

**TESTNEVELÉSI EGYETEM**

# Informatikai Biztonsági Szabályzat

---

A Szenátus elfogadta a 74/2017. (X. 19.) számú határozatával.

A 2019. május 30-án elfogadott módosításokkal egységes szerkezetben

Módosító határozatok:

35/2019. (V. 30.) számú szenátusi határozat

## Tartalom

I.	FEJEZET ÁLTALÁNOS RENDELKEZÉSEK.....	3
	Preambulum .....	3
	1. § Az IBSZ célja.....	3
	2. § Az IBSZ hatálya .....	4
	3. § Értelmező rendelkezések .....	4
II.	FEJEZET A HÁLÓZAT HASZNÁLATA.....	8
	4. § A Hálózat használatának alapvető szabályai.....	8
	5. § Központi szolgáltatások az informatikai hálózaton .....	9
	6. § Az InI kötelezettségei .....	10
	7. § Az InI jogai .....	11
	8. § A felhasználók jogai .....	12
	9. § A felhasználók köteleességei .....	12
	10. § A meg nem engedett tevékenységek szankciói .....	14
	11. § A hálózat felépítése .....	14
	12. § A Hálózat üzemeltetése, építése, bővítése .....	15
	13. § Az egyetemi informatikai és kommunikációs Hálózat használatának szabályai ..	15
	14. § A hálózati hibák elhárítása.....	16
III.	FEJEZET AZ INFORMATIKAI HÁLÓZAT SZOFTVER ÜZEMELTETÉSE.....	17
	15. § Támogatott protokollok.....	17
	16. § Kritikus adatokat tartalmazó számítógépek használata .....	17
	17. § Személyi számítógépek felkészítése a használatra.....	17
	18. § Szerverek üzemeltetése .....	18
	19. § Távoli munkavégzés .....	18
	20. § Adatok elhelyezésének szabályai a Hálózaton .....	19
	21. § Adatok, információk elhelyezésének szabályai az Egyetem web szerverén .....	19
	22. § Domain nevek használatának, tanúsítványok igénylésének szabályai.....	20
IV.	FEJEZET JOGOSULTSÁGOK ÉS INFORMATIKAI BIZTONSÁG .....	20
	23. § Jogosultságok az Egyetem informatikai hálózatán .....	20
	24. § A jelszavak használatának szabályai.....	23
	25. § Internet és elektronikus levelezés használata.....	23
	26. § megtévesztés (Social engineering) .....	25
	27. § Saját eszközök használata (BYOD).....	26
	28. § Közösségi hálózatok használata.....	27
	29. § Szoftverjogtisztaság, szoftverek telepítése, frissítése .....	27
	30. § A számítógépes vírusvédelem .....	28
	31. § Katasztrófakezelés, mentés, visszaállítás, a szolgáltatás folytonossága .....	28
V.	FEJEZET A BERUHÁZÁSI PROGRAMIRODÁRA VONATKOZÓ KÜLÖNÖS SZABÁLYOK	
	29	
	32. § AZ V. FEJEZET HATÁLYA .....	29
	33. § Feladatmegosztás az InI és BPI között .....	29
	34. § BPI felhasználók köteleességei.....	32
VI.	FEJEZET A GYAKORLÓ ISKOLÁRA VONATKOZÓ KÜLÖNÖS SZABÁLYOK .....	32
	35. § A VI. fejezet hatálya.....	32
	36. § Feladatmegosztás az InI és Gyakorló Iskola között.....	33
	37. § Gyakorló Iskola felhasználóinak köteleességei.....	36
VII.	FEJEZET KOCKÁZATKEZELÉS.....	36
	38. § KOCKÁZATMENEDZSMENT .....	36
VIII.	FEJEZET VEGYES ÉS ZÁRÓ RENDELKEZÉSEK.....	37
	39. § Vegyes és Záró rendelkezések .....	37

---

# I. FEJEZET ÁLTALÁNOS RENDELKEZÉSEK

---

---

## PREAMBULUM

---

A Testnevelési Egyetem (a továbbiakban: Egyetem) Szenátusa – a nemzeti felsőoktatásról szóló 2011. évi CCIV. törvény (a továbbiakban: Nftv.), az információs önrendelkezési jogról és információszabadságról szóló 2011. évi CXII. törvény (Infotv.), az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Infobizttv.) vonatkozó rendelkezéseire figyelemmel – az informatikai hálózat üzemeltetésének, használatának, továbbá a megfelelő szintű informatikai biztonsági védelem biztosíthatóságának érdekében az alábbi szabályzatot alkotja.

