

AZ ÓBUDAI EGYETEM

Informatikai Felhasználói Szabályzata

Budapest, 2022.

(2024. október 15. napjától hatályos 2. verziószámú, a módosításokkal egységes szerkezetbe foglalt változat)

Tartalomjegyzék

PREAMBULUM.....	4
I. Fejezet	5
Általános rendelkezések	5
A Szabályzat hatálya	5
Értelmező rendelkezések	5
II. Fejezet.....	7
AZ ÓE informatikai szervezetei, jogállása és feladata	7
Az Informatikai Iroda	7
Az Informatikai Bizottság	7
III. Fejezet	8
AZ ÓE informatikai szervezetei, jogállása és feladata	8
Az informatikai szolgáltatások célja.....	8
Egyetem polgárainak jogai	8
Egyetemi felhasználói köteleességek	8
Egyetemi felhasználói tilalmak	8
Üzemeltetői jogok.....	9
Üzemeltetői köteleességek	9
Üzemeltetői tilalmak.....	9
Egyetemi felhasználói és üzemeltetői szankciók.....	9
Felhasználók, erőforrások és szolgáltatások névhasználata	10
IV. Fejezet	11
Informatikai biztonsági szabályok	11
Az informatikai biztonsági szabályok célja és feladata.....	11
A számítógép-használat általános alapelvei	11
Vírusvédelem.....	13
Elektronikus levelezés - Elektronikus levelezéssel kapcsolatos biztonsági szabályok	13
Elektronikus levelezés - Kéretlen levelek, reklámok szűrése (spam)	15
Felhőszolgáltatás	15
Weblap és portál szolgáltatások	15
Az internethasználattal kapcsolatos biztonsági szabályok (ÓENET).....	16
Hálózathasználattal kapcsolatos biztonsági szabályok.....	17
Hozzáférés ellenőrzése	18
V. Fejezet	19
Kiemelt informatikai szakrendszerek használati szabályai rendszerek.....	19

A NEPTUN Integrált Tanulmányi Rendszerrel kapcsolatos szabályok.....	19
A POSZEIDON Irat- és Dokumentumkezelő	19
Gazdasági szakrendszerek (SAP, KIRA, EOS).....	19
VI. Fejezet	20
Hatályba léptető és záró rendelkezések.....	20
Mellékletek.....	21
1. számú melléklet Óbudai Egyetem központi e-mail cím igénylése	21
2. számú melléklet Poszeidon jogosultság igénylőnyilatkozat	22
3. számú melléklet VPN igénylő nyilatkozat	24

PREAMBULUM

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

Az Informatikai Szabályzat (a továbbiakban: Szabályzat) az Egyetem informatikai rendszerének rendeltetésszerű használatához kiadott szabályok gyűjteménye, amelyben foglaltak betartása az Egyetem összes hallgatójára és munkavállalójára 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.

I. Fejezet

Általános rendelkezések

A Szabályzat hatálya

- 1. §** (1) A Szabályzat személyi hatálya kiterjed:
- az Egyetem valamennyi hallgatójára és munkavállalójára,
 - 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,
 - 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 életciklusa alatt.

Értelmező rendelkezések

2. § E szabályzat értelmében

- Informatikai infrastruktúra: az egyetemhez kapcsolódó feladatokat ellátó, illetve az egyetemi hálózatba kapcsolt hardverelemek, az azokon futó szoftverek és a rajtuk megtalálható adatok együttese.
- Aktív hálózati eszköz: kapcsolók (switch-ek), forgalomirányítók (router-ek), vezeték nélküli hozzáférési pontok és egyéb eszközök, amelyek segítségével a hálózat üzemvitele biztosítható.
- Alkalmazásfelelős: meghatározott rendszer üzemeltetéséért felelős felhasználó, aki kizárólag az adott rendszerre vonatkozóan rendelkezik többlet-, vagy egyedi jogosultsággal (például a NEPTUN vagy a POSZEIDON alkalmazásfelelősei).
- Biztonsági incidens: biztonsági problémát okozó jelenség.
- DNS (Domain Name Server): az IP címeket és a számítógépneveket egymáshoz rendelő adatbázis, mely általában külön kiszolgáló gépen fut.
- Domainnév (tartománynév) az Internet egy meghatározott részét, tartományát egyedileg leíró megnevezés. A domainnevek kiosztása és értelmezése a Domain Name System (DNS) szabályai szerint, hierarchikusan történik.
- Felhasználó: az a természetes személy, aki az informatikai infrastruktúrát használja.
- Felhasználói azonosító: az intézményi címtárban tárolt egyedi azonosításra szolgáló rövid karaktorsorozat, amely általában a felhasználó nevéből képződik.
- Hálózat: felhasználói számítógépek és/vagy szerverek közötti adatátvitelt biztosító közeg.
- Központi szolgáltatások: levelezés, címtár, fájl kiszolgálás, web szolgáltatás, névszolgáltatás.
- Szerver feladatokat ellátó eszköz: olyan számítógépek, szoftverek, vagy speciális eszközök, amelyek különböző szolgáltatásokat biztosítanak más számítógépek számára.
- Alkalmazásfelelős: meghatározott rendszer üzemeltetéséért felelős felhasználó, aki

kizárólag az adott rendszerre vonatkozóan rendelkezik többlet-, vagy egyedi jogosultsággal (például a NEPTUN vagy a POSZEIDON alkalmazásfelelősei).

