő betartása**	**Emberi kapcsolatok**	**Minősítés összesített eredménye**	**Minősítést végezte/ dátum**

Egyéb megjegyzés, probléma (munkaszámhoz rendelve):	

PARTNER / BESZÁLLÍTÓI ELÉGEDETTSÉG MÉRÉS (PEM)			
		Azonosító Szám	
	Tel: +36-.....; Fax: +36-.....	**Változat száma:**	
		Indítási dátum	

Véleményezett szervezet	**Véleményező Főosztály/Osztály**	**Dátum**	
		Kitöltő Neve; aláírása	

Tisztelt Fő/Osztály vezető!

Annak érdekében, hogy beszállítóink színvonalát emelhessük, és a vállalkozások eredményét mérhessük, szeretnénk folyamatosan figyelemmel kísérni véleményüket.

Számunkra a legfontosabb a Központ elégedettségének elérése, ezért kérjük, hogy a kérdőív kitöltésével segítse elő, hogy a szolgáltatások minőségének dinamikus fejlesztését a Partnereink és Szolgáltatóink tevékenységét és minőségét, mint a Központ számára legfőbb minőségcélt, meg tudjuk valósítani.

Amennyiben a kérdések olvasása során találkozik olyan tényezővel, amely Önt vagy Szervezetét nem érinti, kérjük, azt jelölje, és mellőzze annak megválaszolását.

Nemzeti Agrárkutatási és Innovációs Központ Vezetője

No	**Kérjük, jelölje az 1-től 9-ig terjedő skálán az Ön által megfelelőnek tartott választ!** **9 (teljes mértékben),** 8, 7, 6, **5 (részben),** 4, 3, 2, **1 (egyáltalán nem) 0 (nem releváns) (javasoljuk a jelzet cellát X-elni)**									
1.	**Elégedett-e az ajánlatok stílusával, pontosságával, áttekinthetőségével?**									
	9	8	7	6	5	4	3	2	1	0
2.	**Mennyire felelt meg az elvárásainak a Véleményezett szervezet által végzett szolgáltatások minősége?**									
	9	8	7	6	5	4	3	2	1	0
3.	**Jónak tartja-e a Vizsgált szervezet együttműködését és tevékenységét a projekt során?**									
	9	8	7	6	5	4	3	2	1	0
4.	**Mennyire tartotta elfogadhatónak, a Véleményezett szervezet által beszerelt egységek minőségét?**									
	9	8	7	6	5	4	3	2	1	0
5.	**Mennyire tartotta elfogadhatónak, a Véleményezett szervezet által végzett tevékenység minőségét?**									
	9	8	7	6	5	4	3	2	1	0

6.	Mennyire tartotta elfogadhatónak, a Véleményezett szervezet által vállalt, tervezet és projekt tevékenységet?									
	9	8	7	6	5	4	3	2	1	0
7.	Mennyire érezte korszerűnek a szállított eszközöket?									
	9	8	7	6	5	4	3	2	1	0
8.	Mennyire érezte minőséginek és az elvártnak megfelelőnek a szállított eszközöket?									
	9	8	7	6	5	4	3	2	1	0
9.	Mennyire érezte korszerűnek és szakszerűnek a Véleményezett szervezet által nyújtott szolgáltatásokat?									
	9	8	7	6	5	4	3	2	1	0
10.	Mennyire érezte korszerűnek a Véleményezett szervezet szervizszolgáltatásait?									
	9	8	7	6	5	4	3	2	1	0
11.	Mennyire érezte szakszerűnek, felkészültnek és tájékozottnak a Véleményezett szervezet szakembereit?									
	9	8	7	6	5	4	3	2	1	0
12.	Mennyire tartja megfelelőnek a hiba bejelentésétől, a kiszállásig/javításig eltelt időt?									
	9	8	7	6	5	4	3	2	1	0
13.	Mennyire tartja, megfelelőnek a Véleményezet szervezet rugalmasságát és kötelezettségteljesítését?									
	9	8	7	6	5	4	3	2	1	0
14.	Mennyire érezte megfelelőnek a Véleményezett szervezet műszaki-szakmai felkészültségét?									
	9	8	7	6	5	4	3	2	1	0
15.	Kedvesek és segítőkészek voltak-e a Véleményezett szervezet szakemberei kiszálláskor?									
	9	8	7	6	5	4	3	2	1	0
16.	Jónak tartja-e a Véleményezett szervezet garanciális és/vagy garancia utáni tevékenységét?									
	9	8	7	6	5	4	3	2	1	0
17.	Jónak tartja-e a Véleményezett szervezet fejlesztőinek hozzáállását és rugalmasságát?									
	9	8	7	6	5	4	3	2	1	0
18.	Jónak tartja-e a Véleményezett szervezet, szerviz ügyintézési folyamatát?									
	9	8	7	6	5	4	3	2	1	0
19.	Jónak tartja-e a Véleményezett szervezet Help desk és Hibajavító tevékenységét?									
	9	8	7	6	5	4	3	2	1	0
20.	Véleményezett szervezetnek milyen mértékben sikerült a megrendelő igényeit szem előtt tartani a reklamációkezelés során?									
	9	8	7	6	5	4	3	2	1	0
21.	A Véleményezett szervezet kellő szakszerűség jellemezte-e a projekt során a műszaki és/vagy szoftver tanácsadás során?									
	9	8	7	6	5	4	3	2	1	0
22.	A Véleményezett szervezet tevékenységét, közreműködését tudná-e más alkalommal is javasolni?									