---

### 1. § AZ IBSZ CÉLJA

---

- (1) Az Egyetem Informatikai Biztonsági Szabályzatának (a továbbiakban: IBSZ vagy szabályzat) alapvető célja, hogy az elérhető szolgáltatások használata, alkalmazása során biztosítsa az adatvédelem alkotmányos elveinek, az adatbiztonság követelményeinek érvényesülését. Megakadályozza a jogosulatlan hozzáférést, az adatok jogosulatlan megváltoztatását és nyilvánosságra hozatalát. Az Egyetemen működő informatikai rendszerekre specializálva a megelőző kontrollok alkalmazásával csökkenti az informatikai biztonsági kockázatok bekövetkezésének valószínűségét. Az IBSZ elő kell, hogy mozdítsa az informatikai és kommunikációs eszközök előírásoknak megfelelő és biztonságos használatát, ezzel támogatva, hogy az Egyetem által kezelt információvagyon sértetlensége, bizalmassága és rendelkezésre állása biztosított legyen.
- (2) Az Informatikai Iroda (a továbbiakban: InI) informatikai és kommunikációs hálózatot (a továbbiakban: hálózat), valamint a hálózathoz köthető informatikai eszközöket üzemeltet. Az Egyetem telephelyein strukturált és menedzselt hálózat működik, amely aktív, passzív és végponti elemekből áll.
- (3) A Hálózat célja az Egyetem egyes szervezeti egységei valamint a felhasználók között az információáramlás biztosítása, továbbá egyéb szolgáltatások nyújtása a felhasználók számára.

---

## 2. § AZ IBSZ HATÁLYA

---

- (1) A szabályzat hatálya kiterjed az Egyetem hálózatát használó felhasználókra és rendszergazdákra, továbbá a Hálózat teljes infrastruktúrájára, azaz a fizikai, infrastrukturális eszközökön kívül az adatok, szoftverek teljes körére, a folyamatokra, valamennyi telephelyre és a létesítményekre is. Felhasználónak minősülnek az Egyetem foglalkoztatottjai, hallgatói, valamint mindazok, akik oktatási, kutatási, tudományos, adminisztrációs és egyéb feladataikhoz állandó vagy eseti jelleggel, illetve egyéb jogviszony alapján az Egyetem hálózatát használják. Az egyetemi hálózat vonatkozásában az oktatók, a rendszergazdák, a hallgatók, és a felhasználók csoportjai különböző jogosultságokkal és kötelezettségekkel rendelkezhetnek.
- (2) A Beruházási Programirodára (a továbbiakban: BPI) valamint a Testnevelési Egyetem Gyakorló Sportiskolai Általános Iskola és Gimnáziumra (a továbbiakban: Gyakorló Iskola) vonatkozó speciális szabályok külön fejezetben kerülnek meghatározásra.

---

## 3. § ÉRTELMEZŐ RENDELKEZÉSEK

---

1. **Adatbiztonság:** Az adatok jogosulatlan megszerzése, módosítása és tönkretétele elleni műszaki és szervezési intézkedések és eljárások együttes rendszere.
2. **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.
3. **Adatgazda:** Felelős az általa kezelt adatokért, továbbá jogosult az adatok minősítése vagy osztályba sorolása elvégzésére.
4. **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, az adatokkal kapcsolatos fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők rögzítése.
5. **Adatkezelő:** Az a személy, aki vagy amely önállóan vagy másokkal együtt az adatok kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált

eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az általa megbízott adatfeldolgozóval végrehajthatja.

