BUDAPESTI
METROPOLITAN
EGYETEM

A Budapesti Metropolitan Egyetem

Informatikai Biztonsági Szabályzata

2019. október

A Budapesti Metropolitan Egyetem informatikai rendszereinek, alkalmazásainak biztonságát garantáló eljárások és előírások egységes keretbe foglalása érdekében a Budapesti Metropolitan Egyetem Szenátusa az Egyetem Informatikai Biztonsági Szabályzatát a következőkben határozza meg.

ÁLTALÁNOS RENDELKEZÉSEK

1. Az Informatikai Biztonsági Szabályzat (a továbbiakban: Szabályzat) célja a Budapesti Metropolitan Egyetem (a továbbiakban: METU vagy Egyetem) használatában lévő és az általa üzemeltetett informatikai rendszerek, alkalmazások, továbbá az informatikai rendszerek, alkalmazások által kezelt adatok bizalmasságának, sértetlenségének és rendelkezésre állásának biztosítása, ennek érdekében az informatikai rendszerekkel, alkalmazásokkal összefüggő tevékenységekre vonatkozó szervezeti, személyi, fizikai, informatikai és adminisztratív biztonsági követelmények meghatározása, illetve ezen követelmények teljesítésével összefüggő felelősségi előírások rögzítése.
2. A Szabályzat személyi hatálya kiterjed az Egyetem minden informatikai rendszert használó hallgatójára, valamint az oktatói és nem oktatói munkakörben foglalkoztatott valamennyi munkavállalójára, illetve az Egyetemmel polgári jogi jogviszonyban álló személyekre és szervezetekre.
3. A Szabályzat területi hatálya kiterjed az Egyetem valamennyi ingatlanára, képzési helyszínére és telephelyére, valamint külső helyszínen zajló rendezvényeire.
4. Az Egyetem különös gondot fordít arra, hogy az érintett személyek a Szabályzatot (eseti kivonatát) a szükséges mértékben megismerjék és betartsák.
5. A Szabályzat tárgyi hatálya kiterjed az Egyetem informatikai rendszereire, alkalmazásaira és azok moduljaira (a továbbiakban együttesen: rendszer), az informatikai rendszerekhez csatlakoztatható informatikai, irodatechnikai, multimédiás eszközökre és adathordozókra, az informatikai rendszerekben kezelt, feldolgozott, tárolt adatokra, dokumentumokra, valamint ezekkel kapcsolatos informatikai és biztonsági tevékenységre.

ÉRTELMEZŐ RENDELKEZÉSEK

6. Jelen Szabályzat alkalmazásában:

6.1. **adat**: elektronikus formában megjelenő tény, feltevés (elemi információ);

6.2. **adatállomány**: az egy nyilvántartásban kezelt adatok összessége;

6.3. **adatbázis**: egymással összefüggő adatok (adatállományok) szervezett összessége, amely lehetővé teszi, hogy az egymással összefüggő adatok az egymásra való hivatkozás alapján hatékonyan megtalálhatók legyenek;

6.4. **adathordozó**: az elektronikus adatkezelő rendszerhez csatlakoztatható vagy abba beépített olyan eszköz, amelynek segítségével az elektronikus adatok tárolása, terjesztése megvalósítható;

6.5. **adminisztratív biztonsági követelmények**: az informatikai rendszer használata, üzemeltetése vagy fejlesztése során az adatok és a munkafolyamatok nyilvántartását, nyomon követhetőségét, továbbá az ezzel kapcsolatos feladatok ellátásának ellenőrzését lehetővé tevő segédletek és eljárásrendek meglétére, alkalmazására vonatkozó elvárások (pl. naplók, nyilvántartások vezetése, ellenőrzése, ennek rendje);

6.6. **archiválás**: speciális mentési eljárás, amelynek során az adatokat, az adatállományt az informatikai rendszerből törlik és az informatikai rendszertől független adathordozóra helyezik át. Célja a napi tevékenység során már nem szükséges, de megőrzendő adatok biztonságos, hosszú távú, visszakereshető formában történő tárolásának biztosítása;

6.7. **azonosítás:** informatikai eljárás, amelynek során a felhasználó az informatikai rendszerben az autorizáció megszerzése érdekében igazolja személyazonosságát tudás alapú (jelszavas), birtoklás alapú (tokenes) vagy tulajdonság alapú (biometrikus), illetve ezek kombinációitból képzett azonosítóval;

6.8. **autorizáció (feljogosítás)**: azonosításra épülő informatikai eljárás, amelynek eredményeként egyértelműen azonosított személy (eszköz) a feladatai ellátásához meghatározott hozzáférési, eljárási vagy egyéb jogosultságokat kap;