	9	8	7	6	5	4	3	2	1	0
23.	**Egyéb észrevételek, javaslatok:**									
24.	**Összesítés az egyes mezőkben lévő igenlő válaszok száma (db)**									
	9	8	7	6	5	4	3	2	1	0
	Az adott cellákban lévő válaszok száma szorozva a cella értékkel									
	Véleményezés összesen a kapott szorzatok (∑pontszám*db) :									

Gödöllő év hó nap

.....

aláírás

BESZÁLLÍTÓK MINŐSÍTÉSE (ALM)	Azonosító:	Oldalszám:
BESZÁLLÍTÓ megnevezése:	Címe:	

ALAPMINŐSÍTÉS

1. Cégbírósági adatok állapota:	**RENDEZETT**	**RENDEZETLEN**	**NEM VIZSGÁLT**	
2. Ismertsége az informatikai piacon:	**Nemzetközileg ismert**	**Országosan ismert**	**Szakmai körökben ismert**	**Nem ismert**
3. Ismertsége az Központon belül (korábbi szállító):	jól ismert	ismert	kevésbé ismert	nem ismert

JAVASLOM NEM JAVASLOM	MEGJEGYZÉS:	
Osztályvezető neve:	Aláírás:	Dátum:

KÖVETŐ MINŐSÍTÉS

Minősítési értékek lehetnek:

Teljesítményre: kiváló, megfelelő, elfogadható, gyenge

Határidőre: határidőre, kisebb késés, nagyobb késés

Kapcsolatra: kiváló, megfelelő, gyenge

Munkaszám: _ _ _ _ _ _ / _ _ _ _	**Megbízás jóváhagyva/ dátum**	**Teljesítmény**	**Határidő**	**Kapcsolat**	**Minősítést végezte/ dátum**

Egyéb megjegyzés (munkaszámhoz rendelve):

6 számú melléklet – A SZÁLLÍTÓ / FEJLESZTŐ / KARBANTARTÓ / RENDSZERTÁMOGATÓ / STB. SZERVEZET(EK) MEGNEVEZÉSE(I) ÉS ELÉRHETŐSÉGE(I)

Cég név	A MATE-nál végzett tevékenység	Képviselő neve	Mobil elérhetőség	Cím

7 számú melléklet – A SZÁLLÍTÓ / FEJLESZTŐ / KARBANTARTÓ / RENDSZERTÁMOGATÓ / STB. SZERVEZET(EK) NEVÉBEN MUNKÁT VÉGZŐ(K) és/vagy kapcsolattartásra jogosult(ak) neve(i) és elérhetősége(i):

No	Cég név	A MATE-nál végzett tevékenység	Dolgozó neve	Mobil elérhetőség	IT Területei korlátozás
1.					
2.					
3.					
4.					
5.					
6.					

Minden külsős munkavégző esetében (cég, személy) a rájuk vonatkozó IBSZ megismerését aláírással igazoltatni kell.

8 számú melléklet - AZ ADATOK MINŐSÍTÉSÉNEK ÉS KEZELÉSÉNEK RENDJE

1. Az adatok osztályozása

A bizalmasság, sértetlenség, és rendelkezésre állás, sérüléséből vagy elvesztéséből vagyoni, erkölcsi, és jogi hátrány származhat. Az egyes kritikusnak tetsző vagy annak tapasztalt vagyontárgyak besorolását egy vagyonleltár tartalmazza, melyben az alábbi értékeléseket végzi el a MATE megbízott munkacsoportja. A besorolásokat évről évre felül kell vizsgálni és fejleszteni kell a tapasztalatok alapján. A hátrány mértéke az alábbi besorolás szerint határozható meg:
A táblázat három jelentős oszlop értékelési lehetőségét bontottuk le.

INFORMATIKAI VAGYONELEM LELTÁR

Sorszám	Vagyonelem Megnevezése	Típusa	Értéke (Ft)	Leírása (funkció)	Felelőse / admin	biztonsági besorolása (osztály)	Rendelkezésre állási besorolása (sorrend)	Feldolgozás kritikus időszak (-tól; -ig)	Megengedett kiesési idő (perc)	Feldolgozó/Kapcsolódó alkalmazás(ok)	Kockázati tényezők (internet, intranet, adat tartalom, személyes adat, kutatási adat, publikáció)	Kritikussági besorolásuk (kockázati tényező %)	Elvárt rendelkezésre állásuk (%)	Lehetséges kár értékük (teljes, részleges, érték %-a)	Védelmi elem, rendszer, környezet (HW,SW)	Futtató hardver (fájl szerver azonosító, adatbázis szerver azonosító)
1.																
2.																
3.																
4.																
5.																
6.																
7.																
8.																
9.																
10.																

2. Besorolás a keletkezett lehetséges kár alapján

Az osztályozás alapját a bizalmasság, a sértetlenség, és a rendelkezésre állás sérüléséből, vagy elvesztéséből keletkező, a MATE számára kimutatható lehetséges hátrány nagysága képezi.

	A hátrány mértéke (Vagyontárgy értéke)		
	Elhanyagolható	**Jelentős**	**Súlyos**
Vagyoni hátrány			
Vagyoni kár, vagy többletköltség,	A kár nagysága meghaladja a szabálysértési értékhatárt.	A kár nagysága meghaladja az 500.000 forintot.	A kár nagysága meghaladja a 1.000.000 forintot.
Erkölcsi hátrány			
Bizalomvesztés a hallgatók körében	A MATE megítélése lényegesen nem változik.	Bizalomvesztés a MATE 1-2 alkalmazottjával szemben	Bizalomvesztés a MATE egy szervezetével szemben.
Bizalomvesztés a dolgozók körében (Munkahelyi hangulat).	A MATE alkalmazottai körében legfeljebb kisebb, átmeneti elégedetlenség (csalódottság) áll fenn.	Bizalomvesztés a MATE egy szervezetének vezetőjével szemben.	Bizalomvesztés a MATE felső vezetésével szemben.
Jogi hátrány			
A törvényesség megsértése	A MATE-vel szemben nem indul jogi eljárás.	A MATE-vel vagy a MATE egy alkalmazottjával szemben jogszabálysértés elkövetése miatt indul eljárás.	A MATE-vel, vagy a MATE egy alkalmazottjával szemben vétség vagy bűncselekmény elkövetése miatt indul eljárás.
Jogi és oktatási kötelezettségek	A kár a MATE jogi, szerződéses és oktatási kötelezettségeinek teljesítését zavarja (kisebb, incidens jellegű fennakadásokat okoz).	A kár a MATE jogi, szerződéses és oktatási kötelezettségeinek teljesítését gátolja (a teljesítés, és annak minősége csak újabb erőforrás bevonásával biztosítható).	A MATE csak jelentős késéssel, esetleg nem megfelelő minőséggel tudja teljesíteni a jogi, szerződéses és oktatási kötelezettségeit.
	A hátrány mértéke (Vagyontárgy értéke)		
	Elhanyagolható	**Jelentős**	**Súlyos**
Információk bizalmasságának, sértetlenségének sérülésével kapcsolatos incidensek	Nyilvános információk, dokumentumok illetéktelen személy által történő megváltoztatása, az információk pontosságának, és teljességének sérülésével.	„Bizalmas" vagy „Belső használatú" minősítésű információk illetéktelen kezekbe, vagy nyilvánosságra kerülése, vagy illetéktelen személy által történő megváltoztatása, az információk pontosságának, és teljességének sérülésével.	„Titkos" minősítésű információk illetéktelen kezekbe, vagy nyilvánosságra kerülése, vagy illetéktelen személy által történő megváltoztatása, az információk pontosságának, és teljességének sérülésével.
Üzletmenet (ügyvitel, iktatás)			
Az üzletmenet minősége és folytonossága	Az üzletmenet folyamatos, kisebb incidens jellegű fennakadások észlelhetők.	A kár az üzletmenetet gátolja (az üzletmenet folytonossága, vagy minősége csak újabb erőforrások bevonásával biztosítható).	A kár a MATE-et az üzletmenet folytonossági terv aktiválására vagy ezzel egyenrangú intézkedésekre kényszeríti.

