



AZ ÓBUDAI EGYETEM Informatikai Felhasználói Szabályzata

BUDAPEST, 2017.

(2017. november 14. napjától hatályos, 1. verziószerű változat)

Tartalomjegyzék

PREAMBULUM	3
ELSŐ RÉSZ: Általános rendelkezések.....	4
A szabályzat hatálya	4
Értelmező rendelkezések.....	4
MÁSODIK RÉSZ: Informatikai szolgáltatások igénybevétele	5
Az informatikai szolgáltatások célja	5
Az Egyetem polgárainak jogai	5
A szolgáltatást igénybe vevő kötelessége	5
A szolgáltatások igénybevétele során tiltott tevékenységek	6
A jogok korlátozása.....	6
A szolgáltatást igénybevevő büntetőjogi felelőssége	6
Felhasználók, erőforrások és szolgáltatások névhasználata	7
HARMADIK RÉSZ: Informatikai biztonsági szabályok.....	7
Az informatikai biztonsági szabályok célja és feladata	7
A számítógép-használat általános alapelvei	8
Vírusvédelem.....	9
Kéretlen levelek, reklámok szűrése (spam)	9
Elektronikus levelezéssel kapcsolatos biztonsági szabályok	10
Az internethasználattal kapcsolatos biztonsági szabályok.....	11
Hálózathasználattal kapcsolatos biztonsági szabályok.....	11
Hozzáférés ellenőrzése	13
NEGYEDIK RÉSZ: Kiemelt informatikai rendszerek használati szabályai.....	13
A NEPTUN integrált tanulmányi rendszerrel kapcsolatos szabályok.....	13

PREAMBULUM

Az Óbudai Egyetem (a továbbiakban: Egyetem) Szenátusa a nemzeti felsőoktatásról szóló 2011. évi CCIV. törvényben előírtak alapján az informatikai felhasználókra vonatkozó szabályzatot az alábbiakban állapítja meg.

Az Informatikai Felhasználói Szabályzat (a továbbiakban: Szabályzat) az Egyetem informatikai rendszerének rendeltetésszerű használatához kiadott szabályok gyűjteménye, amelyben foglaltak betartása minden felhasználó és az Egyetem közalkalmazottjai részére kötelező érvényű, és amely szabályok tudomásulvételének a számítástechnikai eszközön megkezdett munkavégzés tekinthető.

A Szabályzat célja, hogy meghatározza az informatikai infrastruktúra felhasználóira vonatkozó jogokat, felelősségi köröket és feladatokat. Az egyértelmű felelősség meghatározása érdekében kijelöli az egyes infrastrukturális elemekre és szolgáltatásokra vonatkozó felelősségi köröket és szolgáltatási határokat, valamint meghatározza a szabálytalan használat szankcióit.

ELSŐ RÉSZ: Általános rendelkezések

A szabályzat hatálya

1. § (1) A Szabályzat személyi hatálya kiterjed:

- a) az Egyetem valamennyi hallgatójára és közalkalmazottjára,
- b) az Egyetem informatikai rendszerével, szolgáltatásaival szerződéses, vagy más módon kapcsolatba kerülő természetes és jogi személyekre, jogi személyiséggel nem rendelkező szervezetekre (a továbbiakban: külső személy) a velük kötött szerződésben, megállapodásban rögzített mértékben. A Szabályzatban foglaltak tudomásulvételét, valamint a titoktartásra vonatkozó szabályok betartását a szerződéses partnerrel megkötött szerződésben rögzíteni kell,
- c) minden olyan személyre, aki használja az Egyetem informatikai infrastruktúráját.

(2) A Szabályzat tárgyi hatálya kiterjed az Egyetem tulajdonában lévő, vagy az általa üzemeltetett valamennyi meglévő, illetve fejlesztés alatt álló és a jövőben fejlesztendő informatikai rendszerre, az adatok, szoftverek teljes körére, továbbá azok környezetét alkotó rendszerelemekre, azok teljes életciklusában (a fejlesztés előkészítésétől a rendszerből történő kivonásig), függetlenül azok területi elhelyezkedésétől.

