MOHOLY-NAGY MŰVÉSZETI EGYETEM
MOHOLY-NAGY UNIVERSITY OF ART AND DESIGN BUDAPEST

Hatály: 2016. IX. 27-

A MOHOLY-NAGY MŰVÉSZETI EGYETEM

INFORMATIKAI RENDSZEREK ÉS ADATOK BIZTONSÁGOS KEZELÉSÉNEK, ÜZEMELTETÉSÉNEK ÉS HASZNÁLATÁNAK RENDJÉRŐL SZÓLÓ SZABÁLYZATA

2015.

Tartalomjegyzék

I. Általános rendelkezések

A szabályzat célja

1. §

(1) Jelen szabályzat (a továbbiakban: Szabályzat) célja, hogy a Moholy-Nagy Művészeti Egyetem (a továbbiakban: Egyetem) feladatait, valamint informatikai rendszerének sajátosságait figyelembe véve, a vonatkozó jogszabályoknak megfelelően szabályozza az informatikai adatok és rendszerek biztonságos kezelésének, üzemeltetésének és használatának rendjét.

(2) A szabályzat alapvető célja, hogy az Egyetemen elérhető szolgáltatások használata, alkalmazása során biztosítsa az adatvédelem alkotmányos elveinek, az adatbiztonság követelményeinek érvényesülését, és megakadályozza a jogosulatlan hozzáférést, az adatok megváltoztatását és jogosulatlan nyilvánosságra hozatalát. A Szabályzatnak elő kell segítenie, mozdítania az informatikai és kommunikációs eszközök (a továbbiakban: Informatikai rendszer) előírásoknak megfelelő és biztonságos használatát, ezzel támogatva, hogy az Egyetem által kezelt információvagyon sértetlensége, bizalmassága és rendelkezésre állása biztosított legyen.

(3) A Szabályzat megalkotásával és hatálybaléptetésével elérni kívánt cél továbbá elősegíteni az informatikai biztonsággal összefüggő szabályok és intézkedések egységes értelmezését. Kialakítani azokat az alapvető informatikai biztonsági normákat és működési kereteket, amelyek érvényesítésével a minimumra csökkenthetők az adat- és információkezelés kockázatai.

A szabályzat hatálya

2. §

(1) A Szabályzat személyi hatálya kiterjed az Egyetem valamennyi szervezeti egységére és dolgozójára, valamennyi hallgatójára. Jelen Szabályzat hatálya kiterjed továbbá az Egyetem hálózatát használó felhasználókra és rendszergazdákra.

(2) A Szabályzat tárgyi hatálya kiterjed az Informatikai rendszer teljes infrastruktúrájára, azaz a fizikai, infrastrukturális eszközökön kívül az adatok, szoftverek teljes körére, a folyamatokra, valamennyi telephelyre és a létesítményekre is. Felhasználónak minősülnek az Egyetem foglalkoztatottjai, hallgatói, illetve mindazok, akik oktatási, kutatási, tudományos, adminisztrációs és egyéb feladataikhoz állandó vagy eseti jelleggel vagy szerződés alapján az Egyetem hálózatát használják. Az egyetemi hálózat vonatkozásában az oktatók, a rendszergazdák, a hallgatók, és a felhasználók más csoportjai különböző jogosultságokkal és kötelezettségekkel rendelkezhetnek.

Kötelező felülvizsgálat időpontja

3. §

A Szabályzatot minden alkalommal felül kell vizsgálni, ha a hatályos jogszabályok pénzeszközök kezelésére vonatkozó rendelkezései módosulnak vagy az Egyetem tevékenységében olyan feladatváltozás történik, mely megkívánja a tárgyat érintő belső rendelkezések korrekcióját.

II. Kapcsolódó fontosabb jogszabályok

Kapcsolat a magasabb szintű jogszabályokkal

4. §

A jelen szabályzat az adatvédelem és az informatikai szabályozásának egyetemi szintjét valósítja meg. A Szabályzatban található intézkedéseken túl a magasabb szintű jogi szabályozást is figyelembe kell venni.

Fontosabb jogszabályok

5. §

A vonatkozó jogszabályok az alábbiak:

- 1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról,
- 1992. évi LXVI. törvény a polgárok személyi adatainak és lakcímének nyilvántartásáról,
- 1995. évi LXV. törvény az államtitokról és a szolgálati titokról,
- 3/1988. (XI.22.) KSH rendelkezés az államtitok és szolgálati titok számítástechnikai védelméről
- 79/1995. (VI. 30.) Korm. rendelet a minősített adat kezelésének rendjéről,
- 2001. évi XXXV. törvény az elektronikus aláírásról,
- ITB 12. ajánlása az Informatikai Rendszerek Biztonsági követelményeiről.

III. Értelmező rendelkezések

Alapfogalmak

6. §

1. **AD (Acive Directory)**: A Microsoft egyes hálózati szolgáltatásainak gyűjtőneve.
2. **Adatbiztonság**: Az adatok jogosulatlan megszerzése, módosítása és tönkretétele elleni műszaki és szervezési intézkedések és eljárások együttes rendszere.
3. **Adatfeldolgozás**: Az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől, feltéve hogy a technikai feladatot az adatokon végzik.
4. **Adatfeldolgozó**: Az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely az adatkezelővel kötött szerződése alapján - beleértve a jogszabály rendelkezése alapján történő szerződéskötést is - adatok feldolgozását végzi.

5. **Adatfelelős**: Az a közfeladatot ellátó szerv, amely az elektronikus úton kötelezően közzéteendő közérdekű adatot előállította, illetve amelynek a működése során ez az adat keletkezett.
6. **Adatgazda**: Felelős az általa kezelt adatokért, továbbá jogosult minősítés vagy osztályba sorolás elvégzésére.
7. **Adatkezelés**: Az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők rögzítése.
8. **Adatkezelő**: Az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely önállóan vagy másokkal együtt az adatok kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az általa megbízott adatfeldolgozóval végrehajtatja.
9. **Aktív hálózati eszköz**: Kapcsolók (switch-ek), forgalomirányítók (router-ek), vezeték nélküli hozzáférési pontok (Acces Pointok) és egyéb eszközök, amelyek segítségével a hálózat üzemvitele biztosítható (bridge-ek, tűzfalak).
10. **Asztali munkaállomás**: A felhasználó rendelkezésére bocsátott számítástechnikai eszköz, mely alapvetően a számítógépből, monitorból, billentyűzetből és egérből, illetve más csatlakoztatható számítástechnikai eszközökből (különösen: mikrofon, kamera, scanner, stb.) állhat.
11. **Bizalmasság**: Az információ azon jellemzője, hogy csak egy előre meghatározott felhasználói kör (jogosultak) részére hozzáférhető, mindenki más számára titok. A bizalmasság elvesztését felfedésnek nevezzük, mely esetén a bizalmas információ arra jogosulatlanok számára is ismertté, hozzáférhetővé válik.
12. **Biztonság**: Az informatikai rendszerekben olyan előírások és szabványok betartását jelenti, amelyek a rendszer működőképességét, az információk rendelkezésre állását, sértetlenségét, bizalmasságát és hitelességét erősítik.
13. **BYOD (Bring Your Own Device – BYOD):** Saját mobileszközök (különösen: notebookok, tabletek, okos telefonok) munkahelyi környezetben való használata.
14. **Csomópont**: Szerver feladatokat ellátó eszközök és aktív eszközök csoportja az informatikai szolgáltatások ellátására.
15. **Domain név**: Tartománynév (műszaki azonosító), amelyet elsősorban a könnyebb megjegyezhetősége miatt, az internetes kommunikációhoz nélkülözhetetlen Internet cím tartományok (IP címek) helyett használnak. Az Internet egy meghatározott részét, tartományát egyedileg leíró megnevezés, a számítógépek (kiszolgálók) azonosítására szolgáló névtartomány.
16. **DNS (Domain Name System)**: Az internet neveket és címeket egymáshoz rendelő adatbázis, amely általában külön kiszolgáló gépen fut.