6.9. **belső hálózat (intranet)**: a METU saját, védett hálózata, amelynek rendeltetése, hogy elérhetővé tegye a funkcionális rendszereket, az oktatási rendszereket, a belső kommunikációs rendszert, a munkavégzéshez szükséges egyéb alkalmazásokat, adatbázisokat, a felhasználók számára biztosított − személyes és csoportos használatú − elektronikus tárhelyeket;

6.10. **bizalmasság**: az informatikai rendszer azon tulajdonsága, hogy a benne tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról;

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

- belső okra visszavezethető, információs rendszer nem rendeltetésszerű, nem a szakmai előírásoknak megfelelő használata, működtetése, valamint a jogosulatlan adathozzáférés, az IT rendszer fizikai védelmi rendszerének megsértése, kártékonykód informatikai rendszerbe jutása;
- üzletmenet-folytonosságot érintő: működésfolytonosságot megszakító, illetve katasztrófahelyzetet előidéző történés vagy cselekvés;
- külső okra visszavezethető, az informatikai rendszer külső fél jóhiszemű tevékenységével összefüggésben tapasztalt hibás működése, külső támadás;

6.12. **biztonsági megfelelőség**: az informatikai rendszer tulajdonsága: mennyiben, milyen mértékben felel meg az informatikai biztonsági követelményeknek;

6.13. **felhasználó**: az informatikai rendszert feladatai ellátásához igénybe vevő személy;

6.14. **fizikai (környezeti) biztonsági követelmények**: az informatikai rendszer használata, üzemeltetése vagy fejlesztése fizikai környezetére (épület, helyiség, tároló) vonatkozó elvárások (pl. objektumvédelem, tűzvédelem stb.);

6.15. **funkcionális megfelelőség**: az informatikai rendszer tulajdonsága, hogy mennyiben, milyen mértékben felel meg a vele szemben támasztott funkcionális követelményeknek;

6.16. **hálózat:** számítógépek és hozzájuk kapcsolódó eszközök meghatározott szabályok szerinti összekapcsolása, amely adat- és információcserét tesz lehetővé;

6.17. **hardver**: az informatikai rendszer fizikai elemei, a működéshez szükséges műszaki-technikai eszközök összefoglaló neve.

6.18. **információbiztonság**: az a dinamikusan változó állapot, amikor az információ − megjelenési formájától függetlenül − védelmet élvez, azaz bizalmassága, rendelkezésre állása és sértetlensége biztosított;

6.19. **informatikai biztonság**: az informatikai rendszer azon állapota, amikor a rendszer rendeltetésszerűen működik és a rendszerben kezelt adatok bizalmassága, rendelkezésre állása, sértetlensége biztosított;

6.20. **informatikai biztonsági követelmények**: az informatikai rendszer használatával, üzemeltetésével és fejlesztésével kapcsolatos elvárások;

6.21. **informatikai rendszer**: a számítógépek és a hozzájuk kapcsolódó eszközök (hálózat), a számítógépeken futó programok, valamint a számítógépeken kezelt, feldolgozott adatok együttese, amelyek célja meghatározott feladatok, feladatsorok, tevékenységek végrehajtása;

6.22. **jogosultság**: az informatikai rendszerben meghatározott adatokon (adatkörökön) meghatározott tevékenységek végrehajtására adott felhatalmazás. Ilyen a valamely adatra vonatkozó olvasási jog, írási jog, módosítási jog, törlési jog.
6.23. **mentés (biztonsági mentés)**: biztonsági másolat készítése az informatikai rendszerben tárolt adatokról, adatállományokról, illetve az informatikai rendszerben használt alkalmazásokról. A másolat célja az elsődleges adattároló megsérülése esetén az adatok helyreállíthatóságának biztosítása;
6.24. **mobil eszköz**: asztali munkaállomásnak nem minősülő egyes informatikai és kommunikációs feladatok ellátására használható, kommunikációs szolgáltatásokkal rendelkező, hordozható elektronikus eszköz. Ide tartoznak a laptopok és notebookok, valamint táblagépek, mobiltelefonok, okostelefonok, külső modemek;
6.25. **munkaállomás**: a felhasználó számára biztosított számítógép;
6.26. **oktatási rendszer**: a METU mint felsőoktatási intézmény tevékenységét támogató, a hallgatókat információkkal és segédanyagokkal ellátó, valamint az oktatást segítő informatikai rendszer;
6.27. **naplózás**: az informatikai rendszerben bekövetkező események, felhasználói tevékenységek és ezek időpontjának automatikus rögzítése a változások észlelése és a számon kérhetőség biztosítása érdekében;
6.28. **program**: számítógépes nyelven megírt utasítássorozat;
6.29. **rendelkezésre állás**: annak biztosítása, hogy az informatikai rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek;
6.30. **szoftver**: a számítógép, az informatikai rendszer logikai elemei; a működtető programok (rendszerprogramok, operációs rendszerek) és a felhasználói programok (alkalmazások) összefoglaló neve.