13. Üzemeltető: az Egyetem informatikai üzemeltetéséért felelős személy, aki lehet az Informatikai Iroda, valamint speciális informatikai terek, laboratóriumok és műhelyek vonatkozásában az adott kar alkalmazottja is.
14. Informatikus: egy az Egyetem informatikai rendszerének végberendezései üzemeltetéséért, valamint ügyfélszolgálat fenntartásért felelős informatikus.
15. VLAN: a hálózat egy meghatározott része a feladatoknak megfelelően, logikai csoportba van szervezve.
16. VPN (Virtual Private Network) szolgáltatás: speciális hálózati elérés, amely az Egyetem hálózatához titkosított, és hitelesített kapcsolatot tesz lehetővé a világ bármely részéről.
17. WiFi (Wireless Fidelity): szabványos vezeték nélküli adatátviteli technika. Legtöbb notebook, laptop számítógép, okostelefon gyárilag rendelkezik ilyen kapcsolódási lehetőséggel. Csak olyan vezeték nélküli eszköz telepíthető, amely képes központi adatbázisból azonosítani (Radius autentikáció) és logikai csoportokba rendezni (VLAN) a felhasználókat.
18. UPN (User Principal Name): a központi szolgáltatásokhoz használt felhasználónév. Alapértelmezetten a felhasználó nevéből van létrehozva a következő formában: *vezeteknev.keresztnev@uni-obuda.hu* A felhasználónév nem tartalmazza a szervezeti egységhez tartozó aldomaint.
19. Vírusfertőzés: Informatikai infrastruktúra biztonsági kockázata.

II. Fejezet

AZ ÓE informatikai szervezetei, jogállása és feladata

Az Informatikai Iroda

3. § Az Egyetem Szervezeti és Működési Rendjében foglaltak alapján

Az Informatikai Bizottság

4. § (1) Az Informatikai Bizottság az Egyetem informatikai tevékenységeit, fejlesztéseit összehangoló, az informatikai döntés-előkészítő, konzultatív, javaslattevő, illetve tanácsadó testülete.

(2) Az Informatikai Bizottságnak tizenhat tagja van:

a) hivatalból:

- a. a rektori hivatalvezető,
- b. az informatikai irodavezető,
- c. az Elektronikus és Digitális Tananyagok Iroda irodavezetője,

b) delegálás útján:

- a. az Oktatási Főigazgatóság képviselője,
- b. a tudományos rektorhelyettes képviselője,
- c. a karok és az EKIK által delegált képviselők (8 fő),
- d. a kollégiumigazgató,
- e. az EHÖK képviselője.

(3) Az Informatikai Bizottság elnöke az informatikáért és minőségbiztosításért felelős rektorhelyettes.

(4) Az Informatikai Bizottság feladat- és hatáskörei különösen:

- a) meghatározza a teljes IT infrastruktúra közép és hosszú távú fejlesztésének irányvonalait,
- b) javaslatokat dolgoz ki az Egyetem egészét, illetve az egyes szervezeti egységeket érintő informatikai fejlesztésekre, biztosítja a karok és egyéb szervezeti egységek informatikai rendszereinek összehangolását és egységesítését,
- c) véleményezi az Egyetem Informatikai Felhasználói Szabályzatának, illetve az Informatikai üzemeltetési szabályzatának módosítására irányuló javaslatokat,
- d) véleményezi az Egyetem valamennyi informatikai tevékenységét, fejlesztését, informatikai területet érintő döntését, azok technikai jellegű kérdéseinek vonatkozásában javaslatot tesz, közreműködik a döntések előkészítésében, koordinálja és ellenőrzi azok végrehajtását,
- e) az Informatikai Iroda a végrehajtott fejlesztésekről félévente beszámolót terjeszt a bizottság elé.

III. Fejezet

AZ ÓE informatikai szervezetei, jogállása és feladata

Az informatikai szolgáltatások célja

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

Egyetem polgárainak jogai

- 5. §** (1) Az Egyetem minden polgára alanyi jogon igénybe veheti az Egyetem alapvető informatikai szolgáltatásait. Alapvető informatikai szolgáltatások alatt az alábbiak értendők:
- a) az ÓE informatikai infrastruktúrájának szabályozott használatához,
 - b) szabad internet elérés egyetemi és saját tulajdonú számítástechnikai eszköz felhasználásával (vezetékes és vezeték nélküli közegen keresztül),
 - c) a központilag szabályozott felhőalapú szolgáltatások használata,
- (2) Az Egyetem minden munkavállalója, illetve a megbízási jogviszony alapján tartós munkavégzést végző 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) VPN szolgáltatás.
- (3) Panaszt tenni az üzemeltető személyzet, illetve azok intézkedései ellen az alkalmazásfelelősnél vagy annak felügyelő szervénél.