3. Az adatok kezelésének követelményei

A következő táblázat az adatok kezelésével kapcsolatos követelményeket foglalja össze **bizalmasság** és **sértetlenség** szerint (**Vagyonelem biztonsági besorolása**):

	„Nyilvános" illetve „Nem védett"	**„Bizalmas" illetve „Védett"**	**„Titkos" illetve „Fokozottan védett"**
Tárolás	Központi tároló helyen kell tárolni.	Személyes, vagy korlátozott hozzáférésű mappában/ dossziéban kell tárolni.	Titkosított mappában/ dossziéban kell tárolni.
Adatátvitel	Nincs követelmény.	A MATE-en kívülre jelszó védett állományban (pl.: ZIP vagy jelszóval védett Office dokumentum) kell küldeni.	A fájl titkosításával kell küldeni (pl.: PGP).
Adatmegosztás	A központi nyilvános tároló helyeken megosztható.	A központi tároló helyen a betekintésre jogosultak körében megosztható.	Nem megosztható, szükség esetén több példányban kell tárolni.
Megsemmisítés, törlés	Nincs követelmény.	Csak az adatgazda engedélyével törölhető/semmisíthető meg.	Csak az adatgazda engedélyével törölhető/semmisíthető meg. Az elektronikus adathordozón lévő adatokat törölni kell, a papír alapú dokumentumokat a MATE Iratkezelési szabályzata szerint kell kezelni. A hibás adathordozókat fizikailag meg kell semmisíteni.
Felülvizsgálat	Nincs követelmény.	Minimálisan kétévente.	Minimálisan évente.

Az adatok kezelésének követelményei **rendelkezésre állásuk** szerint:

	„Általános"	**„Fontos"**	**„Kritikus"**
Tárolás	Elégséges a központi tároló helyen való elhelyezés.	Kötelező a kétpéldányos tárolás (egy online elérésű és egy rendszeres napi mentésű off-line példány). Az off-line példány esetében adatok tárolási helyét rögzítő nyilvántartás (back-up log, lista, stb.) kíséretében.	Kötelező a kétpéldányos tárolás (egy online elérésű és egy rendszeres napi mentésű off-line példány). Az off-line példány esetében adatok tárolási helyét rögzítő nyilvántartás (back-up log, lista, stb.) kíséretében.
Adatátvitel	Nincs követelmény.	A forráshelyen és a nyilvántartásban megjelölt tárolási helyen maradjon egy példány az adatból.	Tartalék vagy redundáns eszközt, csatornát kell biztosítani.

9 számú melléklet - AZ ADATOK MINŐSÍTÉSÉNEK ÉS KEZELÉSÉNEK RENDJE

Zóna követelmények	1. számú biztonsági zóna	2. számú biztonsági zóna	3. számú biztonsági zóna
Általános követelmények			
Természeti katasztrófák kockázatainak csökkentése	-	-	A zóna kialakításánál figyelembe kell venni az árvíz, belvíz, villámcsapás és egyéb természeti katasztrófák kockázatait.
Hozzáférési követelmények			
Belépés, beléptetés	Információbiztonsági szempontból nincsen előírás.	Az irodákba történő belépés kulccsal történik.	A zónába történő belépés egyedi azonosítással (mágneskártya, kód, stb.) történik.
A belépés engedélyeztetése	Külön engedély nem szükséges.	A fogadó szervezet vezetőjének szóbeli engedélye szükséges.	Írásbeli engedély szükséges.
Környezeti követelmények			
Klimatizálás	-	-	Klimatizálás szükséges.
Páratartalom mérése	-	-	A páratartalom mérése szükséges.
Áramellátás szabályozása	-	-	Az áramellátás szabályozása, és a működés redundanciája szükséges.
Tűzvédelem	Kézi tűzoltó készülékek kihelyezése szükséges a folyósón.	Kézi tűzoltó készülékek kihelyezése szükséges a folyósón.	Tűzvédelmi füstérzékelő és a közelben kézi riasztó szükséges. A helységben vagy annak bejáratánál kézi tűzoltó készülék kihelyezése szükséges.
Kontroll követelmények			
Biztonsági felügyelet	-	-	Felügyeleti (riasztó) eszközökkel kell ellátni.
Behatolás-védelem	Passzív behatolás védelmi eszközök szükségesek az alagsori, földszinti, és 1. emeleti ablakokra.	Passzív behatolás védelmi eszközök szükségesek az alagsori, földszinti, és 1. emeleti ablakokra.	Passzív behatolás védelmi eszközök szükségesek az alagsori, földszinti, és 1. emeleti ablakokra, valamint aktív behatolás-védelmi eszközök felszerelése szükséges a helységbe vagy a folyosókra.
Dokumentálási követelmények			
A beléptető rendszer naplózásával vagy a kulcs felvételénél kell dokumentálni	-	A kulcs felvételnél kell dokumentálni.	A belépések naplózása.
Biztonsági események	-	-	A felügyeleti eszközök jelentéseit naplózni kell.

10 számú melléklet – A RENDSZERBIZTONSÁGI TERV ÉS TARTALMA

Szerver db szám	Kliens db szám	Campus/telephely
0	**0**	**2100 Gödöllő, Páter Károly u. 1.**
0	**0**	

A lista összeállítása szerint a szükséges és elégséges feltételek teljesülése, mint minimális konfiguráció jelenik meg.

