A Budapesti Metropolitan Egyetem Informatikai Biztonsági Szabályzata

A Budapesti Metropolitan Egyetem informatikai rendszereinek/alkalmazásainak biztonságát garantáló eljárások és előírások egységes keretbe foglalása érdekében a Budapesti Metropolitan Egyetem (a továbbiakban METU) az Informatikai Biztonsági Szabályzatát (a továbbiakban: Szabályzat) a következőkben határozza meg.

A Szabályzat célja a METU 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.

I. A Szabályzat hatálya

A Szabályzat személyi hatálya kiterjed az Egyetem minden - informatikai rendszert használó - hallgatójára, valamint az oktatói és nem oktatói munkakörben foglalkoztatott valamennyi munkavállalójára (továbbiakban: dolgozó), illetve az Egyetemmel polgári jogviszonyban (pl. megbízási, vállalkozási) álló személyekre, szervezetekre.

A Szabályzat területi hatálya kiterjed az Egyetem valamennyi ingatlanára, képzési helyszínére és telephelyére, valamint külső helyszínen zajló rendezvényeire.

Az Egyetem különös gondot fordít arra, hogy az érintett személyek a Szabályzatot (eseti kivonatát) a szükséges mértékben megismerjék és betartsák.

A Szabályzat tárgyi hatálya kiterjed a METU informatikai rendszereire, alkalmazásaira és azok moduljaira (a továbbiakban együtt: rendszer), az informatikai rendszerekhez csatlakoztatható informatikai, irodatechnikai, multimédiás eszközökre és adathordozókra, az informatikai rendszerekben kezelt, feldolgozott, tárolt adatokra, dokumentumokra, valamint az előzőekben felsoroltakkal kapcsolatos informatikai és biztonsági tevékenységre.

II. Értelmező Rendelkezések

A Szabályzatban alkalmazott, a Szabályzat értelmezését, továbbá az informatikai biztonság tárgykörét érintő informatikai fogalmak:

1) **Adat**: elektronikus formában megjelenő tény, feltevés (elemi információ).

2) **Adatállomány**: az egy nyilvántartásban kezelt adatok összessége.

3) **Adatátvitel**: elektronikus adatok informatikai rendszerek közötti továbbítása, amely lehet párbeszédre épülő (on-line) vagy nem párbeszédre épülő (off line) elektronikus kapcsolat.

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

5) **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.

6) **Adathordozó**: az elektronikus adatkezelő rendszerhez csatlakoztatható vagy abba beépített olyan eszköz, amelynek segítségével az elektronikus adatok tárolása, terjesztése megvalósítható. Pl. CD, DAT, DVD, merevlemez, USB-memória.

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, megsemmisítése, valamint az adatok további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (pl. ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítése.

8) **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).

9) **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.

10) **Autentikáció (Azonosítás)**: informatikai eljárás, amelynek során a felhasználó az informatikai rendszerben az autorizáció megszerzése érdekében igazolja személyazonosságát. Lehet tudás alapú (pl. jelszavas), birtoklás alapú (pl. tokenes) vagy tulajdonság alapú (pl. biometrikus), illetve ezek kombinációi.

11) **Autorizáció (Feljogosítás)**: azonosításra épülő informatikai eljárás, amelynek eredményeként egyértelműen azonosított személy (eszköz) a feladatai ellátásához meghatározott hozzáférési, eljárási vagy egyéb jogosultságokat kap.

12) **Belső hálózat (Intranet)**: a METU saját, védett hálózata, amelynek rendeltetése, hogy elérhetővé tegye

- a funkcionális rendszereket,
- az oktatási rendszereket,

- a belső kommunikációs rendszert,
- a belső intranet portált,
- a munkavégzéshez szükséges egyéb alkalmazásokat, adatbázisokat,
- a felhasználók számára biztosított – személyes és csoportos használatú – elektronikus tárhelyeket.

13) **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.

14) **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.