Egyetemi felhasználói köteleességek

- 6. §** Valamennyi egyetemi felhasználó köteles:
- a) jelen szabályzat előírásait betartani,
 - b) rendeltetésszerűen használni az Egyetem informatika infrastruktúráját,
 - c) az egyetem polgárától elvárható etikai normákat betartani,
 - d) titokban tartani az ÓE informatikai infrastruktúrájának igénybevételéhez biztosított azonosítókat,
 - e) tájékoztatni az illetékes üzemeltetőket a működési hibákról, a nem rendeltetésszerű vagy törvénytelen használatról,
 - f) együttműködni és segíteni az üzemeltetőt, alkalmazásfelelőst, vagy nyomozó hatóságot a működési hibák, nem rendeltetésszerű vagy törvénytelen használat felderítésére indult vizsgálatban,
 - g) az Internet etikus használatára vonatkozó szabályokat megtartani.

Egyetemi felhasználói tilalmak

- 7. §** (1) Valamennyi egyetemi felhasználó számára tilos:
- a) olyan jogosultságok megszerzése, illetve megszerzésére való kísérlet, amely a felhasználó számára nem engedélyezett,
 - b) a biztonsági rendszerek feltörése, illetve feltörésükre tett kísérlet,

- c) másoknak jogosultságok átadása,
 - d) személyes jövedelemszerzés, illetve profitorientált tevékenység folytatása az Egyetem informatikai infrastruktúráján,
 - e) szoftver, hardver elemek megrongálása, működésük veszélyeztetése,
 - f) szoftver, hardver elemek jogosulatlan módosítása, átkonfigurálása,
 - g) meghibásodás esetén a hiba elhárítását jogosulatlanul megkezdeni,
 - h) hálózati forgalom figyelése, adatgyűjtése,
 - i) aktív hálózati eszközöket vagy szerver feladatokat ellátó eszközöket engedély nélkül a hálózatra kapcsolni.
- (2) Amennyiben a szolgáltatás igénybevevője az 7. §-ban vagy a 8.§ (1) pontjában foglaltak ellen vét, úgy a szolgáltatásból ideiglenesen vagy véglegesen kizárható.

Üzemeltetői jogok

- 8. §** Valamennyi üzemeltetőnek joga van:
- a) 6.§-ban foglalt jogosultságokhoz,
 - b) indokolt esetben, az adott alkalmazásfelelőssel egyetértésben, azonnali hatállyal korlátozni vagy felfüggeszteni a felhasználó(k) vagy felhasználói csoport(ok) jogosultságait, hálózati eszközök, szegmensek, szolgáltatások elérését, működését,
 - c) az informatikai infrastruktúra adott elemének üzemeltetője bármikor jogosult annak szabályos használatát, működését ellenőrizni, és
 - d) a hálózati forgalom monitorozásához, és statisztikai adatgyűjtéshez.

Üzemeltetői köteleességek

- 9. §** Valamennyi üzemeltetőnek kötelessége:
- a) a 7.§-ban foglaltakat betartani,
 - b) a károkat megelőzni, illetve a bekövetkezett károk következményeit mérsékelni, felszámolni,
 - c) titokban tartani a nagyobb jogosultsági köréből eredően birtokába jutott személyes vagy bizalmas információkat,
 - d) az általa működtetett informatikai rendszerről naprakész dokumentációt vezetni és
 - e) egyeztetni nem technikai kérdésekben az általa működtetett informatikai rendszer alkalmazásfelelősével, viszonyuk részleteit az üzemeltető munkaköri leírása tartalmazza.

Üzemeltetői tilalmak

- 10. §** Valamennyi üzemeltetőnek tilos:
- a) a 8. §-ban foglaltak, kivéve, ha a 9. § vagy a 10. § másképp nem rendelkeznek,
 - b) a nagyobb jogosultsági körével való visszaélés, azt a számára kijelölt feladatkörön kívül felhasználni,
 - c) továbbadni a nagyobb jogosultsági köréből eredően birtokába jutott személyes vagy bizalmas információkat és
 - d) a nagyobb jogosultsági köréből eredően az Egyetem informatikai infrastruktúrájáról megszerzett információkat arra illetéktelen személyekkel megosztani.