17. **EHA kód**: Az ETR rendszer szolgáltatásaihoz hozzáférést biztosító betűkből és számokból álló felhasználói azonosító.
18. **Felhasználó**: Az a természetes személy, aki az egyetemi informatikai infrastruktúrát használja.
19. **Felhasználói azonosító**: Az intézményi címtárban tárolt egyedi azonosításra szolgáló rövid karaktersorozat, amely általában a felhasználó nevéből képződik.
20. **Felhőszolgáltatás, felhőszolgáltató** (angolul "cloud computing")**:** A feladatvégzéshez használt adatállományok, programok, szolgáltatások, stb. fizikailag nem a felhasználó számítógépén, hanem az interneten, egy szolgáltatónál (ún. szerver farmon, valahol a "felhőben") találhatók. Az adatok (e-mailek, címjegyzékek, naptárbejegyzések, és kedvenc linkek) felhőben való tárolásának egyik legnagyobb előnye, hogy bárhonnan könnyen elérhetők, és akkor sem vesznek el, ha a felhasználó számítógépe tönkremegy. Ez egyben a felhőszolgáltatás hátránya is: mivel nem tudható pontosan hol tárolják a fájlt, a felhasználók nem lehetnek biztosak afelől, hogy adataik mindig épségben, hozzáférhetők fognak maradni vagy, hogy illetéktelenek nem férnek hozzá. Éppen ezért a biztonsági kérdések figyelembevételével a felhőszolgáltatás igénybevétele nagyrészt bizalmi kérdés is.
21. **Hálózat**: Felhasználói számítógépek és/vagy szerverek közötti adatátvitelt biztosító passzív és aktív eszközökből álló infrastruktúra.
22. **Hálózati rendszergazda**: Az egyes kampuszokon, a teljes Egyetem vagy egy-egy kampusz számára szolgáltató szerverek, valamint a hálózati hardverrendszer hardver és szoftver üzemeltetői.
23. **Hitelesség**: Az információ akkor hiteles, ha az elvárt, hozzáértő, megbízható forrásból származik.
24. **Informatikai erőforrások**: A hardver, szoftver eszközök összessége.
25. **Internet**: A világháló.
26. **Intranet**: Az intézményen belüli hálózat és annak szolgáltatásai.
27. **IP telefónia**: Olyan számítógép-hálózati alkalmazás, amely dedikált eszközök (készülék és központ, számítógépes hálózat) segítségével telefonszolgáltatást tesz lehetővé, ez a hagyományos telefonközpontokat felváltó számítógépes rendszer.
28. **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.

29. **Közérdekből nyilvános adat**: A közérdekű adat fogalma alá nem tartozó minden olyan adat, amelynek nyilvánosságra hozatalát, megismerhetőségét vagy hozzáférhetővé tételét törvény közérdekből elrendeli.
30. **Központi címtár**: Az Egyetem dolgozóinak felhasználói adatait tároló AD adatbázis.
31. **Központi szolgáltatások**: Levelezés, címtár, fájl kiszolgálás, web szolgáltatás, névszolgáltatás, és más informatikai és kommunikációs szolgáltatások.
32. **LDAP (Light Weight Directory Access Protocol**): Nyílt szabványú címtár struktúra leíró nyelv.
33. **Mobil eszközök**: Notebook, netbook, tablet, palmtop, okostelefon.
34. **NIIFI (Nemzeti Információs Infrastruktúra Fejlesztési Intézet)**: Az Intézet a teljes magyarországi kutatási, felsőoktatási és közgyűjteményi közösség számára biztosít integrált országos számítógép-hálózati infrastruktúrát, valamint erre épülő kommunikációs, információs és kooperációs szolgáltatásokat, élvonalbeli alkalmazási környezetet, és tartalom-generálási illetve tartalom-elérési hátteret.
35. **Okostelefon**: Internetezésre és/vagy dokumentumkezelésre is használható mobil telefon.
36. **Passzív eszközök**: Hálózati kábelezés és csatlakozók.
37. **Rendelkezésre állás**: Annak biztosítása, hogy a szükséges információ a szükséges időben az arra jogosultak számára meghatározott formában hozzáférhető, elérhető legyen.
38. **Sértetlenség**: Az információ létének, hitelességének, épségének, önmagában teljességének kritériuma.
39. **Social engineering**: Megtévesztés, az emberek bizalomra való hajlamának manipulatív kihasználása, információgyűjtés számítógépes rendszerekbe történő behatolás érdekében.
40. **Számítógép**: Olyan informatikai eszköz, amelyet a felhasználó a napi munkája során használ, és amellyel igénybe veheti a hálózat szolgáltatásait.
41. **Szerver-feladatokat ellátó eszköz**: Olyan számítógépek, szoftverek, vagy speciális eszközök, amelyek különböző szolgáltatásokat biztosítanak más számítógépek, felhasználók számára.
42. **Szerverhelyiség**: Fokozottan védett, naplózott bejutású, klimatizált, zárt helyiség, ahol a folyamatos működés feltételei az informatikai erőforrások számára biztosítottak.
43. **Szervezeti rendszergazda**: Az egyes egyetemi szervezetek felügyeletében lévő számítógép adminisztrátora.
44. **Titkosítás (encrypting)**: A titkosítás az adatok konvertálása egy speciális formátumba (ciphertext), amely nem értelmezhető az arra nem jogosult személyek számára. A visszafejtés (dekriptálás) az a folyamat, amely során a titkosított adatokat az eredeti formátumukra hozzuk, s így azok értelmezhetőek.
45. **Tűzfal**: Olyan kiszolgáló eszköz (számítógép vagy program), amelyet a lokális és a külső hálózat közé, a csatlakozási pontra telepítenek, annak érdekében, hogy az

illetéktelen behatolásoknak ezzel is elejét vegyék. Ezzel együtt lehetővé teszi a kifelé irányuló forgalom, tartalom ellenőrzését is.