15) **Biztonsági kockázat**: az informatikai rendszerrel szembeni fenyegetés, amely a rendszer rendeltetésszerű működését és/vagy a rendszerben kezelt adatok bizalmasságát, rendelkezésre állását, sértetlenségét veszélyezteti vagy veszélyeztetheti.

16) **Biztonsági megfelelőség**: az informatikai rendszer tulajdonsága: mennyiben, milyen mértékben felel meg az informatikai biztonsági követelményeknek.

17) **Felhasználó**: az informatikai rendszert – feladatai ellátásához – igénybe vevő személy.

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

19) **Funkcionális rendszer (alkalmazás)**: a METU mint szervezet működését támogató informatikai rendszer (alkalmazás).

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

21) **Hálózat:** számítógépek és hozzájuk kapcsolódó eszközök meghatározott szabályok szerinti összekapcsolása, amely adat- és információcserét tesz lehetővé. Alapelemei: a szerver (kiszolgáló eszköz), a hálózat működését biztosító aktív és passzív hálózati elemek (router, bridge stb.) és a

munkaállomások. Kiterjedés és az alkalmazott technológia alapján három fő típusa: helyi hálózat (LAN), országra illetve városokra kiterjedő hálózat (MAN) és világméretű hálózat (WAN).

22) **Hardver**: az informatikai rendszer (különösen: számítógép) fizikai elemei; a működéshez szükséges műszaki-technikai eszközök összefoglaló neve.

23) **Információbiztonság**: az a dinamikusan változó állapot, amikor az információ – megjelenési formájától függetlenül – védelmet élvez, azaz bizalmassága, rendelkezésre állása és sértetlensége biztosított.

24) **Információvédelem**: szervezeti, személyi, fizikai, informatikai és adminisztratív előírások kidolgozása és intézkedések végrehajtása az információbiztonság érdekében.

25) **Informatikai alkalmazás**: számítógépen, illetve egyéb informatikai eszközön futó program, amelynek célja meghatározott tevékenységek végrehajtása, terítése központilag történik, üzemeltetése központilag vagy helyileg is történhet, jogosultságkezelése, valamint funkcionális és biztonsági naplózása biztosított, és amely állhat egy vagy több (program) modulból.

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

25) **Informatikai biztonsági követelmények**: az informatikai rendszer használatával, üzemeltetésével és fejlesztésével kapcsolatos elvárások.

26) **Informatikai környezet**: azon információtechnológiai megoldások (hardver és a hozzá tartozó alapszoftverek) összessége, amelyek biztosítják az informatikai rendszerek (alkalmazások) logikai működési feltételeit, meghatározzák alapvető adat(bázis)kapcsolatait.

27) **Informatikai modul**: a METU informatikai rendszereiben az alkalmazáson belül a legkisebb elkülöníthető önálló funkcióval bíró olyan egység.

28) **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.

29) **Informatikai segédalkalmazás**: az informatikai rendszerrel/alkalmazással kapcsolatos támogató tevékenység elősegítésére szolgáló olyan kisalkalmazás, amely adatkezelési és adatfeldolgozási tevékenységet nem végez.

30) **Informatikai szolgáltatás**: a METU informatikai rendszereiben az alkalmazáson belül a felhasználó számára elérhető olyan funkció vagy funkcióösszesség, amely nem értékelhető modulként.

31) **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.

32) **Kritikus informatikai rendszer/alkalmazás**: olyan informatikai rendszer/alkalmazás, amely legfeljebb 4 óra időtartamig nélkülözhető anélkül, hogy abból a METU-nak bármilyen kára származna.

33) **Kommunikációs rendszer (alkalmazás)**: a METU kommunikációs csatornáit (levelező, üzenetküldő valamint VOIP) biztosító informatikai rendszer (alkalmazás).

34) **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.

35) **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.

36) **Munkaállomás**: a felhasználó számára biztosított számítógép; lehet asztali vagy hordozható (laptop, notebook stb.).