Egyetemi felhasználói és üzemeltetői szankciók

- 11. §** Valamennyi egyetemi felhasználóra és üzemeltetőre vonatkozó szankciók:
- a) a nem rendeltetésszerű vagy törvénytelen használatból eredő károkért büntetőjogi és polgári jogi kártérítési felelősséggel tartozik,

- b) a szabályok be nem tartása esetén az adott informatikai infrastruktúra üzemeltetője, alkalmazásfelelőse a felhasználó hozzáférési jogát korlátozhatja, vagy teljes mértékben ideiglenesen vagy véglegesen felfüggesztheti és
- c) bűncselekmény elkövetésének alapos gyanúja esetén azonnali hatállyal minden hozzáférési jogot megvon az üzemeltető, értesíti a hatóságokat és az alkalmazásfelelőst, aki kezdeményezheti a hallgatói vagy munkavállalói fegyelmi eljárását.
- d) a szabályok ismeretének hiánya nem mentesít a szankciók, illetve a büntetőjogi és polgári jogi kártérítési felelősség alól.

Felhasználók, erőforrások és szolgáltatások névhasználata

- 12. § (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 Iroda tartja nyilván.
 - (4) A központi informatikai szolgáltatások összehangolt működése lehetővé teszi, hogy egy felhasználó minden központi szolgáltatást ugyanazzal az azonosítóval és jelszóval vehessen igénybe. A központi címtárat a Microsoft Active Directory, és az arra épülő Exchange rendszer biztosítja a UPN felhasználónév segítségével.
 - (5) A felhasználói név és elektronikus levelezés névhasználati szabályai:
 - a) a felhasználói nevet a következő formában kell létrehozni,

vezeteknev.keresztnev@uni-obuda.hu
 - b) az elektronikus levelezéshez minden felhasználó jogosult a szervezeti egységének megfelelő alapértelmezett levelezési alias használni.

vezeteknev.keresztnev@<szervezeti egység neve>.uni-obuda.hu
 - c) Az Egyetem vezetőségének (rektor, rektorhelyettesek, gazdasági főigazgató, főigazgatók, dékánok, dékánhelyettesek, rektori hivatalvezető, rektori kabinetvezetők, irodavezetők) részére biztosított a levelezési alias a következő formában is:

vezeteknev@uni-obuda.hu
 - d) a szervezeti egységek saját információáramlásuk meggyorsítására úgynevezett terjesztési és/vagy levelezési listákat igényelhetnek. Az igényelni a <https://support.uni-obuda.hu> oldalon vagy support@uni-obuda.hu címre küldött levélben lehet, az igénylést az Informatikai Iroda irodavezetőjének szükséges jóváhagynia. A levelezési listát az igénylő szervezeti egységnek kell adminisztrálnia egy felelős személy kijelölésével. Terjesztési listában történő változásokat a <https://support.uni-obuda.hu> oldalon vagy support@uni-obuda.hu címen kell jelezni.

(6) A DNS nevek névhasználati szabályai:

- a) a nemzetközi regisztrált névhasználati rendszerben minden domain név az egyetem tulajdonát képezi,
- b) a DNS nevet a következő formában kell megalkotni:

<szolgáltatás>.<szervezeti egység rovidítve>.uni-obuda.hu,
például: szervezeti egység.uni-obuda.hu,

- c) a szervezeti egység saját hatáskörébe tartozó szervert az alábbiak szerint kell azonosítani:

<szervernev>.<szervezeti egység rovidítve>.uni-obuda.hu,

például: labor.szervezeti egység.uni-obuda.hu,

- d) a fentiekől eltérő DNS nevek a rektor hozzájárulásával alkalmazhatók.

IV. Fejezet

Informatikai biztonsági szabályok

Az informatikai biztonsági szabályok célja és feladata

- 13. §** (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

- 14. §** (1) Az Egyetemen működő számítógépek csak rendeltetésszerűen, kizárólag 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 jelszavakkölcsonadásával vagy nem biztonságos kezelésével, a hozzáférési jogosultságok nem megfelelő kezelésével, a számára biztosított – az Egyetem tulajdonát képező – informatikai, kommunikációs eszközökben) okozott szabályellenes, jogellenes 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) a biztonsági esemény bekövetkezésének okát,
 - b) az esetleges személyi felelősséget és
 - c) az okozott kár mértékét.
- (4) A vizsgálat eredményeképpen az alábbi szankciók kiszabására kerülhet sor:
- a) a szabályzat gondatlan megszegése esetén az elkövetőt figyelmeztetésben kell részesíteni,

- b) a szabályzat szándékos megsértése esetén az elkövető a hálózat használatából ideiglenesen vagy véglegesen kizárható,
 - c) a szándékos elkövető – amennyiben a fentiekén túl kimutatható anyagi kár is keletkezett – köteles megtéríteni az általa okozott károkat a vonatkozó jogszabályok előírásai szerint,
 - d) bűncselekmény elkövetésének gyanúja esetén a munkáltatói jogkör gyakorlója vagy az utasítási jog gyakorlója (megbízási jogviszony esetén) kezdeményezi az elkövető felelősségre 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 Iroda 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) Az Egyetemen működő számítógépekre csak támogatott, biztonsági frissítésekkel rendelkező szoftverek, operációs rendszer telepíthető.
- (9) A felhasználóknak a munkahelyükön használata során a következő általános szabályokat kell betartaniuk:
- a) személyes használatban lévő számítógépen felhasználói jogokkal ajánlott rendelkeznie,
 - b) jelszóval védenie kell a számítógépe integritását,
 - c) illetéktelen személynek felhasználói jogát át nem adhatja,
 - d) közepes vagy magas biztonsági kockázattal járó feladatvégzésekor a számítógépét 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.
- (10) 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.
- (11) Nem személyhez kötött használatú eszközök esetében a fenti feladatokat az Informatikai Iroda végzi.
- (12) Amennyiben a személyes használatú eszköz biztonságáról a felhasználó nem maga kíván gondoskodni, köteles ezt a feladatot az operátorra bízni.