6. **Aktív hálózati eszköz:** Kapcsolók (switch-ek), forgalomirányítók (router-ek), vezeték nélküli hozzáférési pontok (Acces Pointok) és egyéb eszközök, amelyek segítségével a hálózat folyamatos üzemvitele biztosítható (bridge-ek, tűzfalak).
7. **Bizalmasság:** Az információ azon jellemzője, hogy csak egy előre meghatározott felhasználói kör (jogosultak) részére hozzáférhető, mindenki más számára titok. A bizalmasság elvesztése esetén a bizalmas információ arra jogosulatlanok számára is ismertté, hozzáférhetővé válik.
8. **Biztonság:** Az informatikai rendszerekben olyan előírások és szabványok betartását jelenti, amelyek a rendszer működőképességét, az információk rendelkezésre állását, sértetlenségét, bizalmasságát és hitelességét erősítik.
9. **BYOD (Bring Your Own Device – BYOD):** Saját mobileszközök (különösen: notebookok, tabletek, okos telefonok) munkahelyi környezetben való használata.
10. **Csomópont:** A szerver feladatokat ellátó és aktív eszközök csoportja az informatikai szolgáltatások ellátására.
16. **Felhasználó:** Az a természetes személy, aki az egyetemi informatikai infrastruktúrát használja.
17. **Felhasználói azonosító:** Az egyetemi címtárban tárolt egyedi azonosításra szolgáló rövid karaktersorozat, amely általában a felhasználó teljes nevéből képződik.
18. **Domain név:** Tartománynév (műszaki azonosító), amely elsősorban a könnyebb megjegyezhetősége miatt, az internetes kommunikációhoz nélkülözhetetlen Internet cím tartományok (IP címek) helyett használatos. Az Internet egy meghatározott részét, tartományát egyedileg leíró megnevezés, a számítógépek (kiszolgálók) azonosítására szolgáló névtartomány (különösen: tf.hu).
19. **DNS (Domain Name System):** Az internet neveket és címeket egymáshoz rendelő adatbázis, amely általában külön kiszolgáló gépen fut.
20. **Felhőszolgáltatás, felhőszolgáltató:** A feladatvégzéshez használt adatállományok, programok, szolgáltatások, stb. fizikailag nem a felhasználó számítógépén, hanem az interneten, egy szolgáltatónál található. Az adatok (e-mailek, címjegyzékek, naptárbejegyzések, és kedvenc linkek) felhőben való tárolásának előnye, hogy bárhonnan könnyen elérhetők, és akkor sem vesznek el, ha a felhasználó számítógépe tönkremegy.

21. **Hálózat:** Felhasználói számítógépek, illetve szerverek közötti adatátvitelt biztosító passzív elemekből és aktív eszközökből álló infrastruktúra.
22. **Hálózati rendszergazda:** A hálózati hardverrendszer hardver és szoftver üzemeltetője.
23. **Központi címtár:** Az Egyetem foglalkoztatottjainak felhasználói adatait tároló adatbázis.
24. **Közérdekű adat:** Az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv, vagy személy kezelésében lévő és tevékenységére vonatkozó vagy közfeladatának ellátásával összefüggésben keletkezett, a személyes adat fogalma alá nem eső, bármilyen módon vagy formában rögzített információ vagy ismeret, függetlenül kezelésének módjától, önálló vagy gyűjteményes jellegétől. Így különösen a hatáskörre, illetékességre, szervezeti felépítésre, szakmai tevékenységre, annak eredményességére is kiterjedő értékelésére, a birtokolt adatfajtákra, és a működést szabályozó jogszabályokra, valamint a gazdálkodásra, a megkötött szerződésekre vonatkozó adat.
25. **Közérdekből nyilvános adat:** A közérdekű adat fogalma alá nem tartozó minden olyan adat, amelynek nyilvánosságra hozatalát, megismerhetőségét vagy hozzáférhetővé tételét törvény közérdekből elrendeli.
26. **Megtévesztés (Social engineering):** Megtévesztés, az emberek bizalomra való hajlamának manipulatív kihasználása, információgyűjtés számítógépes rendszerekbe történő behatolás érdekében.
27. **Mobil eszközök:** Notebook, netbook, tablet, palmtop, mobiltelefon.
28. **Munkaállomás:** A felhasználó rendelkezésére bocsátott számítástechnikai eszköz, amely alapvetően hordozható vagy asztali számítógépből és a hozzá tartozó kiegészítőkből, illetve más, a hálózathoz vagy a munkaállomáshoz csatlakoztatható számítástechnikai eszközökből (különösen: mikrofon, kamera, scanner, tablet, telefon stb.) állhat.
29. **NEPTUN kód:** A NEPTUN rendszer szolgáltatásaihoz hozzáférést biztosító betűkből és számokból álló, legalább 6 karakter hosszúságú kód.
34. **Passzív eszközök:** Hálózati kábelezés, rendezők és csatlakozók.
35. **Rendelkezésre állás:** Annak biztosítása, hogy a szükséges információ a szükséges időben az arra jogosultak számára meghatározott formában hozzáférhető és elérhető legyen.