SZERVEZETI INFORMATIKAI BIZTONSÁGI KÖVETELMÉNYEK

7. Az informatikai rendszerek, adatbázisok és eszközök felügyelete és üzemeltetése vonatkozásában meg kell valósítani, hogy a feladategyesítésből eredő hibák és rosszindulatú tevékenységek kockázatát az Egyetem kizárja, vagy elfogadható szintre csökkentse.

SZEMÉLYI INFORMATIKAI BIZTONSÁGI KÖVETELMÉNYEK

8. Jelen Szabályzat megismeréséről és elfogadásáról a METU minden munkavállalójának írásban kell nyilatkoznia. Biztosítani kell a jelen Szabályzat megismerését a hallgatók részére is.

9. Az informatikai rendszerekhez, a rendszerekben tárolt adatokhoz kizárólag a 8. pontban foglalt nyilatkozatot megtevő személyek férhetnek hozzá.

10. A megismerési és elfogadási nyilatkozatot minden munkavállalónak a belépéskor ki kell tölteni.

11. A Humánerőforrás Igazgatóság a nyilatkozatokat a személyi anyagokhoz csatolva megőrzi.

FIZIKAI BIZTONSÁGI KÖVETELMÉNYEK

12. Az informatikai eszközöket úgy kell telepíteni és tárolni, hogy azokhoz a jogosultsággal rendelkező személyeken kívül más személy hozzáférése kizárt legyen.

13. A METU tulajdonát képező informatikai, irodatechnikai, multimédiás eszközt vagy adathordozót a METU területéről kivinni csak a közvetlen vezető, oktató engedélyével lehet, kitöltött METU eszköz átadás-átvételi jegyzőkönyv alapján.

INFORMATIKAI BIZTONSÁGI KÖVETELMÉNYEK

14. Az egyes informatikai rendszerekkel és adathordozókkal kapcsolatos fejlesztési, üzemeltetési

és biztonsági tevékenységet úgy kell megtervezni és végrehajtani, a fejlesztési, működtetési és védelmi terveket, dokumentumokat, előírásokat úgy kell elkészíteni, hogy azok a biztonsági osztályozási előírások figyelembevételével garantálják az információbiztonság szükséges és elégséges szintjét. Ezen elvek alapján kockázatarányos, differenciált, többszintű informatikai védelmi rendszert kell kialakítani és működtetni.

15. Az informatikai infrastruktúrára vonatkozó beszerzések és a fejlesztések során a tervezési dokumentáció összeállítása során, még a fizikai megvalósítás megkezdése előtt, az egyes funkciók elérhetővé tételét a megrendelő által szakmai és információvédelmi szempontból véleményezni kell. Ennek során figyelemmel kell lenni arra, hogy a legszűkebb funkcionalitás elvének a rendszer teljes életciklusában érvényesülnie kell.

16. Az Egyetem informatikai rendszereiben csak jogtiszta, központilag beszerzett, engedélyezett és nyilvántartott szoftver telepíthető. A szoftver telepített példányszáma nem lépheti túl a beszerzett licenc mennyiségét. Az Egyetem központi licenc nyilvántartását az Informatikai Igazgatóság vezeti.

17. A METU informatikai rendszerei csak olyan rendszerelemmel bővíthetőek, illetve csak olyan új rendszerelemek telepíthetőek, amelyet a METU informatikai, technikai szempontból bevizsgált és megfelelőnek talált és biztonsági szempontból jóváhagyott.

18. A METU informatikai rendszereihez csak olyan informatikai, irodatechnikai, hálózati eszköz csatlakoztatható, amelyet az Informatikai Igazgatóság informatikai, technikai szempontból bevizsgált és megfelelőnek talált és biztonsági szempontból jóváhagyott. Nincs szükség bevizsgálásra és jóváhagyásra az USB memória (pendrive) esetében.

19. A METU hálózatán kívüli kommunikációra képes eszközök és technológiák − wifi, bluetooth, külső modem, rádiós internet elérés stb. − METU hálózatára kapcsolt eszközön történő használata, az Informatikai Igazgatóság által engedélyezett eseteket és biztosított eszközöket kivéve, tilos.

20. Az informatikai rendszerekben végrehajtott műveleteket a felhasználó azonosítását lehetővé tevő módon naplózni kell. Az informatikai rendszerekbe adatállomány, szoftver csak vírusvédelmi ellenőrzést követően, jelen Szabályzatban foglaltaknak megfelelően tölthető.

ADMINISZTRATÍV BIZTONSÁGI KÖVETELMÉNYEK

21. Az informatikai rendszerek teljes életciklusát az Egyetem informatikai igazgatósága köteles dokumentálni, külső partner közreműködése estén a szükséges dokumentumokat átvenni és nyilvántartani, így a tervezés, a fejlesztés és továbbfejlesztés, a tesztelés és ellenőrzés, az üzemeltetés és karbantartás, valamint a megszüntetés fázisait is.