11 számú melléklet – VÉSZHELYZETI TERVEK TENNIVALÓI ÉS FELELŐSEI

1. Vészhelyzeti elérhetőségek

Név	Érintett terület	Elérhetőség
Madarász Miklós	papír alapú információk, informatika alapú információk	20/968 8356

2. Vészhelyzeti értesítési lánc

	Nappal			Éjszaka / munkaidőn túl	
1.	észrevételező			észrevételező	
				portaszolgálat	
2.	alkalmazásgazda / informatikai központ munkatársa	informatikai igazgató / Koordinációs főigazgató		informatikai igazgató / koordinációsfőigazgató / rektor	intézeti információbiztonsági felelős
3.	rektor (szükség esetén)				

3. A kritikus területek meghatározása

A kritikus információbiztonsági területek meghatározása az információbiztonsági kockázatértékelés során történik.

4. Vészhelyzet elrendelése

Aszerint, hogy a kialakult hiba milyen hatáskörzetben észlelhető, megkülönböztethető:

1. a folyamatban résztvevők jelentései alapján,
2. külső jelzés útján előforduló rendkívüli eseményeket.

Minden olyan esetben, amikor a munkatársba felmerül a gyanú, hogy a MATE bármely folyamata során az információbiztonsági szempontokat veszélyeztető esemény várható vagy az már be is következett, akkor köteles jelenteni azt **közvetlen felettesének** és/vagy a **adatvédelmi tisztviselőnek, rendszergazdának**. Amennyiben az észrevétel külső féltől ered, a kapcsolattartó kötelessége az információ továbbítása.

A vészhelyzetnek megfelelő minősítést, valamint a vészhelyzeti terv alkalmazását

1. rektor,
2. koordinációs főigazgató
3. informatikai igazgató,
4. intézetigazgató,
5. adatvédelmi tisztviselő rendelheti el.

5. Az irányítási feladatok

Amennyiben a vészhelyzet kezelése az intézet / campus/telephely egységein túli szervezetek bevonását is jelenti a vészhelyzet kezelésének összehangolása, koordinálása a **rektor** feladatköre. Az intézeti **adatvédelmi tisztviselő** feladata a hatáskörük alá tartozó területek esetén az intézkedések közvetlen irányítása, a munkatársa koordinálása, kapcsolattartás a **rektorral, koordinációs főigazgatóval, informatikai igazgatóval,** és szükség szerint más **területek vezetőivel**. Amennyiben a vészhelyzet az üzem területi egységein belül jelentkezik a vészhelyzet irányítása a **területi vezető** feladatköre.

6. Veszélyhelyzeti tevékenységek

	Tevékenység	***Felelős***
1.	Riasztás, vezetők kiértesítése az értesítési láncnak (0. pont) megfelelően	észrevételező
2.	Információk pontosítása, a vészhelyzeti állapot elrendelése	irányításért, minősítésért felelős személy
	Szükség szerint külső szervek bevonása (pontosítani: pl. Rendőrség, Kárelhárítás stb.)	rektor, koordinációs főigazgató, informatikai igazgató
	Az információbiztonságot veszélyeztető tényező következtében jelentkező személyi és tárgyi erőforrások biztonságának szükség szerinti kezelése a Katasztrófa- és polgári védelmi szabályzat/Tűzvédelmi szabályzat szerint	területi vezető
3.	Biztonsági eljárások, kárelhárítás (Katasztrófa- és polgári védelmi szabályzat, Tűzvédelmi szabályzattal összhangban) □ Szükség szerint a további információs rendszerek eltávolítása, veszélyes és veszélyessé váló területek kiürítése. □ Védelmi szakaszolások, elhatárolások. □ Szükség szerinti adatmentések. □ Szükség szerint külső felek azonnali tájékoztatása.	információ biztonsági felelős, informatikai igazgatóság munkatársa

4.	Kivizsgálás, elhárító intézkedések A folyamat leállítása után ki kell vizsgálni, hogy mekkora információbiztonság megsértésének hatása, egyedi intézkedések. Amennyiben az információbiztonság sérülése az intézet / campus/telephely kompetenciáján túlmutat, hatáskörének megfelelően az **intézetigazgató campus igazgató** értesíti az illetékes hatóságokat. Helyreállítási lépések.	információ biztonsági felelős, informatikai igazgatóság munkatársa
5.	A vészhelyzet feloldása, dokumentálás A vészhelyzet feloldását ugyanaz a személy rendelheti el, aki azt kezdeményezte, de csak abban az esetben, ha az információbiztonsági problémát megszüntették, és az elhárító intézkedés dokumentáltan megtörtént. A vizsgálat befejezésekor Megbízókönyv megírásával dokumentálni kell.	információ biztonsági felelős, informatikai igazgatóság munkatársa
6.	A vészhelyzet típusától függően bejelentés további külső szervek felé.	rektor / koordinációs főigazgató
7.	Helyreállítás, újraindítási feltételek és ezek meglétének ellenőrzése	rektor / koordinációs főigazgató, informatikai igazgató/ intézetigazgató

7. Helyreállítási lehetőségek

Veszély	Megoldás	Jellegzetes helyreállítási lehetőségek	Megjegyzések
Informatikai szempontból, üzletmenet folytonosság szempontjából kritikus helyiségek (pl. szerverszoba) megrongálódása vagy megközelíthetetlensége	Kisegítő helyiségek keresése és biztosítása. A helyreállítás gyorsabb, ha a helyiség előre el van látva árammal, telefonnal, és hálózati végponttal	A karon belüli, vagy kívüli megfelelő kisegítő helyiségek találása, és rendelkezésre állásuk figyelmen kísérése	Helyiségeket lehet felszabadítani, de valószínűleg fel kell szerelni őket, mielőtt használhatóak lesznek
		Kijelölt kisegítő helyiség az karon / csoporton belül	Az intézet felügyelete alatt megfelelően fel lehet szerelni előre
		Külső helyreállítási szolgáltatás: Mobil helyiségek	Megfelelő hozzáférést és elhelyezést igényel
		Külső helyreállítási szolgáltatás: Szolgáltató campus/telephelyén biztosított helyiségek	Az alkalmazottaknak a szolgáltató campus/telephelyére kell utazniuk
		Kisegítő egyezmény egy harmadik féllel	Harmadik félre is hatással van
		Otthonról dolgozó alkalmazottak	Kommunikációs nehézségek. Megvalósítható lehet, de csak rövidtávon.
		Rugalmas munkafolyamatok, vagyis a pótolhatatlan alkalmazottak elosztása több helyszínre	Költséges lehet