Vírusvédelem

- 15. §** (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
- (3) Az Informatikai Iroda minden évben biztosítja informatikai eszközei számára a legfrissebb vírusvédelmi szoftver jogtisztá használatát, illetve emailben küldött tájékoztatásokkal fejleszti a felhasználók biztonsági ismereteit. A munkahelyi munkaállomáson az Informatikai Iroda 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 Irodát a support@uni-obuda.hu email címen értesíteni kell abban az esetben is, ha a vírus terjedését sikerült helyben megakadályozni.

Elektronikus levelezés - Elektronikus levelezéssel kapcsolatos biztonsági szabályok

- 16. §** (1) Az Egyetem valamennyi munkatársa, illetve a megbízási jogviszony alapján tartós munkavégzést végzők jogosultak felhasználói jogosultságot igényelni az elektronikus levelezéshez, vagyis a munkavállaló 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 irodavezető engedélyével állítható be,
- d) az elektronikus levélhez fájl csatolható, amelynek mérete korlátozott (teljes üzenet felső méret korlát: 25MB, számítógépre telepített kliensnél 100 MB),

- 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 munkavállaló postafiókja a munkaviszonyának megszűnésével törlendő, kivételt képez ez alól a felsőbb vezetői engedéllyel (rektor, gazdasági főigazgató, dékánok, főigazgatók) a postafiók határozott időre történtő megtartása.
 - k) a felhasználó beállíthatja az automatikus válaszüzeneteket a munkavégzésére irányulóan (távollét, szabadság, akadályoztatás, helyettesítés jelzése),
 - l) mindenki@uni-obuda.hu dinamikus terjesztési listán kizárólag az Egyetemmel munkavállalói jogviszonyban álló személyek szerepelhetnek, a terjesztési listára küldési joggal kizárólag a rektor – illetve az általa megbízott közvetlen munkatárs – rendelkezik.
 - m) tilos a levelezést külső domainre átirányítani, illetve bármilyen külső szolgáltató rendszeréről egyetemi domainnel levelet küldeni,
 - n) tilos a levelezéshez használt felhasználói adatokat külső szolgáltatásoknak átadni,
 - o) tilos rasszista, szemérmes és jó ízlést sértő, esetlegesen bűncselekményt megvalósító, annak gyanúját keltő, valamint politikai nézeteket képviselő tartalmú levelet küldeni.
- (3) A munkavállalók, illetve a megbízási jogviszony alapján tartós munkavégzést végzők tudomásul veszik, 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 munkavállaló, illetve a megbízási jogviszony alapján tartós munkavégzést végző az Egyetem más munkavállalójának, illetve a megbízási jogviszony alapján tartós munkavégzést végzőnek küld.
- (4) A munkáltatói jogkör gyakorlója a szabályzat rendelkezései megszegésének gyanúja esetén a munkavállaló, illetve a megbízási jogviszony alapján tartós munkavégzést végző 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 munkavállalótól 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.

Elektronikus levelezés - Kéretlen levelek, reklámok szűrése (spam)

17. § (1) A kéretlen levelek központi szűréséről az Informatikai Iroda üzemeltetésében álló szerverek gondoskodnak. A levelek kéretlenségének 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. A levél egy hónap múlva törlődik,
- d) gyanús vagy futtatható csatolt fájlokat (pl.: exe, bat stb.) tartalmazó leveleket blokkoljuk, ezekről értesítést kap a feladó.

Felhőszolgáltatás

18. § (1) Az Egyetem által biztosított felhőszolgáltatás használatára az Egyetem összes polgára jogosult.

- (2) Egyetemi felhőszolgáltatáshoz a Microsoft 365 szolgáltatások tartoznak.
- (3) Az felhőszolgáltatás infrastruktúráját és a szolgáltatások folytonosságát a Microsoft biztosítja. A rendszerüzemeltetést, valamint a felhasználói támogatást az Informatikai Iroda munkatársai végzik.
- (4) Az ügyfeladatokat a Microsoft csak a szolgáltatás biztosítására használja, kivéve ha a felhasználó másként rendelkezik.
- (5) Az Egyetem által használt felhőszolgáltatási fióknév a felhasználó nevéből tevődik össze, megegyezik a levelezéshez használt felhasználói névvel (vezeteknev.keresztnev@uni-obuda.hu).