22. Az informatikai rendszer dokumentációja akkor teljes, ha tartalmazza mind a funkcionális, mind a biztonsági megfelelőségre vonatkozó valamennyi lényeges adatot.

23. A METU tulajdonában levő és a METU által használt hardver és szoftver elemeket, licenceket, informatikai, irodatechnikai, multimédiás, oktatási és kommunikációs eszközöket, továbbá az adathordozókat egyedi azonosításra alkalmas módon nyilván kell tartani.

A FELHASZNÁLÓ JOGAI ÉS KÖTELEZETTSÉGEI

24. A felhasználó jogosult a munkavégzéséhez szükséges informatikai, irodatechnikai, multimédiás, oktatási és kommunikációs eszközöket használni, a használatukhoz szükséges ismereteket dokumentáció alapján vagy oktatás formájában elsajátítani.

25. A felhasználó a rendelkezésére bocsátott informatikai, irodatechnikai, oktatási és

kommunikációs eszközöket – személyi számítógép, szerver, notebook, tablet, vezetékes és mobiltelefon, nyomtatók, szkennerek, fénymásolók, hálózati és intranet hozzáférések és egyéb szoftverek – elsődlegesen a METU céljaival, feladataival összefüggésben, a munkaköri feladataihoz kapcsolódóan, azok teljesítése érdekében, a számára biztosított jogosultságok keretein belül, rendeltetésszerűen használhatja.

26. A METU által biztosított munkaállomások és a notebookok esetén a METU által telepített, elérhetővé tett alkalmazások, szolgáltatások magáncélra használhatóak, ha nem ütköznek jogszabályba, intézményi szabályzatba, munkaszerződésbe, és a felhasználói szabályokat nem sértik. Magáncélú felhasználás esetén a felhasználó felelőssége, hogy milyen adatokat ad meg, és rögzít az eszközökön.
27. A nyomtatási, fénymásoló rendszer magáncélú használata munkavállalók esetén nem engedélyezett, kivéve a költséggel nem járó szkennelési folyamatot. A hallgatók a feltöltött összeg erejéig a rendszert magáncélra is használhatják.
28. Mobiltelefonon és tableteken – kivéve speciális rendeltetési eszközöket (pl Feedback eszközök) – a magáncélú használat a METU által fizetett mobilelőfizetésekről szóló vezérigazgatói utasításban meghatározott keretig, mértékig engedélyezett, használatuk azonban nem ütközhet jogszabályba, intézményi szabályzatba, munkaszerződésbe, és felhasználói szabályokat nem sérthet. A METU a céges adatokhoz bármikor hozzáférhet, a személyesnek megjelölt fájlokat azonban csak komoly kockázatot jelentő, illetve kivételes esetben nyithatja meg, ezeket is csak a felhasználó jelenlétében, vagy annak időben való értesítését követően.
29. A munkaállomás illetéktelen hozzáférés elleni védettségéért, a munkaállomáson végzett minden tranzakcióért a bejelentkezéstől a kijelentkezésig a bejelentkezett felhasználó a felelős. Ez a felelősség akkor is fennáll, ha a tranzakciókat harmadik személy hajtotta végre, amennyiben erre jelen Szabályzat előírásainak felhasználó általi be nem tartása miatt kerülhetett sor.
30. A munkaállomás illetéktelen hozzáférés elleni védelme érdekében a felhasználó köteles a munkaállomást zárolni, jelszavas képernyőkímélővel védeni, illetve ha ez nem lehetséges, köteles a munkaállomásból kijelentkezni, vagy azt kikapcsolni, amennyiben azt felügyelet nélkül hagyja. Az automatikus képernyőzárolást lehetőség szerint ki kell kényszeríteni.
31. A munkaállomást a munkaidő végén, de legkésőbb a munka befejezésekor – eltérő rendelkezés hiányában – a felhasználó köteles kikapcsolni.
32. Amennyiben a munkaállomást több személy is használhatja, a felhasználó a munkaállomást csak akkor hagyhatja el, ha minden futó programból és az azonosított kapcsolatból is kijelentkezett.
33. A felhasználó a rendelkezésére bocsátott, hordozható informatikai, irodatechnikai, multimédiás, oktatási eszközt, mobil eszközt vagy adathordozót köteles megőrizni, az illetéktelen hozzáféréstől személyes felügyelettel vagy az eszköz, adathordozó elzárásával megvédeni.
34. Az Egyetem vezető beosztású munkavállalói jogosultak és kötelesek meghatározni az irányításuk alá tartozó foglalkoztatottak munkavégzéséhez szükséges informatikai, irodatechnikai, multimédiás és kommunikációs eszközök körét, a használandó informatikai rendszerek és az ahhoz szükséges jogosultságok körét.
35. A vezetők kötelesek gondoskodni az irányításuk alá tartozó foglalkoztatottak informatikai biztonsági ismereteinek naprakészen tartásáról.
36. A vezetők az informatikai biztonsági előírások megsértésének észlelése esetén kötelesek:
    a) azonnal megtenni a szükséges intézkedéseket a biztonság helyreállítása érdekében,
    b) amennyiben meghatározható rendszerre korlátozódik a biztonsági előírások sérülése, akkor indokolt esetben kezdeményezik a rendszer használatának felfüggesztését,