Értelmező rendelkezések

2. § E szabályzat értelmében:

1. *aktív hálózati eszköz*: kapcsolók (switch-ek), forgalomirányítók (router-ek), vezeték nélküli hozzáférési pontok és egyéb eszközök, amelyek segítségével a hálózat üzemeltetése biztosítható.
2. *alkalmazásfelelős*: meghatározott rendszer üzemeltetéséért felelős felhasználó, aki kizárólag az adott rendszerre vonatkozóan rendelkezik többlet-, vagy egyedi jogosultsággal (például a NEPTUN vagy a POSZEIDON alkalmazásfelelősei).
3. *biztonsági incidens*: biztonsági problémát okozó jelenség.
4. *DNS (Domain Name Server)*: az IP címeket és a számítógépneveket egymáshoz rendelő adatbázis, mely általában külön kiszolgáló gépen fut.
5. *felhasználó*: az a természetes személy, aki az informatikai infrastruktúrát használja.
6. *felhasználói azonosító*: az intézményi címtárban tárolt egyedi azonosításra szolgáló rövid karaktersorozat, amely általában a felhasználó nevéből képződik.
7. *hálózat*: felhasználói számítógépek és/vagy szerverek közötti adatátvitelt biztosító közeg.
8. *informatikai erőforrások*: a hardver, szoftver eszközök összessége.
9. *internet*: a világháló.
10. *központi szolgáltatások*: levelezés, címtár, fájl kiszolgálás, web szolgáltatás, névszolgáltatás.
11. *LDAP (Light Weight Directory Access Protocol)*: nyílt szabványú címtár struktúra leíró nyelv.
12. *szerver feladatokat ellátó eszköz*: olyan számítógépek, szoftverek, vagy speciális eszközök, amelyek különböző szolgáltatásokat biztosítanak más számítógépek számára.
13. *üzemeltető*: az Egyetem informatikai üzemeltetéséért felelős személy, aki lehet az Informatikai Osztály, valamint speciális informatikai terek, laboratóriumok és műhelyek vonatkozásában az adott kar alkalmazottja is.

14. *VLAN*: a hálózat egy meghatározott része a feladatoknak megfelelően, logikai csoportba van szervezve.
15. *VPN szolgáltatás*: speciális hálózati elérés, amely az Egyetem hálózatához titkosított, és hitelesített kapcsolatot tesz lehetővé a világ bármely részéről.
16. *WiFi (Wireless Fidelity)*: szabványos vezeték nélküli adatátviteli technika. Legtöbb notebook, laptop számítógép, okostelefon gyárilag rendelkezik ilyen kapcsolódási lehetőséggel.
17. *Operátor*: egy az Egyetem informatikai rendszerének végberendezései üzemeltetéséért, valamint ügyfélszolgálat fenntartásért felelős informatikus.

MÁSODIK RÉSZ: Informatikai szolgáltatások igénybevétele

Az informatikai szolgáltatások célja

- 3. §** Az informatikai szolgáltatások célja az oktató-, kutató-, tudományos és fejlesztőmunka támogatása, a tanulás, az információszerezés elősegítése, a kapcsolatteremtés és -tartás új lehetőségeinek, valamint az információ szabad áramlásának biztosítása.

Az Egyetem polgárainak jogai

- 4. §** (1) Az Egyetem minden polgára alanyi jogon igénybe veheti az Egyetem alapvető informatikai szolgáltatásait. Alapvető informatikai szolgáltatások alatt az alábbiak értendők:
- a) a feladatok ellátásához szükséges informatikai erőforrások igénybevétele (felhasználói név és jelszó a megfelelő rendszerekhez),
 - b) szabad internet elérés felhasználói számítógépek igénybevétele (vezetékes és vezeték nélküli közegeken keresztül).
- (2) Az Egyetem minden dolgozója alanyi jogon igénybe veheti az Egyetem alapvető informatikai szolgáltatásain felül a központi szolgáltatásokat. Központi informatikai szolgáltatások alatt az alábbiak értendők:
- a) az elektronikus levelezés használata,
 - b) központi tárhely,
 - c) VPN szolgáltatás.

A szolgáltatást igénybe vevő kötelessége

- 5. §** Az informatikai szolgáltatásokat igénybe vevő köteles:
- a) jelen szabályzat előírásait betartani,
 - b) a törvényi előírásokat (különös tekintettel a szoftverekre vonatkozó szerzői jogi előírásokra) betartani,
 - c) az Egyetem polgárától elvárható etikai normákat betartani,
 - d) a használat során a tőle elvárható gondossággal és körültekintéssel eljárni

A szolgáltatások igénybevétele során tiltott tevékenységek

- 6. §** (1) Az informatikai szolgáltatások igénybevétele során tilos:
- a) aktív hálózati eszközöket engedély nélkül a hálózatra kapcsolni,
 - b) szerver feladatokat ellátó eszközöket engedély nélkül a hálózatra kapcsolni,
 - c) jogosultság nélkül informatikai szolgáltatást igénybe venni (betörési kísérlet vagy betörés),
 - d) idegen felhasználói azonosítót, kódot, jelszót használni,
 - e) saját felhasználói azonosítót kölcsönadni,
 - f) idegen jelszót kideríteni, ellopní, azzal bármilyen módon visszaélni,
 - g) az informatikai infrastruktúrát profitszerzést célzó, direkt üzleti célú tevékenységre és reklámra használni,
 - h) a szolgáltatásban részt vevő informatikai eszközöket (hardver és szoftver) módosítani, átkonfigurálni,
 - i) az informatikai szolgáltatásokkal bármely egyéb módon visszaélni,
 - j) az egyetemi email címet magánjellegű levelezésre használni.
- (2) Amennyiben a szolgáltatás igénybevevője az 5. §-ban vagy jelen § (1) pontjában foglaltak ellen vét, úgy a szolgáltatásból időlegesen vagy véglegesen kizárható.