36. **Szerverhelyiség:** Fokozottan védett, naplózott bejutású, klimatizált, zárt helyiség, ahol a folyamatos működés feltételei az informatikai erőforrások számára biztosítottak.
37. **Tűzfal:** Olyan kiszolgáló eszköz (számítógép vagy program), amelyet a lokális és a külső hálózat közé, a csatlakozási pontra telepítenek annak érdekében, hogy az illetéktelen behatolásoknak ezzel is elejét vegyék. Ezzel együtt lehetővé teszi a kifelé irányuló forgalom, tartalom ellenőrzését is.
38. **VLAN:** A hálózat egy – a feladatoknak megfelelő, logikailag elkülönülő – meghatározott része. A VLAN-ok biztonsági feladatot is ellátnak, mivel elválasztják egymástól a részhálózatokat ezzel biztosítva, hogy sérülés, vagy támadás esetén csak az adott részterületre korlátozódjék az esetleges kár.
39. **VPN szolgáltatás:** Speciális hálózati elérés, amely az Egyetem hálózatához titkosított, és hitelesített kapcsolatot tesz lehetővé a világ bármely részéről. Két típusa létezik: felhasználói VPN (munkatársak távoli kapcsolódására), illetve site-to-site VPN (távoli telephelyek kapcsolódására).
40. **WEB adminisztrátor:** Az Egyetem honlapjának felügyeletét ellátó személy.
41. **WiFi, WLAN:** Szabványos vezeték nélküli adatátviteli technika.

---

## II. FEJEZET A HÁLÓZAT HASZNÁLATA

---

---

### 4. § A HÁLÓZAT HASZNÁLATÁNAK ALAPVETŐ SZABÁLYAI

---

Az Egyetem hálózatát csak a hatályos jogszabályokban és a vonatkozó szabályozókban foglaltak szerint lehet használni. A Hálózatot **tilos** használni az alábbi tevékenységekre, illetve ilyen tevékenységekre irányuló próbálkozásokra, kísérletekre:

- a) A mindenkor hatályos magyar jogszabályokba ütköző cselekmények előkészítése vagy végrehajtása, mások személyiségi jogainak megsértése, tiltott haszonszerzésre irányuló tevékenység (különösen: piramisjáték, stb.), szerzői jogok megsértése (különösen: szoftver és médiatartalom nem jogszerű megszerzése, tárolása, terjesztése);
- b) Másokra nézve sértő, vallási, etnikai, politikai vagy más jellegű érzékenységet bántó, zaklató tevékenység (különösen: pornográf, pedofil anyagok közzététele);
- c) A hálózati erőforrások, szolgáltatások olyan célra való használata, amely az erőforrás vagy a szolgáltatás eredeti céljától idegen (különösen: hírcsoportokba/levelezési listákra a csoport vagy lista témájához nem tartozó üzenet küldése);
- d) Profitszerzést célzó, direkt üzleti célú tevékenység és reklám;
- e) Mások munkájának zavarása vagy akadályozása (különösen: kéretlen levelek, hirdetések küldése);
- f) A hálózati erőforrások magáncélra való túlzott mértékű használata;
- g) A Hálózatot, a kapcsolódó hálózatokat, illetve erőforrásaikat indokolatlanul, túlzott mértékben, pazarló módon igénybevevő tevékenység (különösen: levélbombák, hálózati játékok, kéretlen reklámok);
- h) A Hálózat, a kapcsolódó hálózatok, illetve ezek erőforrásainak rendeltetésszerű működését és biztonságát megzavaró, veszélyeztető tevékenység, ilyen információknak és programoknak a terjesztése;
- i) A Hálózat erőforrásaihoz, a hálózaton elérhető adatokhoz történő illetéktelen hozzáférés, azok illetéktelen használata, gépek vagy szolgáltatások - akár tesztelés céljából történő - illetéktelen szisztematikus próbálgatása;