46. **VLAN**: A hálózat egy – a feladatoknak megfelelő, logikailag elkülönülő – meghatározott része. A VLAN-ok biztonsági feladatot is ellátnak, mivel elválasztják egymástól a részhálózatokat, ezzel biztosítva, hogy sérülés, vagy támadás esetén csak az adott részterületre korlátozódjék az esetleges kár.
47. **VPN szolgáltatás**: Speciális hálózati elérés, amely az Egyetem hálózatához titkosított, és hitelesített kapcsolatot tesz lehetővé a világ bármely részéről.
48. **WEB adminisztrátor**: Az Egyetem web szerverét működtető, az Egyetem honlapjának felügyeletét ellátó személyek. A web-es adat- és tartalomszolgáltatást az Egyetem szerveiből kijelölt felelősök végzik.
49. **WiFi (Wireless Fidelity), WLAN**: Szabványos vezeték nélküli adatátviteli technika. A szabad frekvenciatartományt használó rendszer átviteli sebessége nagymértékben függ a rádióhullámok terjedési környezetétől (akadályok, távolság). A legtöbb notebook, laptop, palmtop számítógép, okostelefon gyárilag rendelkezik ilyen kapcsolódási lehetőséggel.

IV. Általános biztonsági előírások

A hálózati biztonság rendje

7. §

(1) Cél az Egyetem belső hálózatán (beleértve a vezeték nélküli hálózatokat is) továbbított adatok biztonságának megóvása és a hálózati infrastruktúra számára megfelelő biztonsági szint meghatározása, az Egyetemen belüli publikus hozzáférési pontok hálózati szabályozásának megvalósítása.

(2) Vonatkozik az Egyetem dolgozóira, szerződéses partnereire vagy egyéb személyre, aki az Egyetem hálózatait igénybe veszi (beleértve az Egyetemre érkező vendég felhasználókat, illetve a publikusan használható munkaállomások Egyetemhez és ahhoz nem tartozó felhasználóit).

(3) Tartalma:

a) A biztonsági kérdéseket kulcsfontosságúként kell kezelni minden hálózattervezési tevékenység során.
b) Az egyetemi fő-domain: mome.hu
c) A belső IP (InternetProtokoll) címek tekintetében alhálózatokhoz dedikált DHCP (DinamikusKilensCímProtokoll) szerverek osztják a kliens gépek számára meghatározott konfigurációnak megfelelően az IP címeket. Ezen IP címekkel és a gépnevekkel azonosítjuk a kliensgépeket. A kiemelt szerepkörű gépek, kiszolgálók (szerverek, hálózati erőforrások, nyomtatók, adminisztrátori gépek, hálózati aktív eszközök, routerek) állandó saját IP címmel rendelkeznek.
d) A nem szeparált hálózati megoldásokat el kell kerülni. E célból bizalmassági besorolások alapján (pl. éles üzemi, teszt) a hálózatot szeparált logikai zónákra kell felosztani.

e) Megfelelő szűrőkkel kell biztosítani, hogy a zónák között csak jóváhagyott hálózati forgalom haladhasson át.
f) A külső hálózatok felől a belső hálózatra irányuló kapcsolatokat átjárókkal, tűzfalakkal kell kontrollálni, megszűrve a nem engedélyezett hálózati forgalmat.
g) Külső – nem megbízható hálózatokból – a belső hálózat közvetlen elérése nem engedélyezett.
h) Megfelelő intézkedéseket kell hozni az információk bizalmasságának, sértetlenségének és rendelkezésre állásának biztosítása érdekében.
i) Gondoskodni kell a vezeték nélküli (WiFi) hálózatok hozzáférhetőségének szabályozásáról, valamint szükség esetén annak titkosításáról. A titkosítatlan hálózatok esetén (publikusan szabadon használható vezeték nélküli hálózatok) hardveres és szoftveres forgalom szabályozást kell alkalmazni, valamint az esetleges belső hálózati csatlakozási pontokon a lehető legmagasabb biztonsági szintű védelmet kell alkalmazni.
j) A hálózati felépítést és konfigurációt dokumentálni kell, és megfelelően karban kell tartani, a teljes hálózat üzemeltetése a Campus Igazgatóság (továbbiakban: CI) feladata.

A biztonsági osztályok meghatározása

7/A. §[1]

(1) Az Egyetem adatainak vonatkozásában négy biztonsági osztályt kell létrehozni, az információkat, adatokat, ezen biztonsági osztályokba kell besorolni valamint a Kancellári Utasításban meghatározott követelményeknek megfelelően kell kezelni.

(2) Biztonsági osztályok:

a) a) „Nyílt" – jogszabályok által nem védett adatok. Ide tartoznak Infotv.-ben foglaltak szerinti közérdekű adatok.
b) b) „Alap" – védendő, belső használatra szolgáló adatok (pl. belső levelezés, ügyiratok, feljegyzések.
c) c) „Fokozott" – adatok, ide tartoznak az Infotv. szerinti személyes adatok, a statisztikáról szóló 1993. évi XLVI. törvény 17. §-a szerinti egyedi adatok, valamint az Egyetem működésére vonatkozó nem közérdekű adatok.
d) d) „Kiemelt" – a Titoktörvény hatálya alá tartozó adatok.

(3) Az Egyetemen üzemeltetett informatikai rendszerek az 1. számú melléklet szerinti információvédelmi biztonsági osztályokba tartoznak.

A Hálózat eszközeinek kezelési rendje

8. §

(1) Cél a CI által üzemeltetett hálózati eszközök kezelési folyamatának meghatározása, a módosítások jóváhagyási folyamatának definiálása. A jogosulatlan, vagy előzetesen megfelelő vezetői szint által jóvá nem hagyott változtatások megakadályozása.

[1] A §-t és a megelőző alcímet beiktatta a 39/2016. (IX. 26.) Határozat.

(2) Ennek hatálya kiterjed minden CI által üzemeltetett hálózati eszközre, melyek a belső informatikai hálózatot vlan-okra, zónákra osztják, illetve a belső hálózatot a külső – nem megbízható – hálózattól elválasztják.

(3) Területi hatálya, az Egyetem valamennyi telephelyére kiterjed.

(4) A CI üzemelteti az Egyetem belső hálózatának hálózati eszközeit. A hatályos jogszabályokhoz és jelen Szabályzathoz igazodva fejleszti a CI a rendelkezésre álló erőforrásokból mind a passzív elemeket, mind az aktív eszközöket.

(5) A hálózati eszközök szolgáltatják az informatikai szolgáltatások működéséhez szükséges alap infrastruktúrát. Mint az informatikai rendszerek kommunikációs alapinfrastruktúrája, biztosítani kell a hálózati eszközök biztonságos, nagy rendelkezésre-állású üzemeltetését. Biztosítani kell, hogy az üzemeltetés során, a hálózati eszközökön csak jóváhagyott változtatások kerüljenek végrehajtásra.