37) **Oktatási rendszer**: a METU, mint oktatási intézmény tevékenységét támogató, a hallgatókat információkkal és segédanyagokkal ellátó, valamint az oktatást segítő informatikai rendszer (alkalmazás)

38) **Napló**: az informatikai rendszerben bekövetkező eseményeket, felhasználói tevékenységeket és ezek időpontját rögzítő, a rendszer által automatikusan kezelt adatállomány, amely a változások észlelését és a számon kérhetőséget biztosítja.

39) **Naplózás**: az informatikai rendszerben bekövetkező események, felhasználói tevékenységek és ezek időpontjának automatikus rögzítése a változások észlelése és a számon kérhetőség biztosítása érdekében.

40) **Program**: számítógépes nyelven megírt utasítássorozat. Állhat egyetlen programmodulból vagy programmodulok halmazából.

41) **Rendelkezésre állás**: annak biztosítása, hogy az informatikai rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek.

42) **Rendszergazda**: olyan személy, akinek a feladata az operációs rendszerek, adatbázis-kezelő rendszerek és egyéb rendszerprogramok felügyelete és kezelése. A rendszerek által biztosított legmagasabb jogosultsággal rendelkezik. A rendszerszintű jogosultságok kezelésével megbízott személy.

43) **Személyi biztonsági követelmények**: az informatikai rendszert használó, üzemeltető vagy fejlesztő személyekkel szembeni szakmai és biztonsági elvárások, amelyek a szándékos vagy vétlen emberi magatartásból, tevékenységből eredő biztonsági kockázatok kiküszöbölését vagy minimalizálását célozzák.

44) **Szervezeti biztonsági követelmények**: az informatikai rendszert használó, üzemeltető vagy fejlesztő szervezettel szembeni elvárások, amelyek arra irányulnak, hogy a biztonságot érintő munkafolyamatok, munkakörök és felelősségi szabályok egyértelműen tisztázottak, szabályzatban rögzítettek legyenek

45) **Szoftver**: a számítógép, az informatikai rendszer logikai elemei; a működtető programok (rendszerprogramok, operációs rendszerek) és a felhasználói programok (alkalmazások) összefoglaló neve.

46) **Teljes dokumentáció**: a Szabályzatban előírt dokumentáció (pl. fejlesztői dokumentáció, felhasználói és üzemeltetői leírás/kézikönyv, tesztelési dokumentáció).

46) **Tesztrendszer**: olyan informatikai rendszer (környezet), amelynek célja a fejlesztés vagy bevezetés alatt álló program kipróbálásának, oktatásának támogatása.

III. Az informatikai rendszerek osztályozása

Az egyes informatikai rendszerekkel és adathordozókkal kapcsolatos tevékenység tervezésének, végrehajtásának, a vonatkozó szabályozás kidolgozásának alapja, ezek osztályozása.

Az informatikai rendszer az alkalmazás oka alapján lehet:

a) funkcionális informatikai rendszer,

b) oktatási informatikai rendszer,

b) kommunikációs informatikai rendszer.

Az informatikai rendszer a tulajdoni viszonyok alapján lehet :

a) saját tulajdonú informatikai rendszer,

b) idegen tulajdonú informatikai rendszer.

Az informatikai rendszer felügyelet szerint lehet:

a) METU által felügyelt informatikai rendszer,

b) idegen szervezet által felügyelt informatikai rendszer

IV. Szervezeti informatikai biztonsági követelmények

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.

V. Személyi informatikai biztonsági követelmények

A Szabályzat megismeréséről és elfogadásáról írásban kell nyilatkoznia a METU minden munkavállalójának, valamint biztosítani kell a Szabályzat megismerését a hallgatók részére.

Az informatikai rendszerekhez, a rendszerekben tárolt adatokhoz kizárólag a fenti nyilatkozatot megtevő személyek férhetnek hozzá.