Weblap és portál szolgáltatások

19. § (1) Valamennyi szervezeti egység jogosult a feladatainak ellátásával összefüggésben weblap létrehozására.

- (2) A honlap szolgáltatásáért felelős webszervernek a jelen szabályzatban előírt szabályoknak meg kell felelnie.
- (3) A műszaki lehetőségekhez mérten az Informatikai Bizottság engedélye alapján az Informatikai Iroda lehetőséget biztosít az egyetem tevékenységéhez kapcsolódó honlapok elhelyezésére saját webszerverein.
- (4) A honlap tartalmáért minden esetben a honlapot karbantartó tartalomgazda a felelős. Jogszabályba ütköző, a jó erkölcsöt súlyosan sértő, az Egyetem vagy bármely szervezeti egységének érdekeit veszélyeztető, üzleti célú tartalmat nem szolgáltatathat, nem jeleníthető meg a honlapon. A tartalomszolgáltatásért a szervezeti egység vezetője a felelős.
- (5) Az Egyetem központi honlapjának címe, az egyetemi fő domain címe: „<https://uni-obuda.hu>”. A honlapot az Informatikai Iroda üzemelteti.
- (6) Nem képezi az egyetemi webmester feladatát az aldomainek kezelése, kivéve a központi domain, illetve az intranet szolgáltatás. Amennyiben valamely egyetemi szintű szervezeti egység önálló hozzáférési jogosultsággal rendelkező aloldalt hoz létre, az önálló

hozzáférési jogosultsággal rendelkező aldomain vonatkozásában a szervezeti egység látja el aldomainnel kapcsolatos karbantartási, fejlesztési feladatköröket.

- (7) A tartalomszolgáltatók és a szerkesztők feladatukat a szervezeti egységvezető irányításával végzik. A végrehajtásért a szervezeti egység vezetője a felelős.
- (8) A tartalomszolgáltató javaslatot tehet a szerkesztőnek az általa szolgáltatott anyag szerkesztésére, annak a honlap hierarchiájában meghatározott helyen való elhelyezésére. A szolgáltatott anyag kiemelt hírek közti szereplésére javaslatot tehet, de csak a rektor határozhatja meg, mi számít kiemelt hírnek.
- (9) A tartalomgazda felel azért, hogy az általa biztosított anyagok megfelelnek a valóságnak, időszerűek és nem jogszabálysértők. A szerkesztő a tartalomszolgáltatók által nyújtott tartalomért nem felel. Az elavult tartalommal rendelkező weblapokat az Informatikai Iroda azonnali hatállyal leállíthatja.
- (10) A weblap karbantartójának a felelőssége, hogy az általa kezelt weblaphoz tartozó tartalomkezelő rendszernek és a hozzá tartozó beépülő moduloknak naprakésznek kell lenni. Az elavult rendszerrel rendelkező weblapokat az Informatikai Iroda azonnali hatállyal leállíthatja.
- (11) A központi weblappal kapcsolatos módosítási kérelmeket az Intraneten (Intranet>Nyomtatványok>Iratminták>Informatika vagy <https://intranet.uni-obuda.hu/nyit/io/jogosultsag-keres-sablon>) elérhető online kérelemmel lehet kezdeményezni. A módosítási kérelmeket az Informatikai Bizottság jóváhagyása után a tartalom szerkesztő fogják végrehajtani.

Az internethasználattal kapcsolatos biztonsági szabályok (ÓENET)

- 20. §** (1) Az Egyetem belső hálózatában működő munkaállomások alaphelyzetben tűzfalal védett internet-eléréssel rendelkeznek. Kivétel alá esnek, és így az internetet csak korlátozott módon 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) A védett hálózatok eléréséhez VPN jogosultság szükséges. A VPN jogosultság igénylése, illetve visszavonása a 3. számú mellékletben található űrlap értelemszerű kitöltésével lehetséges, amelyet <https://support.uni-obuda.hu> oldalon vagy support@uni-obuda.hu címre küldött levélben szükséges beküldeni.
 - (4) Az internet használata során az Egyetem fenntartja a jogot arra, hogy a felhasználók internet-forgalmát figyelemmel kísérje és naplózza.
 - (5) 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.
 - (6) Az internetről letöltött szoftver vagy fájl jogtisztaságáért az Egyetem, mint jogi személy felel, ezért fenntartja a jogot, hogy a szabályok megsértőivel szemben szankciókat alkalmazzon. Illegális tevékenység céljára használt internet elérés felelősségre vonási

eljárást eredményezhet.