(6) Ezen belül a CI-nek kiemelten kell kezelni az alábbi folyamatokat:

a) Felügyelni a hálózati eszközök kezelésének folyamatát.
b) A hálózati eszközökben történő változások, események függvényében, a szabályzat hatálya alá tartozó eszközök körét módosítani.
c) Évente felülvizsgálni a szabályzatot, szükség esetén javaslatot tenni annak módosítására.
d) Elkészíteni és aktualizálni a rendszerek nyilvántartását.
e) Rendszeresen felülvizsgálni az eszközök beállításait, szükség esetén javaslatokat tenni azok módosítására, majd elvégezni a szükséges beállításokat.
f) A beérkezett igények alapján elvégezni az új szolgáltatások funkcionalitásának biztosításához szükséges hálózati beállítások tervezését és kivitelezését.
g) Elvégezni az eszközök konfigurációjának mentését.
h) Elvégezni az eszközök szoftververzióinak rendszeres frissítését, a gyártók által kiadott javítócsomagok rendszeres telepítését, a nyilvánosságra került biztonsági hiányosságok kihasználásából eredő kockázat minimalizálása.
i) A rendszergazdákon kívül az összes többi hálózati felhasználónak tilos a hálózat szkennelése, tiltott szervizek/portok használata, a hálózati eszközök management rendszereinek támadása, valamint bárminemű támadás jellegű hálózati forgalom generálása.

Javítócsomagok (Patch) kezelése, szoftver javítások rendje

9. §

(1) Cél annak biztosítása, hogy a biztonsági és rendszerprogram javítások megfelelő időben alkalmazásra kerülnek, mind

a) Operációs rendszer,
b) Adatbázis,
c) alkalmazások

szinten.

(2) Annak biztosítása, hogy az üzleti alkalmazások javításai kontrollált környezetben kerülnek alkalmazásra.

(3) Vonatkozik az Egyetem rendszereinek üzemeltetőire (CI és más üzemeltetői területek) és szoftver beszállítóira.

(4) Az Egyetem a következő technikai szinteket különíti el az egyes alkalmazásokon belül:

a) Operációs rendszer szintű javítások:

Alacsony kockázatú rendszerek esetén a megjelenő javításokat azonnal alkalmazni kell.
Közepes kockázatú rendszerek esetén a javításokat akkor kell alkalmazni, ha azok az alacsony kockázatú rendszereken egy hónapos időszak alatt sikeresen tesztelve lettek.
Magas kockázatú rendszerek esetén a javításokat akkor kell alkalmazni, ha azok közepes kockázatú rendszereken egy hónapos időszak alatt sikeresen tesztelve lettek.

b) Adatbázis szintű javítások:

Alacsony kockázatú rendszerek esetében a javításokat automatikusan alkalmazni kell.
Közepes és magas kockázatú rendszerek esetében csak azok a javítások alkalmazhatók, amelyeket a vonatkozó Szállító(k) elfogadtak.

c) Alkalmazás szintű javítások:

Csak Szállító által kifejlesztett, tesztelt és elfogadott javítások telepíthetőek.

Új fejlesztések vagy üzleti alkalmazásra vonatkozó változtatások:

A Szállító felelőssége a „Fejlesztési procedúra" „Rendszer Teszt" fázisának betartása oly módon, hogy a legalább egy hónappal azelőtti összes kiadott javítással együtt működjön az alkalmazás. Biztosítani kell, hogy a javítások lehetséges következményeit tekintetbe vegyék a fejlesztési folyamatban, valamint hogy a javítások telepítésének hiányából fakadó kockázatok minimalizálva legyenek.

Internet hozzáférésre vonatkozó szabályok

10. §

(1) Alapvető elvárás biztonságos keretekbe foglalni az egyetemi internet-használatot, a hozzáférés teljes kontrollálása mellett.

(2) Az internet hozzáférés alapvető biztonsági szabályai:

a) Az Egyetem rendszereiből a hálózati belső forgalmat és az Internet hozzáférést menedzselhető berendezések biztosítják. A központi tűzfal szerepét Juniper SSG350 hardveres tűzfal látja el.
b) Definiálni kell az alkalmazottak számára az engedélyezett Internet szolgáltatások listáját.
c) Az Egyetemi rendszerek közvetlen elérése az Internet irányából hardveres tűzfal szabályozásával megvalósított.
d) Engedélyezett szolgáltatások a belső hálózat irányából internet felé (alapértelmezett csoportokra): DNS –névfeloldás- (Egyetemi és szolgáltatói szerverre), http –internet böngészés-, HTTPS –titkosított internet böngészés-, FTP –fájletöltés-, SMTPS –levélküldés-, POP, POPS valamint IMAP, IMAPS –levél letöltés-, NTP – időszolgáltatás - , ICMP – hálózat felderítés.
e) Egyes területek (informatika, könyvtár, TIOK, GI) kiemelt szabályrendszerrel férhetnek hozzá további speciális külső forgalmakhoz. Ezek esetében mindig pontosan kell deklarálni a szűrési feltételeket (forrás gép, célgép, port).
f) Az alkalmazottaknak tilos bárminemű nem engedélyezett forgalmat kezdeményezniük a belső hálózatról (akár belső hálózati eszközre, akár internetes irányba).
g) Az alkalmazottak az Internetet csak az Egyetem által elfogadott szoftverekkel, böngészőkkel érhetik el.
h) Tartalomszűrőt kell működtetni a tiltott tartalmú internetes forgalmak szűrésére. A tartalomszűrő adatbázisát a szállító aktualizálja központilag, abba beavatkozni csak kivételek definiálásával lehetséges.
i) A kollégiumra vonatkozó internetes ellátottság: a kollégiumi belső szeparált hálózat internetes ellátottságát külön tűzfalzóna szabályozza. Ezen hálózat teljesen elkülönített az Egyetem belső hálózatától
j) Nem megengedett tevékenységek az Internet használata közben:
   - minden olyan magatartás, tevékenység, amely jogszabályba ütközik, jogszabályt sért,
   - sávszélesség kiemelkedően nagymértékű használata nem Egyetemi célokra.

A felhasználói fiókok kezelési rendje

11. §

(1) A felhasználói fiókok kezelése során biztosítani kell, hogy az Egyetem informatikai rendszereiben a felhasználói fiókok és a kapcsolódó hozzáférések biztonságos módon kerüljenek kiosztásra, adminisztrálásra.