- j) A Hálózat erőforrásainak, a hálózaton elérhető adatoknak illetéktelen módosítására, megrongálására, megsemmisítésére vagy bármely károkozásra irányuló tevékenység folytatása;
- k) A Hálózat bármely szolgáltatásának szándékos, vagy hiányos ismeretekből, nem megfelelő körütekintéssel végzett beavatkozásokból fakadó zavarása, illetve részleges vagy teljes bénítása (leszámítva a rendeltetésszerű használat fenntartásához szükséges, a hálózati rendszergazdák, rendszermérnökök általi tudatos beavatkozásokat).
- l) Hálózati üzenetek, hálózati eszközök hamisítása: olyan látszat keltése, mintha egy üzenet más gépről vagy más felhasználótól származna.

---

## 5. § KÖZPONTI SZOLGÁLTATÁSOK AZ INFORMATIKAI HÁLÓZATON

---

A Hálózaton elérhető központi szolgáltatások

- a) Vezetékes és vezeték nélküli internet hozzáférés;
- b) Központi címtárszolgáltatás;
- c) Elektronikus levelezés (belső hálózati és távoli hozzáféréssel);
- d) Az egyetem on-line megjelenését biztosító web szerverek, egyetemi intranet szerverek;
- e) A tf.hu és tfgyakorlo.hu domain nevek kezelése;
- f) Jelszavas hozzáférés szabályozáson alapuló, védett adattároló területek a közös munkavégzéshez a központi szervereken;
- g) Biztonságos távoli munkavégzéshez VPN és DIRECTACCESS kapcsolat;
- h) Központi nyomtatási szolgáltatás (SAFEQ);
- i) Központi vírusvédelmi és spamszűrő szolgáltatások;
- j) Video Streaming szolgáltatás;
- k) <sup>1</sup>Továbbá az alábbi rendszerek elérhetőségének biztosítása;
- Tanulmányi információs rendszer (NEPTUN)
  - Gazdálkodási rendszer (SAP NEPTUN Gazdálkodási Modul);

---

<sup>1</sup> Módosította a Szenátus 35/2019. (V. 30.) határozata, hatályos 2019. május 31-től.

- Távoktatási rendszerek (LEARNING AGE, MOODLE);
- Integrált könyvtári adatbázis rendszer (ALEPH);
- Elektronikus iktatórendszer (POSZEIDON);
- Elektronikus szavazó rendszer (UNIPOLL);
- Személyügyi rendszer (SAP NEPTUN HR Modul);
- Complex Jegtár;
- Statistica statisztikai programcsomag;
- Belső kommunikációs rendszer (JAM).