A jogok korlátozása

- 7. §** (1) Az Egyetem polgárainak a 4. §-ba foglalt jogai műszaki, forgalmi okok, illetve az 5. §-ban tárgyalt kötelességek megszegése esetén korlátozható.
- (2) A műszaki, illetve forgalmi okokból történő korlátozás az alábbiak szerint valósulhat meg:
- a) adatátviteli sebesség behatárolása,
 - b) rendelkezésre álló tárterület behatárolása,
 - c) a szolgáltatás igénybe vehetőségének időbeli behatárolása.
- (3) A műszaki, illetve forgalmi okok megszűnésekor a korlátozást haladéktalanul fel kell oldani.

A szolgáltatást igénybevevő büntetőjogi felelőssége

- 8. §** (1) Az informatikai szolgáltatások igénybevétele során elkövetett bűncselekményekért (ilyen bűncselekmények többek között a betörésből fakadó károkozás vagy a szerzői és szomszédos jogok megsértése) a szolgáltatást igénybevevő büntetőjogi felelősséggel tartozik.
- (2) Jogszályon alapuló megkeresés alapján az Egyetem minden, a bűncselekmény elkövetésének gyanúja alá eső felhasználó adatait, valamint naplózott forgalmi adatait az illetékes hatóságoknak köteles kiszolgáltatni.

Felhasználók, erőforrások és szolgáltatások névhasználata

9. § (1) Minden erőforrás-tulajdonos – azaz minden olyan szervezeti egység vagy üzemeltető, amelynek saját kezelésébe tartozó egyéb szolgáltatást nyújtó informatikai eszköz képezi a tulajdonát – joga az általa üzemeltetett szolgáltatásokhoz felhasználói azonosítókat kiadni. Ezen azonosítóknak egyedieknek kell lenniük, az elnevezési szabályoknak alkalmazkodniuk kell a jogszabályok előírásaihoz és az egyetemi szabályzatokhoz. Az azonosító kiadás során, ha az azonosítót már más használja, akkor az újonnan jövőnek kell egy másik azonosítót választania.
- (2) Az azonosító kiválasztása előtt a szolgáltatás üzemeltetőjének konzultálnia kell az illetékes rendszergazdával abból a célból, hogy az új felhasználói azonosító, vagy kód egyedisége és a regisztrálása biztosítható legyen.
- (3) A szervezeti egységek azonosítóit, illetve a központi szolgáltatások azonosítóit az Informatikai Osztály tartja nyilván.
- (4) A központi informatikai szolgáltatások összehangolt működése lehetővé teszi, hogy egy felhasználó minden központi szolgáltatást ugyanazzal az azonosítóval és jelszóval vehessen igénybe.
- (5) Az elektronikus levelezés névhasználati szabályai:
- a levelezési címet a következő formában kell megalkotni: <vezetéknév>.<keresztnev>@<egység rövidítés>uni-obuda.hu; amennyiben pedig nem releváns az egység rövidítés használata: <vezetéknév>.<keresztnev>@uni-obuda.hu,
 - a szervezeti egységek saját információáramlásuk meggyorsítására úgynevezett terjesztési és/vagy levelezési listákat igényelhetnek. Az engedélyt az Informatikai Osztály vezetőjének írt levélben lehet kezdeményezni. A levelezési listát az igénylő szervezeti egységnek kell adminisztrálnia egy felelős személy kijelölésével. Terjesztési listában történő változásokat az Informatikai Osztály osztályvezetőnek kell jelezni.
- (6) A DNS nevek névhasználati szabályai:
- a nemzetközi regisztrált névhasználati rendszerben minden domain név az egyetem tulajdonát képezi,
 - a DNS nevet a következő formában kell megalkotni: <szolgáltatás>.<egység rövidítés>.uni-obuda.hu, például: www.bqk.uni-obuda.hu,
 - a szervezeti egység saját hatáskörébe tartozó szervert az alábbiak szerint kell azonosítani: <szervernév>.<egység rövidítés>.uni-obuda.hu, például: labor.nik.uni-obuda.hu,
 - a fentiekől eltérő DNS nevek a kancellár hozzájárulásával alkalmazhatók.