(2) A felhasználói fiókok kezelésére vonatkozó alapvető elvárások:

a) A felhasználói fiókok életciklusának biztonságos adminisztrálására olyan folyamatot kell életbe léptetni, mely magában foglalja mind a kezdeti azonosítási információk kiosztását, azok érvényességi idejének beállítását és a hozzáférési jogosultságok eltávolítását a munkakör megváltozása vagy a munkaviszony megszűnése esetén.

b) Új felhasználói fiók beüzemelését a humánerőforrás, vagy az adott szervezeti egység vezetője kezdeményezi a CI vezetője felé írásban.
c) Új fejhasználó regisztrálásakor az alábbi elveket kell figyelembe venni:
   - Minden felhasználónak egyedi felhasználói fiókkal kell rendelkeznie.
   - A rendszerek eléréséhez használt felhasználónév/jelszó kombináció használata az azzal a felhasználónévvel azonosított munkavállaló kizárólagos felelőssége. A felhasználót erről a felelősségről a felhasználó fiók elkészítésekor és átadásakor tájékoztatni kell.
   - Csoportos vagy megosztott felhasználói fiókok használata nem megengedett, kivéve ha azt a CI vezetője kifejezett kérésre engedélyezi.
   - A rendszerek kezdeti installációs szakasza után a helyi felhasználó fiókokhoz csak a rendszergazdáknak van jogosultsága hozzáférni.
d) Olyan, biztonságos folyamatot kell bevezetni a kezdeti azonosítási információk átadására és azok elfelejtése esetén visszaállítására, mely ezeket az információkat biztonságos módon képes a felhasználónak eljuttatni.
e) Az informatikai rendszerek hozzáféréseit minden esetben egy jól meghatározott felelősnek kell jóváhagyni.
f) Minden informatikai és távközlési rendszer esetén a jogosultságokat rendszeres ellenőrzésnek kell alávetni, melynek célja a jogosultság kiosztás helyességének és a felhasználói fiókok szükségességének ellenőrzése.

(3)[2] Az Egyetemen használt egyes informatikai rendszerekhez kizárólag a jelen szabályzat alapján lehet hozzáférést biztosítani. A hozzáférés biztosítására és a jogosultságok nyilvántartására a kancellár vagy az általa kijelölt személy jogosult. A jogosultságok kiosztásakor alapelvként kell kezelni, hogy az adott funkcióhoz, illetve feladathoz csak az ellátásához szükséges és elégséges mértékű jogosultságot kell biztosítani.

Jelszavak használatának szabályai

12. §

(1) A jelszavak használatának célja a jelszó alapú azonosítási mechanizmusok megfelelő biztonsági szintjének biztosítása az információ feldolgozó rendszerekben, valamint annak biztosítása, hogy a felhasználók megfelelő iránymutatást és oktatást kapjanak jelszavaik biztonságos kezelésére vonatkozóan.

(2) A felhasználóknak megfelelő jelszóval kell rendelkezniük, azt azonosítás céljából használni és az alábbiak szerint rendszeresen változtatni kötelesek. A jelszavakat minden esetben bizalmasan kell kezelni:
a) A felhasználónak kötelessége a jelszó megváltoztatása a felhasználói fiók létrehozása utáni első belépéskor, vagy akkor, ha feltételezhető, hogy sérült a jelszó bizalmassága.
b) A felhasználó a jelszavát nem oszthatja meg, és nem adhatja ki másoknak. A felhasználó a jelszavát a legrövidebb időn belül megváltoztatni köteles, amennyiben a felhasználó gyanúja alapján a jelszava más tudomására jutott.

[2] Beiktatta a 39/2016. (IX. 26.) Határozat.

c) A felhasználónak tilos más felhasználó jelszavát megkérdeznie és tilos más felhasználó azonosítóját használnia annak belépése után. Hasonlóképpen, a felhasználó nem engedheti meg más felhasználónak az azonosítója használatát és nem engedheti át annak használatát a bejelentkezés után.
d) A felhasználónak tilos a jelszavakat külön adatbázisban tárolnia.
e) A felhasználó csak a rendszer általi megfelelő azonosítása után lehet képes megváltoztatni jelszavát.
f) A kezdeti jelszavak (pl. azok, melyek a felhasználói fiók létrehozásakor vagy jelszó reset esetén állítanak be) csak az első bejelentkezésig maradhatnak érvényben. A kezdeti jelszónak egyedinek és nehezen megfejthetőnek kell lennie.[3]
g) Az Egyetem rendszereinek elérésére használt jelszavakat tilos külső rendszerek elérése is felhasználni.
h) A sikertelen jelszóbevitelek számát egy előre meghatározott értékre kell korlátozni, melynek elérése után a felhasználói fiókot meghatározott időre zárolni kell.
i) A bevitel során a jelszavak megjelenítése tilos.
j) A jelszavak rögzítése naplóállományokban tilos.
k) Az informatikai és/vagy távközlési rendszerekben tárolt jelszavak tárolását úgy kell megoldani, hogy azok ne legyenek visszafejthetők és a jogosulatlan hozzáférésektől védve legyenek.
l) A használt jelszó házirendben rögzítésre kerül. A jelszavak legalább 6 karakterből kell, hogy álljanak és az alábbiak közül legalább hármat tartalmazniuk kell: alfabetikus kisbetű, alfabetikus nagybetű, szám, extra karakter.
m) A jelszavak 6 havonta lejárnak, azok megváltoztatását lejártuk esetén kikényszeríti a rendszer, az új jelszónak meg kell felelni a mindenkori jelszó házirendnek. A lejárt jelszavakkal a belépés nem engedélyezett.

Vírusvédelem rendje

13. §

(1) Vírusvédelmi rendszer célja a kártékony programok megelőzésére és detektálására szolgáló megelőző, folyamatos üzemeltetési intézkedések kidolgozása.

(2) Alapvető elvárások a vírusvédelem körében:
a) Minden asztali és laptop számítógépen, valamint valamennyi file-, alkalmazás-, adatbázis- szerveren víruskereső alkalmazásnak kell működnie.
b) Ideértendő a központi levelezési rendszerek vírus és SPAM védelme.
c) Az alkalmazottak nem kapcsolhatják ki és más módon sem változtathatják meg az Antivirus szoftverek működését a munkaállomásokon, laptopokon vagy egyéb rendszereken, kivéve ha erre különleges engedéllyel rendelkeznek.
d) Minden kiszolgáló szerveren egyedileg telepített vírusvédelmi rendszerről kell gondoskodni, a belső levelező szervereken további helyi SPAM szűrő alkalmazása szükséges.

[3] Módosította a 39/2016. (IX. 26.) Határozat.

e) A víruskeresők definíciós adatbázisainak automatikusan on-line frissülniük kell, a hálózathoz nem kapcsolódó eszközöket pedig rendszeresen, hetente frissíteni kell.
f) Az állandó vírusvédelmi szoftverek fertőzés esetén automatikusan (az előre beállított házirendnek megfelelően) beavatkoznak a felhasználó tájékoztatása mellett.
g) A külső adat hordozók csatlakoztatásuk esetén automatikusan vírus szkennelés alá esnek.
h) Eljárásokat és felelősségeket kell megállapítani a vírustámadások esetén történő riportolásra és kárelhárításra vonatkozóan.
i) Vírustámadás és az azt követő kárelhárítás alatt minden incidens naplózásra kerül helyileg a védelmi szoftver által, ezeket a CI elemzi ki és végez további intézkedéseket.
j) A felhasználóknak tilos bárminemű vírusos állomány vagy ismeretlen eredetű üzenet tárolása, továbbítása az Egyetem bármely eszközén, berendezésén, rendszerén.[4]

V. A felhasználói hibabejelentés és az adatmentés rendje

A felhasználói hibabejelentés

14. §

(1) A hibabejelentések szabályozásának célja a felhasználók által jelzett informatikai, telekommunikációs, oktatástechnikai hibák elhárításának egységes kezelése.