Számítógépes eszközök megsemmisülése, vagy végzetes meghibásodása	Csereeszközök keresése, és biztosítása, amelyek rövid idő alatt beszerezhetőek	Hardverek használata kevéssé fontos szervezeti folyamatokból	Más szervezeti folyamatokat is befolyásolhat
	A helyreállítás gyorsabb, ha a csereeszközt előre telepítik a megfelelő programokkal és kiegészítő eszközökkel, és ennél is gyorsabb, ha az adatokat is rendszeresen karbantartják rajtuk		
	Végül, ha az adatokat valós időben tükrözzük tartalék gépekre, akkor lehetséges a szinte azonnali helyreállítás		
Számítógép szoftver végzetes hibája	Eszközök, amelyek lehetővé teszik a munkafolyamatok alternatív módon való működtetését	Régebbi változatok mentése	Mentési példányokat védeni kell a szándékos károkozástól
		Visszatérés a manuális feldolgozásra a javítások elvégzéséig	Olyan kockázatcsökkentési módszerek, mint a szigorú tesztelés és az új szoftverek szakaszos feltöltése
Számítógépes rendszerek műszaki hibája	Gyors hibajavítás biztosítása, vagy ahol megszakítás nélküli működés szükséges, ott hibatűrő szerkezetek biztosítása	Helyi, vagy gyors reagálású karbantartó személyzet, pótalkatrészekkel és megfelelő szakértelemmel	Fenn áll a veszélye, hogy a helyreállítási célkitűzések nem teljesülnek. Fennáll a veszélye, hogy a szoftver vészhelyzeti javítása veszélyezteti a folyamatos üzemvitelt vagy a biztonságot
		Hibatűrő szerkezetek, úgymint több processzor és / vagy meghajtó	Költséges lehetőség, de megszakítás nélküli működést biztosít
		Szoftver mentése	Mentési példányokat védeni kell a szándékos károkozástól
Adatvesztés	Olyan rendszerességgel végzett mentések, ahogy azt az adatvesztésből eredő szervezeti hatás indokolja. A mentéseket védeni kell, és a működő példányoktól különböző helyen tárolni	Cserélhető adathordozó, mint a szalagos egység, hajlékonylemez, dobozos szalag, CD lemez	Idő szükséges az adatok visszatöltéséhez. Nem teljesen naprakész
		Távoli (naplózás/ elektronikus védelem	Költséges lehet, de gyors helyreállítást tesz lehetővé
		Valós idejű lemeztükrözés	Költséges lehetőség, korlátozva van a meghajtók közötti távolság, de szinte azonnali helyreállítást biztosít
Létfontosságú papír alapú iratok megsemmisülése	Biztosítani kell, hogy az adatok más módon is rendelkezésre álljanak	Másolat készítése, és külső tárolás	Költséges lehet
		Mikrofilm vagy dokumentum beolvasó használata	Költséges lehet, vagy nehézkes az alkalmazása
		Igényli a szállítók / harmadik felek adatduplikálását	Jelentős biztonsági kérdéseket vet fel
Kulcsfontosságú alkalmazottak elérhetetlensége	Kerülni kell a kulcsfontosságú alkalmazottaktól függést, és gondoskodni kell helyettesítő személyzetről	Hasonló szakterületű szakemberek továbbképzése	Naprakészen kell tartani

12 számú melléklet – KONTROLL ÉS FELÜLVIZSGÁLAT

1. Biztonsági rendszerek kontroll pontjai

A minimálisan szükséges kontroll pontok az alábbiak:

Mérendő terület	Mérendő mennyiség	Beszámolóban szerepel
IT tevékenység	Szerverszobába való belépések naplózása	-
	Hozzáférések (logikai) naplózása	-
Illegális informatikai tevékenység	Észlelt behatolási kísérletek száma	X
	Nem MATE dolgozó által végzett tevékenység teljes körű naplózása	-
Vírusvédelem	Beérkezett vírusok, SPAM-ek száma	X
	Hatástalanított vírusok és blokkolt SPAM-ek száma	X
	Nem Internetről beérkezett vírustámadások száma, ezek módja	X
Mentési rendszer	A teszt visszatöltések eredményei	X
Rendelkezésre állás	Rendszerek kieséseinek száma, ezek oka, időtartama, javítási költsége	X
Kapacitás információk	Kritikus rendszerekre vonatkozó teljesítményadatok jelentős változása	kivonat
	Tárolási kapacitásokra vonatkozó információk	X
Ellenőrzések eredményei	Feltárt hiányosságok, és azok megszüntetésére vonatkozó intézkedések	X
Oktatás helyzete	Az információbiztonsági oktatásban részt vett személyek száma, a beszámoltatás eredményei	X
Az információbiztonsággal kapcsolatos fegyelemsértések	Az információbiztonságot megsértő személyekre vonatkozó fegyelmi statisztikák	X
Az információbiztonsági rendszer összesített értékelése	Az informatikai rendszer technikai és biztonsági szintjére vonatkozó megállapítások, javaslatok	X
Javaslatok	Javaslatok kidolgozása a hiányosságok megszüntetésére, a biztonsági és rendelkezésre állási szint emelésére	X

2. Biztonsági rendszerek felülvizsgálata

A szükséges felülvizsgálatok és gyakoriságuk a következő:

A felülvizsgálat tárgya	A felülvizsgálat ciklikussága
Kockázatfelmérés	2 évente
IT biztonsági szabályzat	2 évente
IT biztonsági folyamatok	2 évente
Határvédelem	1 évente
Vírusvédelem	1 évente
Mentés, archiválási rend	1 évente
IT biztonsági oktatás	1 évente

13 számú melléklet – MENTÉSI MÉDIÁK ROTÁLÁSA, SELEJTEZÉSE

1. Mentési médiák újrahasznosítása, rotálása

A mentési adathordozókat, vagy az adathordozókon tárolt adatokat az alábbiak szerint kell rotálni:

Típus	Rotálási ciklus
Napi	7 nap
Heti	5 hét
Havi	1 év
Éves	5 év

2. Mentési médiák selejtezése, megsemmisítése

Az alábbi táblázat a mentési médiák számításba vehető maximális élettartamát tartalmazza. (Az egyes gyártók az itt megadott értékektől eltérhetnek. Amennyiben a gyártói előírások szigorúbbak, úgy azokat kell alkalmazni.)