HARMADIK RÉSZ: Informatikai biztonsági szabályok

Az informatikai biztonsági szabályok célja és feladata

10. § (1) Az informatikai biztonsági szabályok biztosítják az Egyetem informatikai tevékenysége során kezelt eszközök, feldolgozott és továbbított adatok bizalmasságát, sértetlenségét, minimálisra csökkentik a szándékos vagy véletlen károkozást.
- (2) Az informatikai biztonsági szabályok feladata az informatikai rendszereket érintő veszélyforrások azonosítása, elhárítása és a védelmi intézkedések meghatározása.

A számítógép-használat általános alapelvei

11. § (1) Az Egyetemen működő számítógépek csak rendeltetészerűen, elsősorban munkavégzés céljából használhatók. Minden munkatárs csak a munkájának végzéséhez szükséges rendszerekhez kaphat jogosultságot.
- (2) Valamennyi felhasználó köteles e szabályzat rendelkezéseit betartani, és felelős az általa szándékosan vagy gondatlanságból az általa, a nevében, vagy 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) okozott szabályellenes cselekedetekért, károkért.
- (3) A szabályzat rendelkezései megsértésének gyanúja esetén a cselekményt az e célra felállított ad hoc bizottság köteles kivizsgálni. A kivizsgálás kapcsán vizsgálni kell:
- a biztonsági esemény bekövetkezésének okát,
 - az esetleges személyi felelősséget és
 - az okozott kár mértékét.
- (4) A vizsgálat eredményeképpen az alábbi szankciók kiszabására kerülhet sor:
- a szabályzat gondatlan megszegése esetén az elkövetőt figyelmeztetésben kell részesíteni,
 - a szabályzat szándékos megsértése esetén az elkövető a hálózat használatából ideiglenesen vagy véglegesen kizárható,
 - a szándékos elkövető – amennyiben a fentiekben túl kimutatható anyagi kár is keletkezett – köteles megtéríteni az általa okozott károkat a vonatkozó jogszabályok előírásai szerint,
 - bűncselekmény elkövetésének gyanúja esetén a munkáltatói jogkör gyakorlója kezdeményezi az elkövető felelősségére vonását.
- (5) Az Egyetem fenntart minden jogot a levelek kezelésével kapcsolatosan, a levelezés méretének, gyakoriságának, ha szükséges, a tartalmának ellenőrzésére, a működés korlátozására, amennyiben a levelező szerver és az internet csatlakozás kapacitásának kihasználása, valamint az Egyetem informatikai rendszerének biztonsága ezt megkívánja. Az ellenőrzés során a vonatkozó jogszabályi előírások betartásra kell, hogy kerüljenek.
- (6) Számítógépek használata során fokozott figyelmet kell fordítani a tűz-, érintés-, és munkavédelmi szabályokra. A számítógépek és monitorok szellőzőnyílásait letakarni nem szabad, elektromos csatlakoztatások használata során kiemelt figyelmet kell fordítani az áramütés veszélyére. Informatikai hálózat csatlakoztatását megbontani nem szabad.
- (7) Az Egyetemen működő számítógépekre csak az érvényes szabályozás mellett, az Informatikai Osztály engedélyével telepíthetők szoftverek. A beosztástól függően, vagy a megbízott informatikai személy végzi a telepítést, vagy a személyes használatban lévő gép felhasználója. Azokban az esetekben, amikor a számítógép személyes használatban van, a felhasználó felelőssége, hogy gépére illetéktelen szoftver ne kerüljön fel, és az elemi biztonsági feltételeknek a számítógép megfeleljen.
- (8) A felhasználóknak a munkaállomások használata során a következő általános szabályokat kell betartaniuk:
- személyes használatban lévő számítógépen felhasználói jogokkal ajánlott rendelkeznie,
 - felhasználói jogaihoz tartozó jelszóval védeni tudja számítógépe integritását,
 - illetéktelen személynek felhasználói jogát át nem adhatja,

- d) közepes vagy magas biztonsági kockázattal járó feladatvégzésekor a számítógépet senkinek át nem engedheti, információbiztonsági kockázatot nem okozhat,
 - e) biztonsági frissítésről gondoskodnia kell,
 - f) vírusvédelmi szoftver telepítéséről és frissítéséről gondoskodnia kell,
 - g) működő számítógépet csak jelszóval védett állapotban hagyhatja magára.
- (9) A személyes használatban lévő számítógépek, laptopok, tabletek, okostelefonok, stb. (a továbbiakban együttesen: eszköz) felhasználói, biztonsági szempontból felelnek a rájuk bízott eszköz biztonságáért. Ezzel kapcsolatosan a felhasználók feladatai:
- a) biztonsági frissítések, javítócsomagok telepítése,
 - b) személyes jogosultság beállítása,
 - c) rábízott érzékeny adatok védelme.
- (10) Nem személyhez kötött használatú eszközök esetében a fenti feladatokat az Informatikai Osztály végzi.
- (11) Amennyiben a személyes használatú eszköz biztonságáról a felhasználó nem maga kíván gondoskodni, köteles ezt a feladatot az operátorra bízni.