(2) A hibák észlelésével és bejelentésekkel kapcsolatos alapvető követelmények:
a) A felhasználóknak kötelessége bármilyen informatikai, telekommunikációs, oktatástechnikai hiba vagy bizonytalan működés esetén a CI értesítése.
b) A felhasználóknak tilos a probléma kijavítására irányuló, a szoftver és/vagy hardver integritást sértő magatartást mutatniuk és követniük kell a CI utasításait.
c) A felhasználóknak a hibabejelentéseket lehetőleg e-mailben kell elküldeni.
d) A hibajegynek tartalmaznia kell:
   - a hiba helyét (telephely, felhasználó),
   - a hiba leírását,
   - a hibásnak ítélt eszközt vagy szolgáltatást,
   - a hiba jelentkezésének időpontját.
e) A hibák bejelentését telefonon is meg lehet tenni az adott telephely informatikusain keresztül, de ha a lehetőségek adottak, akkor email-en kell a hibákat jelezni a nyomon követhetőség érdekében.
f) Az adott hibabejelentés kivizsgálásának megkezdését a CI-nek kötelessége a lehető legrövidebb időn belül (maximum a bejelentést követő munkanap 16.00 óráig, de lehetőleg még tárgynap) elindítani.

[4] Módosította a 39/2016. (IX. 26.) Határozat.

g) A beérkezett hibák elhárítási sorrendjét azok súlyossága szerint a CI-nek rangsorolni kell, és a hibák elhárítást azok alapján és nem a bejelentések sorrendje alapján kell végeznie.
h) A hiba elhárításáról a hibabejelentőt az elhárítást követően tájékoztatni kell.

Az adatmentés szabályai

15. §

(1) Az adatmentések szabályozásának célja, hogy az Egyetem által használt informatikai rendszerek és az azokban, vagy egyéb file szervereken tárolt adatok bármely okból bekövetkező meghibásodása esetén visszaállíthatók legyenek.

(2) Az adatmentés alapvető szabályai:

a) Valamennyi üzemeltetett rendszernek valamely központi szerveren kell lennie.
b) Az Egyetem közalkalmazottai által munkaidőben (és azon túl, ha erről külön rendelkezett az érintett vezetés) az Egyetemi erőforrások igénybevételével létrehozott dokumentumok az Egyetem tulajdonát képezik. Mint szellemi termék felett a továbbiakban az Egyetem rendelkezik.
c) A szerverek operációs rendszereinek, az azokra installált alkalmazásoknak valamint a rajtuk tárolt adatok napi szintű mentésének beállításáért a CI felelős, vagy lehetőség szerint a rendelkezésre álló technikai eszközök igénybevételével azok teljes kihasználása mellett a CI hivatott a mentési rendszer kidolgozására.
d) Az Egyetemi ügyviteli folyamataiban keletkezett kiemelt területek dokumentumai, amiket nem valamely rendszeralkalmazásban tárolnak, a szerverekre történő mentéséért az azokat létrehozó felhasználó a felelős.
e) Minden felhasználó rendelkezik a szervezeti egységének igényei alapján kialakított csoportosan – de szabályozott módon – hozzáférhető szervezeti tárterülettel.
f) Amennyiben a felhasználó a szerver helyett a saját számítógépének merevlemezére végzi a dokumentumok mentését, úgy annak meghibásodása esetén az adatok elvesztéséért a felhasználó vonható felelősségre.
g) A felhasználók helyben tárolt adatainak archiválásában a CI kollégái igény esetén segítséget nyújtanak, az archiválást elvégzik.
h) Minden felhasználónak törekednie kell arra, hogy az Egyetemi dokumentumokat a biztonsági mentésekkel rendelkező szervereken tárolják. Továbbá minden saját kezelésű állomány, dokumentum esetén gondoskodnia kell annak biztonságos tárolásáról esetleges mentéséről, ha szükséges a CI bevonásával.
i) Tilos a szervereken nem intézményi érdekeket szolgáló adattartalmakat tárolni.

(3)[5] Az adatmentés eljárásrendjét a 2. számú melléklet tartalmazza.

[5] Beiktatta a 39/2016. (IX. 26.) Határozat.

VI. A felhasználók jogai és kötelezettségei

A felhasználók jogai

16. §[6]

A Hálózat használata folyamán a felhasználó jogosult:

a) A munkavégzéshez szükséges programokkal ellátott, egy vagy több személy használatára beállított, felkészített számítógép(ek), kommunikációs eszközök használatára.
b) A munkavégzéshez szükséges mértékben – a használatra vonatkozó feltételek mellett – a hálózati szolgáltatások igénybevételére.
c) Működési zavar, meghibásodás, rendellenes működés esetén segítségkérésre.
d) A munkavégzéshez szükségesnek ítélt eszközök, szoftverek beszerzését, telepítését igényelni.
e) Levelező szolgáltatás és saját elektronikus postafiók használatára.
f) A Hálózat üzemeltetői részéről a személyhez fűződő jogainak tiszteletben tartására, amelytől eltérni csak törvény által meghatározott esetekben lehet.
g) Tájékoztatásra – a lehetőségek függvényében – a Hálózat technikai fejlesztéseiről, problémáiról (tervezett vagy rendkívüli eseményekről).
h) A felhasználókra vonatkozó szabályok megismerésére.

A felhasználók kötelességei

17. §[7]

A Hálózat biztonságos használata érdekében a felhasználó köteles:

a) Jelen szabályzatot megismerni, az abban foglaltakat betartani, valamint együttműködni a Hálózat üzemeltetőivel a benne foglaltak betartatása érdekében.
b) Az egyetemi Hálózatot annak céljaival megegyezően használni.
c) Az Egyetem Hálózatán csak a számára engedélyezett erőforrásokat használni.
d) Tevékenységével nem zavarni, nem akadályozni, nem veszélyeztetni az egyetemi hálózaton feladataikat végzők tevékenységét.
e) A hálózati szolgáltatások igénybevételéhez használatos jelszavait titkosan kezelni, előírt gyakorisággal változtatni, a Szabályzat jelszóhasználattal kapcsolatos előírásait betartani (Tilos a hozzáférési jogosultságok, jelszavak kölcsönadása, átruházása, mások jelszavának elkérése, a hálózat, a levelező szolgáltatás - a tulajdonos felhatalmazása nélkül - más nevében történő igénybevétele.).
f) Gondoskodni adatainak tőle elvárható védelméről és helyi mentéséről.
g) A számára biztosított informatikai és kommunikációs eszközöket működőképes állapotban megőrizni, leltározáskor és más ellenőrzéskor kérésre bemutatni, a jogviszony/munkaviszony megszűnésekor visszaszolgáltatni (a biztosított eszközöket, berendezéseket nem bonthatja meg, a hardver és szoftverkörnyezetet

[6] A §-t, valamint a megelőző alcímet és címet beiktatta a 39/2016. (IX. 26.) Határozat.
[7] A §-t, valamint a megelőző alcímet beiktatta a 39/2016. (IX. 26.) Határozat.