c) kivizsgálni a biztonsági esemény körülményeit, különös tekintettel a személyes felelősség megállapítására,
d) a személyes felelősség megállapítását követően felelősségre vonást kezdeményezni.

37. Az üzemeltető, fejlesztő munkakörrel, feladatkörrel rendelkező foglalkoztatottak a felhasználói jogosultságokon túlmutató többletjogosultságaikat csak a Szabályzattal összhangban, rendeltetésszerűen használhatják.

AZ EGYETEMMEL POLGÁRI JOGI JOGVISZONYBAN ÁLLÓ SZEMÉLYEKRE VONATKOZÓ RENDELKEZÉSEK

38. A METU informatikai rendszereihez és eszközeihez kizárólag érvényes és hatályos szerződés alapján, és a felhasználói jogosultság meghatározásával, dokumentáltan férhet hozzá.

A FELHASZNÁLÓ AZONOSÍTÁSA ÉS FELJOGOSÍTÁSA A RENDSZER HASZNÁLATÁRA, JELSZÓHASZNÁLAT

39. A felhasználó az informatikai rendszert csak egyértelmű azonosítást követően, a számára meghatározott és biztosított jogosultságok keretei között használhatja.

40. Az informatikai rendszer használata során a felhasználók egyedi azonosítását folyamatosan biztosítani kell.

41. Minden felhasználót kizárólagos személyi használatú egyedi azonosítóval kell ellátni, amelyhez egyedi jelszót kell rendelni.

42. A felhasználók azonosítójának a keresztnév első betűjét és a vezetéknevet tartalmaznia kell. Kivételt képeznek az operációs rendszerek különleges, előre rögzített azonosítói és a különleges informatikusi feladatkört ellátó foglalkoztatottak által használt speciális és teszt felhasználói nevek, továbbá az adatbázis-kapcsolatok során használt technikai felhasználók.

43. A felhasználói jelszónak legalább az alábbi követelményeket teljesítenie kell – melyet a rendszer automatikusan ellenőriz és megkövetel:
a) legalább 8 karakter hosszú,
b) kis- és nagybetűket és számokat vegyesen tartalmaz,
c) nem tartalmazhat könnyen kitalálható, ismétlődő karaktersorozatot,
d) nem utalhat a felhasználó személyére,
e) érvényességi ideje legfeljebb 90 nap.

44. A jelszó megváltoztatása kötelező:
a) a felhasználói azonosító informatikai rendszerbe történt felvételét követő első bejelentkezéskor,
b) az informatikai üzemeltető szervezeti egység munkatársa általi újbóli jelszóbeállítást, felülírást követően,
c) ha a jelszó illetéktelen személy tudomására juthatott, vagy bármilyen módon nyilvánosságra kerülhetett,
d) az érvényességi idő lejártakor.

45. A felhasználó köteles a jelszót bizalmasan őrizni, illetéktelenek általi megismerését kizárni. Tilos a jelszót más által megismerhető módon feljegyezni, azt mással bármilyen formában közölni.

A HÁLÓZAT ÉS AZ INTERNET HASZNÁLATA

46. A belső hálózathoz csatlakozó METU által biztosított munkaállomás használata során a vírusvédelmi előírásokat folyamatosan érvényesíteni kell, mely központilag biztosított, melynek kikapcsolása, megkerülése szigorúan tilos.

47. A belső hálózathoz csatlakozó METU által biztosított munkaállomásra csak a munkavégzéshez

szükséges adatállományok, programok tölthetők, illetve telepíthetők. Ezen eszközökre nem telepíthető, nem másolható, ideiglenesen sem, illetve a belső hálózaton nem tehető közzé olyan adatállomány, információ, amely

a) jogszabályt sért, így különösen adatvédelmi, szerzői jogvédelmi, személyiségvédelmi előírásba ütközik,

b) a belső hálózat rendeltetésszerű működését, biztonságát veszélyezteti vagy veszélyeztetheti, így különösen annak erőforrásait indokolatlanul, vagy szándékosan túlzott mértékben, pazarló módon veszi igénybe.