Média	**Max. élettartam**
LTO-x	3 év
CD-R	5 év
CD-RW	5 év
DVD-R	5 év
DVD-RW	5 év

A maximális élettartamuk lejárta után az adathordozókat át kell másolni új adathordozóra, majd a régi adathordozót le kell selejtezni, és meg kell semmisíteni. Megsemmisítéskor az adathordozót fizikailag kell megsemmisíteni.

Az adathordozót le kell selejtezni akkor is, ha vélhetően az adathordozó hibája miatt az adatmentés sikertelen volt, illetve ha a katasztrófa vagy visszatöltési próbák során az adatvisszatöltés sikertelenné vált.

14 számú melléklet – HELPDESK ELÉRHETŐSÉGEI

A HelpDesk-re az incidenseket, problémákat be kell jelenteni:

a) Telefonon (Telefon szám:.....és .....és.....)

b) E-mail-ben (e-mail cím:

A HelpDesk a következő időszakokban érhető el közvetlenül:

c) Munkanapokon 08:00-17:00

A HelpDesk munkaidején kívül a következő telefonszámokon lehet incidenst bejelenteni:

d) Vagyonvédelmi incidenseket. telefon:.....

e) Informatikai incidenseket. telefon:.....és.....

f) Tűzvédelmi incidenseket. telefon:..... és tel: **112**

g) Téves riasztások törlése: telefon..... (azonosító használat kötelező)

h) Katasztrófa esetek: telefon..... és **tel: 112**

15 számú melléklet – FOGALOMTÁR

Adat: A Központos küldemények azon része, amelynek elektronikus eszköz az információ hordozója (pl.: floppy, e-mail üzenet a képernyőn), függetlenül attól, hogy az információ szöveges vagy számszerű.

Adatkezelés: Az adatok tárolásával, továbbításával, megsemmisítésével, nyilvántartásával és feldolgozásával kapcsolatos tevékenységek összessége.

Adatállomány: Valamely informatikai rendszerben lévő adatok logikai összefogása, amelyet egy névvel jelölnek. Ezen a néven keresztül lehet hozzáférni a rendszer által tartalmazott adatokhoz.

Adatgazda: Az ügyviteli, működési folyamatokhoz tartozó adatok kezeléséért felelős személy.

Adatátvitel: Elektronikus adatok szállítása összeköttetéseken, összekötő utakon keresztül. (Például számítógépek között hálózaton keresztül, e-mail-ben, Interneten.)

Adatbiztonság: Az adat bizalmasságának, integritásának és rendelkezésre állásának biztonságos megőrzése.

Adatbiztonsági szint: Az adat sértetlenségét és bizalmasságát jellemző minőségi (kvalitatív) osztályozás.

Adathordozó: Az adat tárolására és terjesztésére alkalmas eszköz.

Adatvédelemi szint: Az adat rendelkezésre állását jellemző minőségi (kvalitatív) osztályozás. Az osztályozás meghatározza, hogy a szóban forgó adat rendelkezésre állása milyen mértékben befolyásolja az általa érintett folyamatok végrehajtását, illetve a MATE tevékenységét tekintve mennyire fontos ügyviteli, működési folyamathoz tartozik.

Bekövetkezési valószínűség: Annak az esélye, hogy a veszélyforrás képezte fenyegetettség támadás formájában bekövetkezik.

Bizalmasság: A MATE ügyfeleire, illetve ügyletmenetére vonatkozó adatok védelme illetéktelen hozzáférés, illetve felhasználás ellen. Az információkhoz, adatokhoz csak az arra jogosítottak és csak az előírt módokon férhetnek hozzá. Ez vonatkozhat programokra, mint szélesebb értelemben vett információkra is. (Például, ha valamely eljárás előírásai egy programmal kerülnek leírásra, és azt szükséges titokban tartani.)

Biztonság: Az informatikával kapcsolatban, az informatikai rendszerekben olyan előírások és szabványok betartását jelenti, amelyek a rendszer működőképességét, az adatok rendelkezésre állását, sértetlenségét, bizalmasságát és hitelességét erősítik.

Biztonsági szint: A rendszerek megbízhatóságát és érzékenységét jellemző minőségi (kvalitatív) osztályozás. Ahol a megbízhatóság a rendszer azon jellemzője, amely megadja, hogy az üzemeltetési feltételek zavartalan fennállása esetén milyen mértékben várható el a hibátlan és rendeltetésszerű működés. Az érzékenység pedig meghatározza, hogy az adott rendszer elemei mennyire védettek és ellenállóak a különböző hatásokkal és károkozásokkal szemben.

Cselekvési (akció) terv: Egy meghatározott (káresemény bekövetkezése esetén végrehajtandó eljárásrend, amely tartalmazza a sebezhetőségi ablakot, a helyettesítő és visszaállítási feladatokat,

meghatározza a végrehajtásban érintett személyeket, csoportokat vagy szervezeti egységeket, valamint azok felelősségi- és jogkörét.

Dologi kár: A MATE eszközeiben, fizikai vagyontárgyaiban közvetlenül bekövetkező kár vagy veszteség.

Elektronikus aláírás: Személyek és/vagy digitális adatok hitelesítésére alkalmas módszer. Két részből áll: a személyhez kötött aláírást generáló részből, és az ellenőrzést bárki számára lehetővé tevő részből.

Esemény: A MATE rendszereiben előálló időleges kiesést vagy zavarokat, és akár - gazdasági, reputációs, személyi vagy dologi - kárt is okozó, illetve törvényi következményekkel járó történés.

Fenyegetettség: A MATE informatikai infrastruktúráját fenyegető azon veszélyforrások összessége, amelyek bekövetkezése esetén az informatikai rendszer nem tudja teljesíteni a vállalt rendelkezésre állást, akadályozva ezzel a normális üzemmenet folytonosságát, illetve az adatok sértetlensége és bizalmassága sérül.

Fenyegetettség-hatáselemzés: Az egyes informatikai szolgáltatásokkal kapcsolatban a kiesés lehetséges okainak, az egyes okok bekövetkezési valószínűségének felmérése. (A vizsgálatot követően lehetővé válik a kiesés legvalószínűbb okaival szemben a hatékony, célzott védekezés.)

Fenyegető tényező: Azon esemény, amelynek bekövetkezése közvetlenül vagy közvetve a kritikus informatikai szolgáltatások kiesését eredményezi.