A nyilatkozatot minden munkavállalónak a belépéskor ki kell tölteni. A bevezetéskor a METU-val jogviszonyban álló munkavállalók a Szabályzatot annak kihirdetését követő 2 hónapon belül aláírni kötelesek.

A HR Iroda a nyilatkozatokat a személyi anyagokhoz csatolva megőrzi.

VI. Fizikai biztonsági követelmények

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

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.

VII. Informatikai biztonsági követelmények

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.

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.

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

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

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.

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

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

VIII. Adminisztratív biztonsági követelmények

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.

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

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.

IX. A felhasználó jogai és kötelezettségei

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

A felhasználó a rendelkezésére bocsátott informatikai, irodatechnikai, oktatási és kommunikációs eszközöket csak a METU céljaival, feladataival kapcsolatos, a munkaköri feladatai elvégzéséhez szükséges tevékenység céljára, a számára megállapított jogosultságok keretein belül, rendeltetésszerűen használhatja.

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 a Szabályzat előírásainak felhasználó általi be nem tartása miatt kerülhetett sor.

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.

A munkaállomást a munkaidő végén, de legkésőbb a munka befejezésekor – eltérő rendelkezés hiányában – a felhasználó köteles kikapcsolni.

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.

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.

Az Egyetem vezető beosztású munkavállalói jogosultak és kötelesek meghatározni az irányítása alá tartozó foglalkoztatottak munkavégzéséhez szükséges informatikai, irodatechnikai, multimédiás és kommunikációs eszközök körét, a használandó informatikai rendszerek és az ahhoz szükséges jogosultságok körét.

A vezetők kötelesek gondoskodni az irányításuk alá tartozó foglalkoztatottak informatikai biztonsági ismereteinek naprakészen tartásáról.

A vezetők az informatikai biztonsági előírások megsértésének észlelése esetén kötelesek

1. azonnal megtenni a szükséges intézkedéseket a biztonság helyreállítása érdekében, továbbá
2. amennyiben meghatározható rendszerre korlátozódik a biztonsági előírások sérülése, akkor indokolt esetben kezdeményezi a rendszer használatának felfüggesztését,
3. kivizsgálni a biztonsági esemény körülményeit, különös tekintettel a személyes felelősség megállapítására,
4. a személyes felelősség megállapítását követően felelősségre vonást kezdeményezni.

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

X. Az Egyetemmel polgári jogviszonyban álló külső személyre vonatkozó rendelkezések

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

XI. A felhasználó azonosítása és feljogosítása a rendszer használatára, jelszóhasználat

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

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

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

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.

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.

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.

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

XII. A hálózat és az internet használata

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

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.

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.

A nem METU által biztosított munkaállomás nem csatlakoztatható a belső hálózathoz, kivéve az Infomatikai 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.

Az internet (WIFI) 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.

XIII. Az elektronikus levelezőrendszer használata

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

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.

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

Kéretlen, ismeretlen levelek esetén alapos körültekintés nélkül tilos megnyitni a csatolt állományokat, a levélben szereplő hivatkozásokat, és ott a felhasználónévvel, jelszóval kapcsolatos adatokat megadni. (AZ IT SOSEM KÉRHET LEVÉLBEN JELSZAVAKAT, BIZALMAS INFORMÁCIÓKAT!)

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

A METU levelezőrendszerében használt munkavállalói postafiókok a munkavállaló kilépését követően archiválásra kerülnek, a mellékelt 1. számú nyilatkozat elfogadásával hozzájárul, hogy azt hivatali célra a METU használhassa.

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

XIV. Az üzemeltetés-biztonság általános követelményei

Az informatikai rendszerek rendeltetésszerű működéséért, folyamatos rendelkezésre állásáért az Informatikai Igazgató felel.

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.

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

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

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

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

XV. Vírusvédelem

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) tegye lehetővé az általános vírusbiztonsági helyzet értékelését,
e) biztosítsa az új fenyegetések időben történő felismerését.