- (7) Az Internet használata során elvárt magatartás:
- a felhasználó nem titkolja el személyazonosságát az internet használat közben,
 - az Egyetem összes felhasználója véleménynyilvánításhoz való jogukat az Egyetem jó hírnevét, jogos gazdasági és szervezeti érdekeit súlyosan sértő vagy veszélyeztető módon nem gyakorolhatják,
 - a szellemi tulajdon védelme az internetre is kiterjed,
 - 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

- 21. §** (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 Iroda jogosult.
- (2) A VLAN-ok biztonsági feladatot látnak el, mert elválasztják egymástól az alhálózatokat, ezzel biztosítva, hogy sérülés, vagy támadás esetén csak az adott részterületre korlátozódjék az esetleges kár. A VLAN-ok kialakítása az Informatikai Iroda hatásköre.
- (3) Az Egyetem hálózata nem használható az alábbi tevékenységekre:
- 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),
 - profitszerzést célzó, direkt üzleti célú tevékenység és reklám,
 - a hálózat, a kapcsolódó hálózatok, illetve ezek erőforrásainak rendeltetésszerű működését és biztonságát megzavaró, veszélyeztető tevékenység, ilyen információknak és programoknak a terjesztése,
 - a hálózatot, a kapcsolódó hálózatokat, illetve erőforrásaikat indokolatlanul, túlzott mértékben, pazarló módon igénybe vevő tevékenység (pl. körlevelek, hálózati játékok, kéretlen reklámok, fájlcsere használata),
 - a hálózat erőforrásaihoz, a hálózaton elérhető adatokhoz történő illetéktelen hozzáférés, azok illetéktelen használata, gépek/szolgáltatások – akár tesztelés céljából történő – túlzott mértékben való szisztematikus próbálgatása,
 - a hálózat erőforrásainak, a hálózaton elérhető adatoknak illetéktelen módosítására, megrongálására, megsemmisítésére vagy bármely károkozásra irányuló tevékenység,
 - másokra nézve sértő, vallási, etnikai, politikai vagy más jellegű érzékenységet bántó, zaklató tevékenység (pl. pornográf/pedofil anyagok tárolása, közzététele),
 - 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 felhasználók kötelessége a Szabályzat megismerése és az abban foglaltak betartása, valamint együttműködni a hálózat üzemeltetőivel a szabályzat betartatása érdekében,
 - a felhasználó viseli a felelősséget minden műveletért, amely az adott felhasználóhoz tartozó azonosítóval kerül végrehajtásra,
 - a felhasználó kötelessége és felelőssége, hogy a munkahelyén jogtiszt szoftvereket használjon.
- (5) A felhasználók jogai a hálózat használata során:
- 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,
- d) a szervezeti egységek speciális igényeiket emailben az informatikai irodavezetőnek megküldve kéri az Informatikai Iroda további hálózati szolgáltatásainak beüzemelését.

Hozzáférés ellenőrzése

- 22. §** (1) Az Egyetem munkavállalóinak döntő többsége napi munkája során hálózatba kötött munkaállomáson végzi el a feladatait, a munkaállomásokon központosított felhasználó regisztrálás nem történik.
- (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) hálózatához a felhasználók az központi felhasználói nevükkel (vezeteknev.keresztnev@uni-obuda.hu) vagy a Neptunkódjukkal és hozzá tartozó jelszavukkal tudnak csatlakozni.
 - (5) Különleges alkalmi csoportot alkothatnak a vendégek, akiknek a WiFi hálózat használatához ideiglenes regisztrációt generál az Informatikai Iroda.

V. Fejezet

Kiemelt informatikai szakrendszerek használati szabályai rendszerek

A NEPTUN Integrált Tanulmányi Rendszerrel kapcsolatos szabályok

23. § (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 Irodához és az Oktatási Főigazgatósághoz tartozó alkalmazásfelelősök látják el.
- (4) Az Informatikai Irodához tartozó NEPTUN alkalmazásfelelős a szerver-oldali üzemeltetésért felel.
- (5) Az Oktatási Főigazgatósághoz tartozó NEPTUN alkalmazásfelelős a rendszerszintű üzemeltetésért felelős.

A POSZEIDON Irat- és Dokumentumkezelő

24. § (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.
- (4) A POSZEIDON rendszerhez jogosultság az arra kijelölt munkatárs számára adható, meghatározott jogosultsági körben, a szervezeti egység vezetője által meghatározott jogosultsági körben, illetve a szervezeti egység vezetője által meghatározott időtartamra. A jogosultság igénylése, illetve visszavonása a 2. számú mellékletben található űrlap értelemszerű kitöltésével lehetséges.

Gazdasági szakrendszerek (SAP, KIRA, EOS)

25. § (1) A gazdasági rendszerek céljai az Egyetem gazdasági folyamatainak támogatása, adminisztrálása.
- (2) A szakrendszereket használó munkavállalókra annak felhasználói kézikönyvének utasításai a mérvadóak.
- (3) A szakrendszerhez jogosultság az arra kijelölt munkatárs számára adható, meghatározott jogosultsági körben, meghatározott időtartamra. A jogosultságok kezelését a Gazdasági Főigazgatóság adminisztrálja.

VI. Fejezet

Hatályba léptető és záró rendelkezések

Az Óbudai Egyetem Informatikai Felhasználói Szabályzatának módosítását a Szenátus 2024. szeptember 30. napján megtartott ülésén az SZ-2024/2025 (IX.30.) 5. számú határozatával fogadta el. Hatályba lép 2024. október 15. napján.