Vírusvédelem

- 12. §** (1) A veszélyes programok által okozott incidensek kiküszöbölésére meg kell tenni minden lehetséges lépést. Ennek érdekében hatékony vírusellenőrző alkalmazásokat kell telepíteni mind a munkaállomásokra, mind pedig a szerverekre és határvédelmi eszközökre.
- (2) A felhasználóknak be kell tartaniuk a vírusvédelemre vonatkozó elemi szabályokat és az egyéb intézkedéseket. Tisztában kell lenniük azzal, hogy vírusfertőzést kapni csak egy a biztonsági kockázatok közül. Előfordulhat, hogy a felhasználó maga válik vírusszűrővé, ezzel veszélyeztetve a környezetében dolgozó munkatársait, és a hálózat többi felhasználóját, illetve az világhálóra kikerülve ismeretlen felhasználókat is.
- (3) Az Informatikai Osztály minden évben biztosítja informatikai eszközei számára a legfrissebb vírusvédelmi szoftver legális használatát, illetve emailben küldött tájékoztatásokkal fejleszti a felhasználók biztonsági ismereteit. A munkahelyi munkaállomáson az Informatikai Osztály által javasolt vírusvédelmi rendszert kötelező használni. A laborokban elhelyezett számítógépek vírusvédelméről a laborfelelősöknek (a karok megbízással rendelkező alkalmazottjai) kell gondoskodni. A vírusvédelmi szoftver frissítéséről és a védelmi adatbázis aktualizálásáról a felhasználónak kell gondoskodnia.
- (4) Nem ellenőrzött forrásból származó állományokat használat előtt ellenőrizni kell.
- (5) A felhasználónak tilos lánclevelet, hamis vírusriasztásokat (hoax) küldeniük a központi levelező rendszeren keresztül.
- (6) Vírusfertőzésről, mint biztonsági incidensről, az Informatikai Osztályt a support@uni-obuda.hu email címen értesíteni kell abban az esetben is, ha a vírus terjedését sikerült helyben megakadályozni.

Kéretlen levelek, reklámok szűrése (spam)

- 13. §** A kéretlen levelek központi szűréséről az Informatikai Osztály üzemeltetésében álló szerverek gondoskodnak. A levelek kéretlenség minősítése egy folyamatos valószínűségi skálán történik, amely pontszám alapján három csoportba sorolja a leveleket:

- a) nem gyanús: változatlanul továbbításra kerül a címzettnek,
- b) gyanús: megjelölve kerül továbbításra a címzettnek,
- c) nagy biztonsággal spam: karanténba kerülnek, és a címzett tájékoztatást kap a visszatartott levélről, amelyet a karanténban megtekinthet. A levél egy hónap múlva törlődik.

Elektronikus levelezéssel kapcsolatos biztonsági szabályok

14. § (1) Az Egyetem valamennyi munkatársa jogosult felhasználói jogosultságot igényelni az elektronikus levelezéshez, vagyis a dolgozó munkába lépésekor a szükséges formanyomtatvány kitöltésével és aláírásával a központi levelezési rendszer tagjává válik. A formanyomtatványon és a mellékelt használati utasításon minden szükséges információt megkap, ami a levelező rendszer biztonságos használatához szükséges. A formanyomtatványt az 1. számú melléklet tartalmazza.

(2) Az Egyetem levelezőrendszere csak hivatalos kommunikációra használható. Az elektronikus levelezés szolgáltatás használata során az alábbi biztonsági szabályokat kell betartani:

- a) a felhasználó tudomásul veszi, hogy a központi levelezés során levelezési forgalma naplózásra kerül,
- b) a levelezési szolgáltatás mind a munkatársak közötti, mind az Egyetemen kívüli kapcsolattartásra felhasználható,
- c) az egyetemi postafiókok felső méretkorlátja: 5GB, ettől nagyobb méretű postafiókot indokolt esetben vezetői kérésre az Informatikai osztályvezető engedélyével állítható be,
- d) az elektronikus levélhez fájl csatolható, amelynek mérete korlátozott (teljes üzenet felső méret korlát: 20MB),
- e) az elektronikus levélhez csatolt fájl nem lehet futtatható állomány, nem lehet tömörített csomagban futtatható állomány, nem lehet továbbított reklám,
- f) a felhasználó tudomásul veszi, hogy a levélcím kötött, és nem változtathatja meg,
- g) a levelezési rendszeren tilos biztonsági szempontból érzékeny anyagot, egyetemi titkot, vagy üzleti titkot kijuttatni az internetre, külső postafiókba továbbítani,
- h) tilos a levelezési rendszeren keresztül olyan tartalmú levelet küldeni, amely bármilyen más személy, csoport vagy társaság személyes, illetve üzleti érdekeit sértheti,
- i) az elektronikus levelezési jogosultsággal rendelkező felhasználó csak saját nevében küldhet levelet, kivéve, ha erre felelős vezető utasítja, a postafiók belépési adatai át nem adhatók (a munkakör átadása esetén sem),
- j) kilépő közalkalmazott postafiókja a munkaviszonyának megszűnésével törlendő, kivételt képez ez alól a felsőbb vezetői utasításra megadható üzenet átirányítási kérelem,
- k) a felhasználó beállíthatja az automatikus válaszüzeneteket a munkavégzésére irányulóan (távollét, szabadság, akadályoztatás, helyettesítés jelzése),
- l) a rektor és kancellár jóváhagyásával az Egyetem teljes címtára felhasználásával egyetemi szintű körlevelet csak az Informatikai Osztályvezető küldhet, a levélmintát neki kell eljuttatni,
- m) tilos rasszista, szemérmes és jó ízlést sértő, valamint szélsőséges politikai nézeteket képviselő tartalmú levelet küldeni.

(3) A közalkalmazott tudomásul veszi, hogy amennyiben az Egyetem által rendelkezésére bocsátott e-mail címet nem munkavégzéssel kapcsolatos levelezésre használja, azt saját felelősségére teszi, tudomásul veszi

továbbá, hogy az Egyetem ellenőrzési jogosultsága azon elektronikus levelek tekintetében is fennáll, amelyeket a közalkalmazott az Egyetem más közalkalmazottjának küld.

(4) A munkáltatói jogkör gyakorlója a szabályzat rendelkezései megszegésének gyanúja esetén a közalkalmazott postaládájában lévő e-mailek fejlécének – amelyben szerepel a küldő és a fogadó e-mail címe, vagy neve, a levél tárgya, a küldés időpontja, a levél mérete – megtekintése után a közalkalmazottól a beérkező, illetőleg a kimenő hivatalos tárgyú elektronikus levelek nyomtatott formában való átadását kérheti. A levél kiadása – a (3) bekezdésben meghatározott esetet kivéve – csak harmadik személy személyiségi jogaira való hivatkozással tagadható meg.

Az internethasználattal kapcsolatos biztonsági szabályok

15. § (1) Az Egyetem belső hálózatában működő munkaállomások alaphelyzetben internet-eléréssel rendelkeznek. Kivétel alá esnek, és így az internetet nem érhetik el a különösen érzékeny adatokkal dolgozó munkaállomások.

(2) Felhasználói jogosultsággal azok a munkatársak rendelkeznek, akik valamilyen központi szolgáltatást használnak munkájuk során. Ilyenek például a Tanulmányi Osztály dolgozói, akik napi munkájuk döntő részében a NEPTUN Egységes Tanulmányi Rendszer bejelentkezett felhasználói.

(3) Az internet használata során az Egyetem fenntartja a jogot arra, hogy a felhasználók internet-forgalmát figyelemmel kíséresse és naplózza.

(4) A felhasználónak tisztában kell lennie azzal, hogy az internet használata biztonsági kockázattal jár, ami nem csak a személyes használatában lévő munkaállomást veszélyeztetheti, hanem a hálózat egyéb eszközeit is. A felhasználónak tisztában kell lennie azzal is, hogy nem használhatja az internet elérés lehetőségét jogszabályok és szabályok tudatos vagy szándékos megsértésére.

(5) Az internetről letöltött szoftver vagy fájl jogtisztaságáért az Egyetem, mint jogi személy felel, ezért fenntartja jogot, hogy a szabályok megsértőivel szemben szankciókat alkalmazzon. Illegális tevékenység céljára használt internet elérés felelősségre vonási eljárást eredményezhet.