Fizikai biztonság: Az erőforrások bizalmassága és sértetlensége, valamint rendelkezésre állása sérelmére bekövetkező szándékos vagy véletlen fizikai támadásokkal, veszélyforrásokkal szembeni védettség.

Fokozott készültségi szint: A napi működés során olyan, előre látható, tervezett esemény következik be, vagy tevékenység kerül végrehajtásra, amelynek magas kockázata miatt - ami adódhat a végrehajtás egyediségéből is - külön tervezés és felkészülés szükséges az esemény elhárításához vagy a tevékenység végrehajtásához, és esély van arra, hogy rossz esetben magas készültségi szintre kerülnek a folyamatok.

Gazdasági kár: Azt fejezi ki, hogy egy adott informatikai szolgáltatás bizonyos ideig tartó kiesése milyen közvetlenül is mérhető, pénzben kifejezhető veszteségeket okoz a MATE-nak (anyagi károk, kártérítések stb. formájában).

Helyreállítási eljárás: A vészhelyzetként értékelhető incidens bekövetkezése és az azt követő észlelése után végrehajtandó eljárásrend, amely biztosítja, hogy a sérült kritikus ügyviteli folyamat, vagy annak valamely alternatívája a sebezhetőségi ablakon belül a MATE által vállalt tevékenységi szinten működőképes.

Helyreállítási terv: A helyreállítási eljárásokat tartalmazó dokumentum

Hitelesség: A rendszerben kezelt adat bizonyíthatóan hiteles forrásból származik. (Az entitás olyan tulajdonsága, amely egy vagy több hozzá kapcsolódó tulajdonságot más entitás számára bizonyíthatóvá tesz.)

Információ: Egy adatküldemény tartalma, függetlenül az információ hordozójától.

Informatikai infrastruktúrájára: A szerverek, kliensek, nyomtatók, rack-szekrények, számítógépes vezetékes illetve vezeték nélküli hálózatok, hálózati aktív eszközök, szünetmentes áramforrások, stb. összességét jelenti.

Informatikai katasztrófa: Az informatikai szolgáltatások olyan kiesése, amelynek következtében megszakad a MATE informatikai rendszerének folyamatos és rendeltetésszerű működése, és ez jelentős hatást gyakorol a normál ügyviteli, ill. működési tevékenységek folyamatosságára és működőképességére.

Informatikai rendszerelemek: Olyan tárgyak, eszközök, programok, adatok, adathordozók, dokumentumok és az informatikai rendszerekkel kapcsolatba kerülő kezelő, üzemeltető, kiszolgáló, karbantartó és felhasználó személyek összességét foglalja magában.

Informatikai vészhelyzet: Az állapot, amikor az informatikai rendszer utolsó működőképes állapotát az üzemeltetési szabályok előírásszerű betartásával és végrehajtásával, a meghatározott erőforrások felhasználásával, a megállapított helyreállítási időn belül, nem lehet visszaállítani.

IT erőforrások: Az ügyviteli folyamatok működéséhez nélkülözhetetlen elektronikus adatok, informatikai alkalmazások, technológiai eszközök, környezeti infrastruktúra és humán erőforrások összessége.

Katasztrófahelyzet kezelés tervezése: A káreseményeknek az informatikai rendszerek kritikus elemeire vonatkozó hatásait elemzi és tervet ad olyan globális helyettesítő megoldásokra, valamint megelőző és elhárító intézkedésekre, amelyekkel a bekövetkezett káresemény után az informatikai rendszer funkcionalitása eredeti állapotában visszaállítható. (DRP - Disaster Recovery Plan)

Kockázat: Annak veszélye, hogy egy esemény, fenyegetettség bekövetkezése vagy intézkedés hátrányosan befolyásolja a MATE lehetőségeit céljainak és stratégiájának megvalósítása során.

Kockázattal arányos védelem: A lehetséges védelmi intézkedések olyan hatékony alkalmazása, amikor egy kellően nagy időintervallumban a védelem költségei arányosak a potenciális kárértékekkel.

Kockázatelemzés: Az információs folyamatokra és az adatra hatással lévő veszélyek felbecsülése. A kockázatfelmérés és kockázatfelbecsülés általános folyamata.

Kritikus ügyviteli folyamat: A MATE azon ügyviteli folyamata, amely működőképességének fenntartása elengedhetetlen a MATE stratégiai céljainak elérése, teljesíthetősége érdekében.

Kritikus kiesési idő: Az az időszak, amely egy adott informatikai szolgáltatás nyújtásának akadályoztatását jelenti és az adatvédelmi tisztviselőnek még nem szükséges semmilyen lépést tennie az alternatív működés elrendelésére.

Kritikus üzemmeneti szint: A kritikus ügyviteli folyamatok működése megszakadt oly módon, hogy a probléma a folyamatot működtetők, illetve az informatikai üzemeltetés hatáskörében közvetlenül, a folyamat működésének — a sebezhetőségi ablakban meghatározott értéknél - hosszabb szüneteltetése nélkül, nem megoldható. A kritikus üzemmeneti szint esetén az elhárítást külön e célra létrehozott szervezet - Krízis Bizottság - szervezi, aki jogosult az intézkedések végrehajtásához szükséges döntéseket meghozni.

Krízisállapot/Krízishelyzet: Az az állapot, amely a folytonosságot biztosító intézkedésekhez kapcsolódó cselekvési tervekben nem definiált, illetve amelyek esetében a kapcsolódó cselekvési terv nem alkalmazható. Krízishelyzetnek tekintendő minden olyan eset, amikor a normál üzemmenet nem folytatható. (A krízishelyzet addig tart, amíg a normál üzemmenet nem indul el, így akkor és csak akkor vonható vissza a BCP (Business Continuity Plan - Üzletmenet Folytonossági terv) eljárásrend hatálya, illetve oszolhat fel a Krízis Bizottság.)

Maximális kiesési idő: Azon időintervallum, amelyen belül a kiesést szenvedett kritikus informatikai szolgáltatást a helyreállítási/visszaállítási eljárás végrehajtásának eredményeként ismételten működővé kell tenni, mert ellenkező esetben a MATE már nem elviselhető károkat szenvedne.