Budapest, 2024. október 15.



Prof. Dr. Kovács Levente
rektor

Melléletek

1. számú melléklet Óbudai Egyetem központi e-mail cím igénylése

Óbudai Egyetem központi e-mail cím igénylése

Az igénylő adatai:

*Név: ¹

Leánykori név:

*Szervezeti egység²:

*Tanszék, osztály, iroda³:

*Használni kívánt e-mail cím⁴:

*Telefon⁵:

/

*Tartózkodási helye, iroda⁶:

Értesítési cím, ahova a jelszó elküldését kérem⁷:

*Beosztás⁸:

A szolgáltatással és az Óbudai Egyetem címtárában tárolt adatokkal kapcsolatosan az Egyetem adatvédelmi és informatikai szabályzatát (<https://uni-obuda.hu/szabalyzatok/>) megismertem, és a bennük foglaltakat elfogadom.

Hozzájárulok, hogy a *-gal jelölt adatokat az Egyetem a weblapján nyilvánosságra hozza.

Budapest , 2024. október 28.

Város

Dátum

igénylő aláírása

Szervezeti egység vezetőjének
aláírása

¹ Az Ön teljes neve, például: Kissné Nagy Valéria

² Például: Neumann János Informatikai Kar

³ Például: Szoftvertológia Intézet

⁴ Az e-mail címnek két tagúnak kell lennie. Ha Önnek kettőnél több tagú neve van, és még nincs ilyen címe, akkor választania kell, hogy melyik kettőt kívánja használni.

Példa: kissne.valeria@nik.uni-obuda.hu, vagy nagy.valeria@nik.uni-obuda.hu

⁵ Telefon és faxszám, / jellel elválasztva. Ha csak az egyik van, a másikat hagyja üresen.

⁶ Az Ön irodája. Csak az utca, ház, épület és szobaszám (emelettel) kell. Példa: **Nagyszombat utca 19. A/113.**

⁷ Az a cím, ahová az azonosító elkészültéről küldünk igazolást házipostán (esetleg már meglévő e-mail cím).

⁸ Például: adjunktus, tanársegéd, műszaki ügyintéző, stb.



2. számú melléklet Poszeidon jogosultság igénylőnyilatkozat

POSZEIDON JOGOSULTSÁG IGÉNYLŐ NYILATKOZAT

Kérem az alábbi adatok alapján a nyilatkozatban szereplő jogosultság(ok) beállítását.

***-gal jelölt mezők kitöltése kötelező!**

Név:*									
Neptun kód:*(Amennyiben rendelkezik Neptun kóddal kitöltése kötelező.)	<table border="1"><tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr></table>								
Email cím:*									
Telefonszám:*									
Telephely, szoba:*									
Szervezeti egység/Szervezeti egység kódja:*									
Szervezeti egység vezetője:									
Munkakör:*									
Igényelt jogosultság(ok):*	<input type="radio"/> Iktató jogosultság regisztrálása <input type="radio"/> <input type="checkbox"/> Vezető jogosultság regisztrálása <input type="radio"/> jogosultság regisztrálása								
Jogosultság érvényessége:*	____.____.____-tól ____.____.____-ig								
Indokolás:									
Helyettesítésre jogosult személy:*									

Dátum:

.....

szervezeti egység vezetője

.....

igénylő aláírása

A jogosultságok beállítását engedélyezem:

Dátum:

.....

rektori hivatalvezető

A jogosultságok beállítását elvégeztem:

Dátum:

.....

rendszergazda



3. számú melléklet VPN igénylő nyilatkozat

VPN HOZZÁFÉRÉS IGÉNYLŐ NYILATKOZAT

Kérem az alábbi adatok alapján a nyilatkozatban szereplő hozzáférés beállítását.

Nyomtatott betűkkel töltendő ki!

***-gal jelölt mezők kitöltése kötelező!**

Név:*	
Email cím:*	
Telefonszám:*	
Szervezeti egység neve/Szervezeti egység kódja:*	
Szervezeti egység vezetője*:	
Igényelt jogosultság(ok):*	<input type="radio"/> gazdasági VPN** <input type="radio"/> általános VPN***
Indokolás, elérni kívánt szolgáltatások:	

Kelt:

.....

szervezeti egység vezetője*

.....

igénylő aláírása*

.....

Gazdasági Főigazgató
(csak a gazdasági VPN esetén)

ki!!

rendszergazda/operátor tölti

Igénylő UPN-je *:

A jogosultságok beállítását elvégeztem:

Dátum:

.....

rendszergazda/operátor

* Kitöltése kötelező!

** gazdasági VPN: a gazdasági szakrendszerek külső elérését szolgálja a Gazdasági Főigazgatóság munkavállalói részére

*** általános VPN: kutatási adatbázisok, óbudai fájlmegosztások külső elérését szolgálja