(6) Az Internet használata során elvárt magatartás:

a) a felhasználó nem titkolja el személyazonosságát az internet használat közben,

b) az Egyetem dolgozói véleménynyilvánításhoz való jogukat a munkáltató jó hírnevét, jogos gazdasági és szervezeti érdekeit súlyosan sértő vagy veszélyeztető módon nem gyakorolhatják,

c) a szellemi tulajdon védelme az internetre is kiterjed,

d) amennyiben valamely incidens bekövetkezik, a felhasználó hozzájárul az összes érintett adat/információ tartalmának az ellenőrzéséhez, a jogszabályi előírásokban foglaltak betartása mellett.

Hálózathasználattal kapcsolatos biztonsági szabályok

16. § (1) Illetéktelen személy a kialakított rendszeren nem változtathat, végpontot át nem helyezhet és aktív- vagy szerver feladatokat ellátó eszközt a hálózatra nem kapcsolhat rá. A hálózat bővítésére vagy átalakításra kizárólag az Informatikai Osztály jogosult.

(2) A VLAN-ok biztonsági feladatot látnak el, mert elválasztják egymástól a részhálózatokat, ezzel biztosítva, hogy sérülés, vagy támadás esetén csak az adott részterületre korlátozódjék az esetleges kár. A VLAN-ok kialakítása az Informatikai Osztály hatásköre.

- (3) Az Egyetem hálózata nem használható az alábbi tevékenységekre:
- a) a mindenkor hatályos magyar jogszabályokba ütköző cselekmények előkészítése vagy végrehajtása, így különösen mások személyiségi jogainak megsértése (pl. rágalmozás), tiltott haszonszerzésre irányuló tevékenység (pl. piramisjáték), szerzői jogok megsértése (pl. szoftver nem jogszerű terjesztése),
 - b) profitszerzést célzó, direkt üzleti célú tevékenység és reklám,
 - c) a hálózat, a kapcsolódó hálózatok, illetve ezek erőforrásainak rendeltetészerű működését és biztonságát megzavaró, veszélyeztető tevékenység, ilyen információknak és programoknak a terjesztése,
 - d) a hálózatot, a kapcsolódó hálózatokat, illetve erőforrásait indokolatlanul, túlzott mértékben, pazarló módon igénybevevő tevékenység (pl. körlevelek, hálózati játékok, kéretlen reklámok),
 - e) a hálózat erőforrásaihoz, a hálózaton elérhető adatokhoz történő illetéktelen hozzáférés, azok illetéktelen használata, gépek/szolgáltatások – akár tesztelés céljából történő – túlzott mértékben való szisztematikus próbálgatása,
 - f) a hálózat erőforrásainak, a hálózaton elérhető adatoknak illetéktelen módosítására, megrongálására, megsemmisítésére vagy bármely károkozásra irányuló tevékenység,
 - g) másokra nézve sértő, vallási, etnikai, politikai vagy más jellegű érzékenységet bántó, zaklató tevékenység (pl. pornográf/pedofil anyagok tárolása, közzététele),
 - h) hálózati üzenetek, hálózati eszközök hamisítása: olyan látszat keltése, mintha egy üzenet más gépről vagy más felhasználótól származna (spoofing).
- (4) A felhasználók kötelességei a hálózat használata során:
- a) a felhasználók kötelessége a Szabályzat megismerése és az abban foglaltak betartása, valamint együttműködni a hálózat üzemeltetőivel a szabályzat betartatása érdekében,
 - b) a felhasználó viseli a felelősséget minden műveletért, amely az adott felhasználóhoz tartozó azonosítóval kerül végrehajtásra,
 - c) a felhasználó kötelessége és felelőssége, hogy a munkahelyén jogtisztan szoftvereket használjon.
- (5) A felhasználók jogai a hálózat használata során:
- a) a felhasználónak joga van a felhasználói fiókhoz való hozzáféréshez. Az egyetemen ez a központi szolgáltatás az oktatóknak az egyetem üzemeltetése alatt álló asztali és hordozható számítógépeivel (saját tulajdonú eszköz esetén: amennyiben elfogadja a szabályzat minden utasítását és alkalmazza azokat a saját üzemeltetése alá eső kliens gépre is), a hallgatóknak pedig a kari laborokban az intézmény gépeivel vagy saját eszközeik használatával, vezeték nélküli hálózati kapcsolaton keresztül válik lehetővé (ez esetben a felhasználó elfogadja a szabályzat minden utasítását és alkalmazza azokat a saját üzemeltetése alá eső kliens gépre is),
 - b) a rendszer technikai problémáiról (tervezett vagy rendkívüli eseményekről) tájékoztatni kell a felhasználókat,
 - c) a felhasználók számára elérhető módon közzé kell tenni a felhasználókra vonatkozó szabályok érvényes változatát,
 - e) a szervezeti egységek speciális igényeiket emailben az informatikai osztályvezetőnek megküldve kéri az Informatikai Osztály további hálózati szolgáltatásainak beüzemelését.