- beleértve a számítógépes vírusellenőrzéssel, és vírusirtással kapcsolatos szoftvereket is – nem módosíthatja, az eszközök hálózati és egyéb beállításaiban működést befolyásoló módosításokat nem végezhet).
h) Felelősséget vállalni az általa szándékosságból, vagy gondatlanságból, vagy a neki felróható módon az általa, a nevében, a felhasználói azonosítójával (különösen: a jelszavak kölcsönadásával vagy nem biztonságos kezelésével, a hozzáférési jogosultságok nem megfelelő kezelésével, a számára biztosított – az egyetem tulajdonát képező - informatikai, kommunikációs eszközökben vagy eszközökkel) okozott szabályellenes cselekedetekért, károkért. Az előbbiekből eredő esetleges működési zavar, adatvesztés utáni helyreállítás, javítás/javíttatás költségeit megtéríteni.
i) Meghibásodás, üzemzavar észlelésekor, vírusfertőzés (vagy annak gyanúja) esetén haladéktalanul értesíteni a rendszergazdát, a számítógép további használatát annak intézkedéséig felfüggeszteni.
j) Külső adathordozók csatlakoztatása után vírusellenőrzést, vírusirtást végrehajtani.

VII. Az informatikai eszközök selejtezése

Eszközök selejtezése

18. §[8]

Az Egyetem tulajdonában levő eszközök selejtezésekor a selejtezések végrehajtásáért a kijelölt rendszergazda felel.

A selejtezést a következő előírások betartása mellett szabad végezni:

a) A selejtezés végrehajtására kijelölt, feljogosított személynek a vonatkozó szakmai, működési ismeretek birtokában kell lennie.
b) A selejtezésről jegyzőkönyvet kell készíteni, amit a Campus igazgatónak meg kell küldeni.
c) Olyan eszközöket, rendszereket nem lehet leselejtezni, amelyek hiánya információvesztéssel jár, vagy fennáll annak a veszélye, hogy a selejtezés során bizalmas adat kerülhet ki a szervezetből.
d) Adathordozót csak annak teljes megsemmisítése, vagy fizikailag olvashatatlanná tétele után lehet selejtezni.
e) Selejtezéssel tilos a folyamatos üzemeltetést veszélyeztetni.
f) Selejtezést csak abban az esetben szabad végezni, ha a selejtezni kívánt eszköz hiánya nem veszélyezteti az informatikai biztonságot. Amennyiben a selejtezés elkerülhetetlen, azt megelőzően gondoskodni kell az eszköz funkcionális pótlásáról.

VIII. Záró rendelkezések

[8] A §-t, valamint a megelőző alcímet és címet beiktatta a 39/2016. (IX. 26.) Határozat.

19. §[9]

(1) Jelen Szabályzatot a Szenátus 2015. október 26-án meghozott, 30/2015. számú határozatával fogadta el és 2016. szeptember 26-án meghozott, 39/2016. (IX. 26.) számú határozatával módosította.

(2) A Szabályzat az elfogadását követő napon lép hatályba.

Budapest, 2016. szeptember 27.

…….
Fülöp József
rektor

……..
Nagy Zsombor
kancellár

Mellékletek:

1. számú: Biztonsági osztályok
2. számú: Mentési rend

[9] A §-t és a megelőző címet beiktatta a 39/2016. (IX. 26.) Határozat.

1. számú melléklet[10]

Biztonsági osztályok

Biztonsági osztályok	**Védelmi intézkedések**
Nyílt	Leírás: Ebben a biztonsági osztályban lévő adatok nyilvánosságra kerülése semmilyen következménnyel nem jár a MOME-re nézve. Az adatok bizalmasságára és rendelkezésre állására nincs semmilyen követelmény. Pl.: bizonyos nyilvánosan szolgáltatott információk, indított képzések, szakok, szakirányok, a pályázatokra vonatkozó nyilvános adatok, az „üvegzseb törvény" által kötelezően nyilvánosságra hozandó adatok, valamint egyéb közérdekű adatok. Jelölés: nincs. Védelmi intézkedések: - Vírusfertőzés megelőzése érdekében, az adatokon rendszeresen vírusellenőrizést kell végezni.
Alap	Leírás: A külső hozzáférést meg kell előzni, azonban az adatok nyilvánosságra kerülésének nincsenek komoly következményei. A belső hozzáférés korlátozott. Az adatok sértetlensége, bizalmassága, rendelkezésre állása fontos, de nem kritikus. Pl.: munkafeljegyzések, találkozók és projektek protokolláris információi, belső levelezés, ügyiratok, személyzeti anyagok stb. Jelölés: „Belső használatra." Védelmi intézkedések: - Tárolt adathordozókon, nyomtatott formában a biztonsági jelölést („Belső használatra") fel kell tüntetni. - Biztosítani kell az adatintegritást.

[10] Beiktatta a 39/2016. (IX. 26.) Határozat.

	A jogosultsági rendszer kialakításával és megfelelő jelszavas védelem kialakításával védeni kell ezen adatokat a jogosulatlan hozzáféréstől, adatmódosítástól. - Vírusfertőzés megelőzése érdekében, az adatokon rendszeresen vírusellenőrizést kell végezni. - Külső partnerekkel való együttműködés kapcsán pontosan meg kell határozni, hogy melyek azok az információk, amelyek a partnerrel megoszthatók. - Az adatkezelés során az adatoknak nem szabad jelszavas védelem nélkül a szervezeten kívülre kerülniük.
Fokozott	Leírás: Ebben a biztonsági osztályban lévő adatok nem nyilvánosak, védeni kell őket a jogosulatlan hozzáféréstől. Jogosulatlan hozzáférés, adatmódosítás következtében a MOME-t anyagi kár érheti, kihatással lehet a MOME működésére nézve. Pl.: ezek az Infotv. szerinti személyes adatok, a statisztikáról szóló 1993. évi XLVI törvény 17.§-a szerinti egyedi adatok, valamint a MOME működésére vonatkozó nem közérdekű adatok. Jelölés: „Nem nyilvános”. Védelmi intézkedések: - Tárolt adathordozókon a biztonsági jelölést („Nem nyilvános”) fel kell tüntetni. - Biztosítani kell az adatintegritást. - Vírusfertőzés megelőzése érdekében, az adatokat rendszeresen ellenőrizni kell. - A jogosultsági rendszer kialakításával és megfelelő jelszavas védelem kialakításával védeni kell ezen adatokat a jogosulatlan hozzáféréstől, adatmódosítástól. - A mentéseket két példányban kell elkészíteni. - A mentéseket tartalmazó adathordozók legalább egyik példányát, illetve a szoftvereket tartalmazó adathordozókat