48. Az Egyetem az internetelérés magáncélra történő használatát korlátozza. A munkavállalók internetelérésének magáncélra történő használatának korlátozásáról, annak terjedelméről a munkavállaló közvetlen felettese jogosult rendelkezni. Indokolt esetben, figyelemmel a munkavállaló munkaköréhez tartozó feladataira, ezen korlátozás alól a munkavállaló közvetlen felettese felmentést adhat.

49. A nem a METU által biztosított munkaállomás nem csatlakoztatható a belső hálózathoz, kivéve az Informatikai igazgató vagy felettesei előzetes engedélyével, ebben az esetben a vírusvédelmi előírásokat hasonlóan a belső gépekhez érvényesíteni kell, a vírusvédelem kikapcsolása, illetve anélküli használata szigorúan tilos. Ezen eszközökön nem használható ezen időszak alatt olyan adatállomány, információ, amely a belső hálózat rendeltetésszerű működését, biztonságát veszélyezteti vagy veszélyeztetheti, így különösen annak erőforrásait indokolatlanul, vagy szándékosan túlzott mértékben, pazarló módon veszi igénybe.

50. Az internet hálózathoz csatlakoztatott eszközök minden esetben az azt használó személy saját felelősségébe tartoznak, így amennyiben a wifi hálózathoz csatlakoztatott eszköz – bizonyítható módon – a belső hálózaton levő bármely eszköz hibás működését, adatvesztést, vagy egyéb kárt okoz, az a használó felelőssége, és ellene kártérítési eljárás indítható.

AZ ELEKTRONIKUS LEVELEZŐRENDSZER HASZNÁLATA

51. A METU feladatainak végrehajtásához alkalmazott elektronikus levelezésben elsősorban a METU által biztosított, hivatali levelezési cím használható.

52. A magán levelezési címekről történő munkalevelezés az azt használó személyi felelőssége, ahogy az abban szereplő adatokért is kártérítési felelősséget vállal visszaélés, vétlen vagy szándékos károkozás esetén.

53. A belső levelezőrendszeren elsősorban hivatali és közösségi célú üzenetek továbbíthatók, kerülni kell a lánclevelek és egyéb nagyméretű magáncélú levelek tárolását a központi levelező rendszerben.

54. Kéretlen, ismeretlen levelek esetén alapos körültekintés nélkül tilos megnyitni a csatolt állományokat, a levélben szereplő hivatkozásokat, és ott a felhasználónévvel, jelszóval kapcsolatos adatokat megadni.

55. A METU által biztosított elektronikus levélcímet tilos nem feladatokhoz kapcsolódó külső levelezőlistákhoz, szolgáltatásokhoz csatolni, alapértelmezett címként megadni.

56. A METU levelezőrendszerében használt munkavállalói postafiókok a munkavállaló kilépését követően archiválásra kerülnek.

57. A hallgatói postafiókok archiválás nélkül törlésre kerülnek a hallgató jogviszonyának megszűnését követően.

AZ ÜZEMELTETÉS-BIZTONSÁG ÁLTALÁNOS KÖVETELMÉNYEI

58. Az informatikai rendszerek rendeltetésszerű működéséért, folyamatos rendelkezésre állásáért

az Informatikai igazgató felel.

59. A távoli segítségnyújtás (távsegítség) során a kliensoldali programot, amely bármilyen módon lehetővé teszi a felhasználó képernyőjén lévő információk távoli elérését, vagy input eszközeinek távvezérlését, csak a felhasználó indíthat el, azt automatikusan induló programként telepíteni tilos. Ez alól kivételt képeznek a METU oktatást támogató alkalmazásai. A távsegítség bevezetése és alkalmazása előtt a szolgáltatás tartalmáról, továbbá a távsegítség során elvégzett beavatkozásról a felhasználókat tájékoztatni kell.

60. A METU központilag szabályozhatja a munkaállomások képernyővédőjének, háttérképének, képernyőzárjának beállításait és az engedélyezett programok telepítését és tiltott, nem engedélyezett programok törlését.

61. A METU eszközeire az Informatikai Igazgatóság által nem engedélyezett programok telepítése, futtatása szigorúan tilos.

62. Az informatikai rendszerekben kezelt és tárolt adatok rendelkezésre állását rendszeres és indokolt esetben soron kívüli mentéssel kell biztosítani.

63. Az informatikai rendszerekben kezelt adatállományokat, amennyiben azok elérése a felhasználók számára napi munkavégzésük során nem szükséges, azonban őrzésük indokolt, archiválni kell.