Hozzáférés ellenőrzése

- 17. §** (1) Az Egyetem dolgozóinak döntő többsége napi munkája során hálózatba kötött munkaállomáson végzi el a feladatait, ezért a munkaállomásokon központosított felhasználó regisztrálás nem történik. Minden személyes használatban lévő munkaállomáson szabadon választható a regisztráció.
- (2) A központi szolgáltatások esetében a regisztráció kötelező, és a feladatok függvényében a jogosultságok hierarchiája valósul meg. Minden felhasználó csak annyi jogot kap, amennyi a feladata elvégzéséhez szükséges. Különösen védett adatok esetében a személyes regisztráción felül, a titkosított csatorna használatához is szükséges azonosítót alkalmazni.
- (3) A felhasználói jelszavak generálásának, átadásának bizalmasan kell történnie, a kezdeti jelszót a felhasználó szabadon megváltoztathatja, aminek gyakoriságát a rendszer nem szabályozza. A jelszavak kiválasztásánál a következő alapvető szabályokat kell betartani:
- a) tilos könnyen kitalálható jelszavakat választani,
 - b) tilos a LOGIN nevet jelszóként használni,
 - c) tilos a vezetéknevet és a keresztnévet jelszóként használni,
 - d) tilos azonos számokból, vagy betűkből álló jelszót használni,
 - e) tilos a jelszót nyilvános helyen kiírva tartani (például monitorra ragasztva),
 - f) ajánlott a számok, betűk és egyéb karakterek keverése jelszavak használatakor,
 - g) ajánlott a kis és nagybetűk keverése jelszavak használatakor.
- (4) Az Egyetem WiFi (vezeték nélküli) hálózatában a felhasználók két nagyobb csoportra vannak osztva. Az egyik csoportba tartoznak az Egyetem dolgozói, mindazok a felhasználók, akiknek LDAP azonosítójuk van. A másik csoportba tartoznak a hallgatók, akiknek NEPTUN kódjuk van. Különleges alkalmi csoportot alkothatnak a vendégek, akiknek a WiFi hálózat használatához ideiglenes regisztrációt generál az Informatikai Osztály.

NEGYEDIK RÉSZ: Kiemelt informatikai rendszerek használati szabályai

A NEPTUN integrált tanulmányi rendszerrel kapcsolatos szabályok

- 18. §** (1) A NEPTUN célja az Egyetem tanulmányi adminisztrációs rendszer feladatainak teljes körű informatikai megoldása elektronikus csatornákon.
- (2) A NEPTUN rendszerét használó hallgatókra, oktatókra annak felhasználói kézikönyvének utasításai a mérvadóak.
- (3) A NEPTUN üzemeltetését az Informatikai Osztályhoz és az Oktatási Főigazgatósághoz tartozó alkalmazásfelelősök látják el.
- (4) Az Informatikai Osztályhoz tartozó NEPTUN alkalmazásfelelős a szerver-oldali üzemeltetésért felel.
- (5) Az Oktatási Főigazgatósághoz tartozó NEPTUN alkalmazásfelelős a rendszerszintű üzemeltetésért felelős.

A POSZEIDON Integrált iktatási rendszerrel kapcsolatos szabályok

- 19.§ (1) A POSZEIDON célja az Egyetem központi iktatási, nyilvántartó és ügyiratkezelő rendszer feladatainak teljes körű informatikai megoldása mind elektronikus, mind digitális csatornákon.
- (2) A POSZEIDON felhasználói kézikönyvébe foglalt szabályok vonatkoznak az Egyetem valamennyi dolgozójára, akik a POSZEIDON rendszert használják.
- (3) A POSZEIDON rendszer paraméterezett felhasználását az Iratkezelési Szabályzat és Irattári Tervben foglaltaknak megfelelően kell végezni.

ÖTÖDIK RÉSZ: Záró rendelkezések

- 20.§ (1) Az Óbudai Egyetem Informatikai Felhasználói Szabályzat 1. verziószámú változata 2017. november 14. napján lép hatályba.
- (2) A Szabályzat hatályba lépésével egyidejűleg hatályukat veszítik az alábbi szabályzatok:
- az Óbudai Egyetem Informatikai Szabályzata,
 - az Óbudai Egyetem Informatikai Biztonsági Szabályzata.

Az Óbudai Egyetem Informatikai Felhasználói Szabályzatát a Szenátus a 2017. november 13-i ülésén az SZ-CXXXVII számú határozatával fogadta el. Hatályos 2017. november 14. napjától.

Budapest, 2017. november 13.


Dr. Réger Mihály
rektor




Szigeti Ádám
kancellár