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

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, illetve kivédése,
c) eljárás biztosítása a bekövetkezett támadás elhárítására, a kár enyhítésére.

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

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.

A METU vírusvédelmi feladatait az Informatikai Igazgatóság tagjai 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 fenyegetettséggel tisztában van,
c) folyamatosan figyelemmel kíséri és elemzi a METU vírusvédelmi helyzetét,
d) dokumentálja a víruseseményeket, felelős a METU vírusvédelmi helyzetéről készülő éves jelentés elkészítéséért,
e) közreműködik a vírusesemények és a biztonsági incidensnek minősülő vírusesemények kezelésében, szükség szerint intézkedést kezdeményez, ellátja a vírusvédelemmel kapcsolatos megelőzési és elhárítási feladatokat
f) támogatja a felhasználók vírusvédelmi tevékenységét

A METU Informatikai Igazgatója által megbízott koordinátor a fentieken felül

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.

Vírusvédelem dokumentumai:

a) Éves jelentés, mely a Gazdasági vezérigazgató-helyettes felé felterjesztett összefoglaló, melyet minden év február 1-ig köteles elkészíteni
b) Vírusvédelmi jegyzőkönyvet a Belső hálózatokban előfordult, bármely munkaállomást vagy szervert érintő víruseseményről a vizsgálatot követően el kell készíteni.
c) Eseti jelentést az Informatikai Igazgató által meghatározott esetekben, és időszakról kell készíteni.

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.
d) Legyen lehetőség egyedi vírusellenőrzésekre, a csatlakoztatható adathordozók és minden input adat ellenőrzésére.
e) A munkaállomás vírusminta-adatbázisa és víruskereső motorja automatikusan frissüljön.
f) A munkaállomás szabályrendszerét úgy kell beállítani, hogy a felhasználó ne tudja a vírusvédelmi eszközt kikapcsolni, azaz a vírusvédelem leállítása tilos. Kivétel a kényszerű, üzemviteli vagy hibaelhárítási okból történő kikapcsolás.
g) Nem működő vírusvédelemmel a munkaállomás nem használható.
h) A munkaállomásokat felügyelő informatikai munkatársak részére ellenőrzési eszköz álljon rendelkezésre, hogy azonosíthatók legyenek azon számítógépek, amelyeken a víruskereső szoftver vagy a frissítés nem működik.

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 minden Windows szerveren.
c) Valósidejű vírusvédelmi eszköz alkalmazása kötelező: 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.
i) Frissítések gyakorisága legfeljebb 24 óra.

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. A víruseseményről értesíteni kell a címzettet. A vírusesemény naplózásra kerül.
c) 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.

Külső forrásból érkező adathordozók ellenőrzésének általános szabályai:

a) A külső adathordozót - ha az adatok betöltése vagy felhasználása személyi számítógépen történik - ellenőrizni kell 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.

A felhasználó jelenteni köteles saját maga, vagy felettese közreműködésével, ha

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

Vírusesemények kezelése:

A felhasználó az észlelt víruseseményt haladéktalanul jelenti közvetlenül vagy vezetője közvetítésével az Informatikai Igazgatóságnak, 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 (a vírusesemény elhárítása után a munkavégzés folytatását is engedélyezni kell),
f) gondoskodik a vírusesemény kivizsgálásáról és a vírusvédelmi jegyzőkönyv elkészítéséről, amennyiben az automatikus eltávolítás sikertelen volt.

XVI. Záró rendelkezések

1. A Budapesti Metropolitan Egyetem Szenátusa 2017. március 17. napi ülésén megtárgyalta és elfogadta az Informatikai Biztonsági Szabályzatot.

2. A Szabályzat szövegét magyar és angol nyelven közzé kell tenni, és hozzáférhetővé kell tenni az Egyetem minden polgára számára.

3. A Szabályzat 2017. március hó 21. napján lép hatályba.

Dr. habil. Vass László CSc

rektor

Budapesti Metropolitan Egyetem