VÍRUSVÉDELEM

64. A vírusvédelmi eljárásokat, a vírusvédelemre vonatkozó szabályozást, beleértve az intézkedési rendet, úgy kell kialakítani, hogy az
    a) a folyamatos vírusvédelmi felügyelet ellátását lehetővé tegye,
    b) támogassa a valós riasztások kiszűrését,
    c) alkalmas legyen a súlyos gondatlanságot, szándékosságot jelentő esetek felismerésére,
    d) lehetővé tegye az általános vírusbiztonsági helyzet értékelését,
    e) biztosítsa az új fenyegetések időben történő felismerését.

65. A vírusvédelemmel kapcsolatos üzemeltetési, üzemeltetés-felügyeleti feladatokat az Informatikai Igazgatóság látja el.

66. A vírusvédelem célja:
    a) a szakmai szabványokon alapuló, kielégítő mértékű, az arányosság elvén alapuló védelmi rendszer meghatározása,
    b) a rosszindulatú szoftverek hatásainak szabályozott és hatékony megelőzése és kivédése,
    c) eljárás biztosítása a bekövetkezett támadás elhárítására, a kár enyhítésére.

67. A METU belső hálózata munkaállomás és szerverszinten vírusvédettek, a hálózatokba kizárólag csak vírusellenőrzött adatok továbbítódhatnak.

68. A belső hálózat védelmében:
    a) a vírusvédelmi rendszer folyamatosan felügyelt,
    b) a vírusvédelmi rendszer központi szerverrel és menedzsment felülettel rendelkezik,
    c) a központi menedzsment alkalmas az üzembiztonsági felügyeletre, így a hibajelzésre, a jogtalan leállítás jelzésére, a vírus esemény felismerésére, központi kezelésére, riasztás adására, elemzési információ szolgáltatására,
    d) a vírusvédelmi rendszer képes a napon belüli többszöri frissítésre,
    e) a vírusesemények kezeltek,
    f) a vírushelyzet rendszeresen elemzett.

69. A METU vírusvédelmi feladatait az Informatikai Igazgatóság munkatársai látják el, akik:
    a) felelősek a vírusvédelem menedzsmentjéért,
    b) ismerik a METU vírusvédelmi rendszereit, figyelemmel kíséri az alkalmazott megoldások és

a szakmai követelmények változásait, a METU-ra irányuló fenyegetettséget,
c) folyamatosan figyelemmel kísérik és elemzik a METU vírusvédelmi helyzetét,
d) dokumentálják a víruseseményeket, felelősek a METU vírusvédelmi helyzetéről készülő éves jelentés elkészítéséért,
e) közreműködnek a vírusesemények és a biztonsági incidensnek minősülő vírusesemények kezelésében, szükség szerint intézkedést kezdeményeznek, ellátják a vírusvédelemmel kapcsolatos megelőzési és elhárítási feladatokat,
f) támogatják a felhasználók vírusvédelmi tevékenységét.

70. A METU informatikai igazgatója által megbízott koordinátor a 69. pontban foglaltakon túl:
a) ellátja a vírusvédelmi rendszerek működtetésének szakmai irányítását és felügyeletét,
b) felelős a METU vírusvédelme szakmai követelményeinek meghatározásáért és teljesítéséért,
c) irányítja és felügyeli a vírusvédelem technológiai feladatainak végrehajtását,
d) az előírásoknak megfelelően, valamint szükség szerint gondoskodik az alkalmazott vírusvédelmi eszközök frissítéseinek letöltéséről és elérhetőségéről,
e) javaslatot tesz a vírusvédelmi rendszerek fejlesztési irányainak kijelölésére,
f) közreműködik a vírusvédelmi beszerzések technológiai specifikálásában,
g) gondoskodik a vírusvédelmi eszközök telepítési és konfigurációs leírásainak, üzemeltetési eljárási rendjeinek elkészítéséről.

71. A vírusvédelem dokumentumai:
a) az éves jelentés, mely a gazdasági vezérigazgató-helyettes felé felterjesztett összefoglaló, melyet minden év február 1-ig köteles elkészíteni,
b) a vírusvédelmi jegyzőkönyv, melyet a belső hálózatokban előfordult, bármely munkaállomást vagy szervert érintő víruseseményről a vizsgálatot követően kell készíteni,
c) az eseti jelentés, melyet az informatikai igazgató által meghatározott esetekben, és időszakról kell készíteni.

72. A METU belső hálózatán a METU által biztosított munkaállomások vírusvédelmi követelményei:
a) kizárólag vírusvédelemmel rendelkező munkaállomás csatlakoztatható a METU belső hálózatára,
b) valósidejű vírusvédelmi eszköz alkalmazása kötelező,
c) a METU-ban rendszeresített vírusvédelmi eszközt kell használni,
legyen lehetőség egyedi vírusellenőrzésekre, a csatlakoztatható adathordozók és minden input adat ellenőrzésére,
d) a munkaállomás vírusminta-adatbázisa és víruskereső motorja automatikusan frissüljön,
e) a munkaállomás szabályrendszerét úgy kell beállítani, hogy a felhasználó ne tudja a vírusvédelmi eszközt kikapcsolni, azaz a vírusvédelem leállítása − a kényszerű, üzemviteli vagy hibaelhárítási okból történő kikapcsolás kivételével − tilos,
f) nem működő vírusvédelemmel a munkaállomás nem használható,
g) a munkaállomásokat felügyelő informatikai munkatársak részére ellenőrzési eszköz álljon rendelkezésre, hogy azonosíthatók legyenek azon számítógépek, amelyeken a víruskereső szoftver vagy a frissítés nem működik.