	zárt, tűzvédelmi rendszerrel ellátott tároló helyiségben szabad csak tárolni. - A hozzáféréshez szükséges jelszavakat tilos plain-textben továbbítani, illetve papíron átadni. - Nyomtatás alkalmával biztosítani kell, hogy az adatok ne kerüljenek illetéktelen kezekbe. - Az adatkezelés során az adatokat belépési időhöz kötött, legalább 8 karakterű jelszóval kell minden esetben védeni, függetlenül attól, hogy az adatok elhagyják a MOME-t vagy sem. - Abban az esetben, ha az adatra nincs már szükség, biztonságos módon le kell törölni, vagy meg kell semmisíteni tekintet nélkül az adattárolás formájára
Kiemelt	Leírás: Ebben a biztonsági osztályban lévő adatokhoz való jogosulatlan belső vagy külső hozzáférés a MOME-ra nézve kritikus következményekkel jár. Az adatintegritás ugyancsak kritikus. Az adatokhoz való hozzáférés igen szűk körben engedélyezett. Az adatkezelésre igen szigorú előírások vonatkoznak. Jelölés: „Titkos, szigorúan titkos." Védelmi intézkedések: - Tárolt adathordozókon, az állomány nevében a biztonsági jelölést (minősítést) fel kell tüntetni. - Az adatintegritást biztosítani kell. - Vírusfertőzés megelőzése érdekében, az adatokat rendszeresen ellenőrizni kell. - A jogosultsági rendszer kialakításával és megfelelő jelszavas védelem kialakításával védeni kell ezen adatokat a jogosulatlan hozzáféréstől, adatmódosítástól. - Nyomtatás alkalmával biztosítani kell, hogy az adatok ne kerüljenek illetéktelen kezekbe.

	- A mentéseket két példányban kell elkészíteni. - A mentéseket tartalmazó adathordozókat a jelölésnek megfelelően, illetve a szoftvereket tartalmazó adathordozókat, kétfázisú beléptető rendszerrel rendelkező, zárt tároló helyiségben (biztonsági zónában), tűzbiztos szekrényben szabad csak tárolni. A hozzáféréseket naplózni kell. - Az adatkezelés során az adatokat a biztonsági zónán kívül az adatokat rejtjelező algoritmussal kell védeni. - Abban az esetben, ha az adatra nincs már szükség, biztonságos módon le kell törölni, vagy meg kell semmisíteni tekintet nélkül az adattárolás formájára

Használt rendszerek besorolása

Rendszer megnevezése	**Nyílt**	**Alap**	**Fokozott**	**Kiemelt**
SALDO pénzügyi-számviteli rendszer			x	
KVI Kincstári Vagyonkezelő rendszer		x		
ETR tanulmányi rendszer			x	
Corvina könyvtári rendszer		x		
Levelező rendszer			x	
Intra WEB	x			
dms One iktatórendszer		x		
Intézményi WEB szerver	x			
Szervezeti egységek közös mappája (minden szervezeti egységnek külön-külön mentve)		x		
KIRA (bérszámfejtés)		x		
Szerződésnyilvántartó rendszer		x		

2. számú melléklet[11]

Mentési Rend

A mentés menete

1. típus: Fokozott biztonsági besorolású rendszerek mentése

Minden hétköznap óránként teljes mentés készül a megadott fájlról, ami a tömörítés befejeztével azonnal a mentést tároló szerverekre kerül. Ezeken a szervereken 23:30-kor az aznapi 23:00-ás mentésről egy egyedi fájlnévvel másolat készül a mentés végleges könyvtárába. Az óránkénti mentés 24 órás rotációval felülíródik.

2. típus: Egyéb, nem fokozott biztonsági besorolású rendszerek mentése

Hétköznap:

A mentés a mentendő adatot tartalmazó gép háttértárolóján lévő dedikált könyvtárba kerül, archiválva. Ha az adatról még nem létezik ott mentés, akkor aznap teljes mentés készül. Ha létezik, akkor frissítő (növekményes) mentésre kerül sor. A mentés minden hétköznap este 22:30 után indul. Ebből a mentésből csak egyetlen példány készül, amely minden este bővül az esetleges friss adatokkal. A mentésről minden esetben automatikusan napló készül, melyeket egy külön program automatikusan ellenőriz, és hiba esetén e-mailben értesítést küld.

Hétvége:

A mentést tároló szervereken megtörténik a megelőző három hétvége mentéseinek példányszám szerinti mozgatása (forgatás), majd az aktuális, azaz pénteki állapot, mint legfrissebb mentés átmásolásra kerül a hálózaton, a mentendő adatokat tartalmazó gépek hétköznapi mentéseket tároló dedikált könyvtárából, a mentést tároló szervereken lévő végleges helyeikre. A visszamenőleg megőrzött példányszám egységesen 4 darab, vagyis a legrégebbi mentés a legfrissebb mentést egy hónappal megelőző pénteki állapot.

2. típusú mentés készül az alábbi rendszerekről:

- Szervezeti egységek közös mappája (minden szervezeti egységnek külön-külön mentve)
- ETR Tanulmányi Rendszer
- SALDO
- Corvina könyvtári rendszer

- dms One
- Levelező rendszer
- Intra WEB
- Intézményi WEB szerver

3. típus: A szerverek rendszernaplóinak mentése

[11] Beiktatta a 39/2016. (IX. 26.) Határozat.

A szerverek rendszernapló-bejegyzései a telepítéskori alapértelmezett elévülési módon kerülnek megőrzésre. Ez alól kivételt képez a MOME fő átjárójának forgalmi naplója (PROXY), amely napi egyszeri mentéssel, 90 napra visszamenőleg megőrződik az átjáró gépén.

4. típus: A felhasználói munkaállomások mentése

A felhasználói munkaállomásokon lévő adatok mentését megnehezítik az alábbi tényezők:
Nagy mennyiség
Nagymértékű differenciálódás az adatok fontosságában
A munkaállomás nehezen követhető készenléti állapota

Ezen okok miatt a munkaállomáson lévő adatok mentését vagy archiválását az Informatikai és Telekommunikációs Csoport csak külön kérésre végzi. A munkaállomás használója vagy felettese kérheti írásban a mentést vagy archiválást. Az igénybejelentést követően a rendszergazdák időpont egyeztetést követően elvégzik a feladatot.

Az egyetem működésében fontos szereppel bíró adatokat fájlszerveren, a minden szervezeti egység számára kijelölt megosztásban kell tárolni, nem a felhasználó saját munkaállomásán.

5. típus: A virtualizált szerverek mentése

A fizikai hostokon futtatott virtuális szerverekről alkalmanként „off-line" üzemben teljes szerver kép, fájl szintű mentés történik. A mentések gyakorisága esetenkénti, a lényeges rendszer szintű változtatások alkalmával. A virtuális szervereken tárolt adatok és adatbázisok mentése az IBSZ erre vonatkozó szakaszai alapján történik.