Megelőző védelem: Azon technikai, szervezeti és adminisztratív intézkedések halmaza, amelyek célja a fenyegető tényezőkből fakadó események/katasztrófaesemények bekövetkezését megelőzni, vagy annak esélyét csökkenteni, valamint a helyettesítő folyamat beindítását lehetővé tenni.

Minimális szolgáltatás: A MATE ügyviteli folyamatai közül azon előre definiált, belső szabályzatban rögzített tevékenységek, amelyeket az adott szervezeti egységnek akkor is nyújtania kell, ha üzemzavar, krízishelyzet áll elő.

Normál üzemmenet szint: A napi működés során nem történik rendkívüli helyzet, az informatikai rendszerekbe épített belső ellenőrző funkciók hibát nem jeleznek, az ügyfelek és a felhasználók nem tapasztalnak a MATE szolgáltatásaival kapcsolatos rendellenességet. Normál üzemi állapotnak tekintett az az eset is, ha az ügyfél a saját üzemeltetésében lévő informatikai rendszer meghibásodása miatt nem képes igénybe venni a MATE szolgáltatásait. A normál üzemmenet esetén az FH és a megyei/fővárosi munkaügyi központok Szervezeti és Működési Szabályzataiban rögzített hatás- és jogkörök érvényesek, külön intézkedésre, beavatkozásra, hatáskör túllépésre nincs szükség.

Rendelkezésre állás: Az a tényleges állapot, amikor az informatikai rendszer eredeti rendeltetésének megfelelő szolgáltatásokat - amely szolgáltatások különbözők lehetnek - nyújtani tudja (funkcionalitás) meghatározott helyen és időben (elérhetőség), és a rendszer működőképessége sem átmenetileg, sem pedig tartósan nincs akadályozva. Ebben az összefüggésben jelentősége van az információ vagy adatok rendelkezésre állásának, elérhetőségének is.

Rendszer-monitorozó eszközök: Az egész informatikai, ill. információs rendszerről, vagy valamilyen csoportosító szempont szerint a rendszer egyes részeiről gyűjtenek folyamatos információkat.

Reputációs (társadalmi, image) kár: A MATE megbízhatóságába, hitelességébe, illetve a MATE által nyújtott szolgáltatásokba vetett hit szempontjából mérhető hatások.

Sebezhetőségi ablak: Azon időtartam, amely alatt a helyettesítő megoldás fenntartható az ügyviteli tevékenységek és a törvény által előírt jogi kötelezettségek komolyabb sérülése nélkül. Az adott informatikai szolgáltatás megszakadását követő időtartam, amelyet normális működési rendjének és tevékenységének megszakadása nélkül képes a MATE elviselni.

Sértetlenség (integritás): Az adatok eredeti állapotának, tartalmának, teljességének és hitelességének biztosítása. Az információkat, adatokat, alkalmazásokat csak az arra jogosultak változtathatják meg, és azok véletlenül sem módosulhatnak. (A sértetlenséget általában az információkra, adatokra, illetve alkalmazásokra is értelmezik, mivel az adatok sértetlenségét csak rendeltetésszerű feldolgozás és átvitel esetén lehet biztosítani.)

Személyi kár: A MATE alkalmazottainak testi épségét, egészségét érintő hatás, következmény.

Szoftverek: A rendszerprogramok, segédprogramok, alkalmazások, adatbázis kezelők, fejlesztő eszközök, operációs rendszerek, firmware-ek, stb. összessége.

Tesztelés: A kialakított üzemmenet folytonossági cselekvési tervek gyakorlati értékelése; a megfogalmazott felkészülési, helyettesítési és helyreállítási tevékenységek szükségességének és megfelelőségének vizsgálata, a szabályozás bármilyen hiányosságának feltárása, az üzemmenet

folytonossági tevékenységek alapját adó (informatikai) helyreállítási eljárások vizsgálata, illetve a külső partnerekkel kötött egyezmények betartásának és használhatóságának vizsgálata.

Teszt-környezet: Az informatikai rendszer azon elkülönített része, amelyben az éles üzembe állítás előtti tesztelések az éles környezethez hasonló körülmények között történnek.

Törvényi következmények: Az esetleges jogi következmények, amelyek egy adott informatikai szolgáltatás kieséséből következhetnek.

Türelmi idő: Az az időszak, amely egy adott informatikai szolgáltatás nyújtásának akadályoztatását jelenti és az adatvédelmi tisztviselőnek még nem szükséges semmilyen lépést tennie az alternatív működés elrendelésére.

Ügyviteli folyamat: Olyan tevékenységek összessége, amelyek szükségesek, hogy a MATE kifejtse szervezeti működését és megvalósítsa oktatási, kutatási, stb. feladatait. (Egy MATE-os szolgáltatás nyújtásához szükséges tevékenységek, feladatok összessége.)

Üzemmenet folytonosság: A MATE zavartalan működését, az ügyviteli folyamatokat támogató - elsősorban informatikai, de emellett telekommunikációs, emberi és infrastrukturális - erőforrások egy hosszabb időn át folyamatosan, megszakítás nélkül üzemelnek, illetve a megkívánt mértékben és funkcionalitási szinten rendelkezésre állnak.

Vészhelyzeti esemény: Azon esemény, amelynek bekövetkezése krízishelyzetet teremt. A vészhelyzeti eseménynek több, egymástól független, vagy egymással összefüggő oka lehet. Az okok azon releváns fenyegető tényezők, amelyek az adott esemény kiváltásához vezetnek különböző valószínűségekkel. A normál ügyvitelre történő visszaállás várható határideje meghaladja az üzemzavarnál leírtakat, illetve a probléma nem csupán a MATE tevékenységeinek egyes elemeit, részlegeit érinti, hanem a MATE ügyviteli tevékenységének jelentős körénél problémát okoz.

Vészhelyzet kezelés tervezése: A káreseményeknek az informatikai rendszerek kritikus elemeire vonatkozó hatásait elemzi és tervet ad olyan globális helyettesítő megoldásokra, valamint megelőző és elhárító intézkedésekre, amelyekkel a bekövetkezett káresemény után az informatikai rendszer funkcionalitása eredeti állapotában visszaállítható (DRP - Disaster Recovery Plan).

Visszaállítási eljárás: Az az eljárásrend, amelynek részeként elvégzett tevékenységek, feladatok biztosítják, hogy a helyreállítási eljárással beindított kritikus informatikai szolgáltatás alternatívájáról az ügyviteli folyamat visszaáll a normál üzemmenetre.