73. Szerverek vírusvédelmi követelményei:
a) hálózatos, vírusfenyegetettségnek kitett szerverek esetében, amennyiben a METU általi bevizsgálás alapján megfelelő védelmet adó, rendszerbe illeszthető vírusvédelmi eszköz rendelkezésre áll, azt kötelező alkalmazni,
b) kötelező vírusvédelmi eszközt alkalmazni valamennyi Windows szerveren,
c) valósidejű vírusvédelmi eszköz alkalmazása kötelező, hogy minden kimeneti és bemeneti eszköz és csatorna esetében biztosítva legyen a valósidejű vírusellenőrzés;
d) olyan beállításokat kell alkalmazni, hogy az állományok vírusellenőrzése közvetlenül a szerverre történő írás előtt megtörténjen;

e) teljes rendszer vírusellenőrzését ütemezetten, a feldolgozási időn kívül, legalább kéthetente egyszer végre kell hajtani.
f) a frissítések között legfeljebb 24 óra teljen el.

74. Elektronikus levelezés vírusvédelmi követelményei:
    a) minden, a METU rendszerébe beérkező elektronikus levél vírusellenőrzését el kell végezni,
    b) vírusesemény központi észlelése esetén a levél nem kerül a címzetthez,
    c) a víruseseményről értesíteni kell a címzettet,
    d) a vírusesemény naplózásra kerül.

75. A METU hálózatába érkező külső elektronikus levelek ellenőrzésére központi, hálózati szintű szűrést kell alkalmazni. A szabályrendszer beállításával biztosítani kell, hogy a spamként megjelölt levelek ne kerüljenek kézbesítésre.

76. Külső forrásból érkező adathordozók ellenőrzésének általános szabályai:
    a) a külső adathordozó – ha az adatok betöltése vagy felhasználása személyi számítógépen történik – ellenőrzése vírusvédelmi eszközzel; erről annak a felhasználónak kell gondoskodnia és azért felelősséget vállalnia, aki az adathordozó tartalmát a beviteli ponton az informatikai rendszerbe betölti,
    b) amennyiben az adathordozó vírust tartalmaz, azt a METU informatikai rendszereibe továbbítani, és feldolgozni tilos.

77. A felhasználó jelezni köteles, ha
    a) munkavégzése során azt tapasztalja, hogy munkaállomásán a vírusvédelem nem, vagy rendellenesen működik, a szoftver hibajelzéseket ad, a kézzel indított fájllellenőrzést vagy külső adathordozó ellenőrzését nem tudja elvégezni,
    b) a munkaállomás vírusvédelme vírusra utaló jelzést ad,
    c) munkaállomásán vírus jelenlétére utaló rendellenességet tapasztal.

78. Vírusesemény észlelésekor a felhasználó az észlelt víruseseményről haladéktalanul tájékoztatja az Informatikai Igazgatóságot akik a megfelelő kezelésről haladéktalanul gondoskodnak, azaz:
    a) az automatikusan elhárított vírusesemény észlelése vagy bejelentése esetén ellenőrzési kötelezettsége van,
    b) többszörös előfordulás észlelése esetén a munkaállomást vagy a szervert, illetve annak kapcsolatait át kell vizsgálni, a rendszer működését figyelemmel kell kísérni,
    c) sikertelen automatikus eltávolítás esetén az elhárítást személyes közreműködéssel kell végrehajtani,
    d) az érintett felhasználókat tájékoztatni kell,
    e) szükség esetén az érintett számítógépeken a munkavégzést meg kell tiltani,
    f) a vírusesemény elhárítása után a munkavégzés folytatását engedélyezni kell,
    g) gondoskodik a vírusesemény kivizsgálásáról és a vírusvédelmi jegyzőkönyv elkészítéséről, amennyiben az automatikus eltávolítás sikertelen volt.

ZÁRÓ RENDELKEZÉSEK

79. Jelen Szabályzat aláírása napján lép hatályba. Ezzel egyidejűleg hatályát veszti a Budapesti Metropolitan Egyetem 2017. március hó 21. napján kiadott Informatikai Biztonsági Szabályzata.

Budapest, 2019. október 11.

Dr. Bachmann Bálint, DLA sk.
rektor