---

## 6. § AZ INI KÖTELEZETTSÉGEI

---

A hálózati szolgáltatások nyújtása érdekében az InI kötelezettségei:

- a) Az oktatás, kutatás, tudományos munka, valamint az Egyetem működését biztosító valamennyi rendszer informatikai kiszolgálása, a belső hálózati szolgáltatásokat, valamint az Egyetem internetes megjelenését, kapcsolattartását biztosító rendszerek folyamatos üzemeltetése.
- b) A Hálózat üzembiztosságának fenntartása, a hatályos szabályozók betartása, az elhelyezett adatok védelme.
- c) A Hálózat folyamatos karbantartása, fejlesztése, a felmerülő igényekhez igazítása, az újabb technikai lehetőségek alkalmazhatóságának folyamatos megteremtése.
- d) Az új informatikai és kommunikációs eszközök, rendszerek szolgáltatásainak, rendszerbe illeszthetőségének vizsgálata, a vonatkozó döntések meghozatalának előkészítése az alkalmazhatóságukról, vagy alkalmazásuk kizárásáról.
- e) A felhasználók részéről felmerülő igények elemzése, rangsorolása, javaslattétel a döntésre jogosult egyetemi vezetők számára.
- f) A felhasználók személyi számítógépeinek (asztali és hordozható) felkészítése, a napi munkához szükséges programok, programrendszerek telepítése és konfigurálása, működési zavar, meghibásodás, rendellenes működés esetén a hibaelhárítás lehető leggyorsabb megkezdése.

- g) Szankciók alkalmazása a biztonsági előírásokat megsértő felhasználókkal szemben és a szankciókkal sújtott felhasználók, valamint munkahelyi vezetőik haladéktalan tájékoztatása. A szankciók alkalmazása ellen a hallgató a Tanulmányi Hivatal vezetőjénél, a foglalkoztatott a munkahelyi vezetőjénél élhet panasszal.
- h) Az Egyetemen belüli levelezés során készült naplók, valamint az Egyetemről kifelé és az Egyetemre befelé irányuló levelezés, továbbá az internet használata során készült naplók 30 napig történő megőrzése.
- i) A kommunikációs rendszerek viszonylatában a jogszabályokban meghatározott nyilvántartások, naplók vezetése, amelyeket meghatározott esetekben, a vonatkozó jogszabályoknak megfelelő megkeresés alapján az illetékes hatóságoknak kiszolgáltathat.
- j) A Hálózat működéséhez, karbantartásához időközönként szükséges, előre tervezhető üzemszünetek, leállások 2 nappal a tervezett időpont előtt az Egyetem honlapján és a JAM rendszer hírek üzenő falán, továbbá az érintettek számára az esedékesség előtt legalább 1 órával belső hálózati üzenet formájában történő bejelentése.
- k) Az általános informatikai ismereteken túli, az adott szolgáltatás igénybevételéhez szükséges ismeretek nyújtása.
- l) A szervezeti egységek vezetői által meghatározott, adatvédelmi szempontból kritikus adatokat (különösen: tanulmányi, személyügyi, pénzügyi, ügyviteli információkat) tároló számítógépek számára internetkapcsolat nélküli biztonságos belső hálózati kapcsolat biztosítása.

---

## 7. § AZ INI JOGAI

---

Az InI jogosult:

- a) A Hálózat által nyújtott szolgáltatások körének, az egyes szolgáltatások igénybevételei feltételeinek meghatározására. A hálózati biztonság érdekében bármely szolgáltatás használatát felhasználói azonosításhoz kötheti, a felhasználók körét szűkítheti, korlátozhatja.
- b) A Hálózat biztonsága érdekében a Hálózat használatának szabályait megsértő felhasználók hozzáférési jogosultságainak szűkítése, vagy kizárása a szolgáltatások igénybevételéből.

- c) A Hálózat biztonságos működését veszélyeztető vagy zavaró számítógépek, kommunikációs és más berendezések, eszközök Hálózatról történő előzetes értesítés nélküli leválasztása, valamint intézkedés a zavar, illetve veszélyhelyzet megszüntetésére.

---

## 8. § A FELHASZNÁLÓK JOGAI

---

A Hálózat használata során a felhasználó jogosult:

- a) A munkavégzéshez szükséges programokkal ellátott, egy vagy több személy használatára beállított, felkészített számítógép, kommunikációs eszközök használatára.
- b) A munkavégzéshez szükséges mértékben – a használatra vonatkozó, a felhasználó által elfogadott (és aláírással igazolt) feltételek mellett – a hálózati szolgáltatások igénybevételére.
- c) Működési zavar, meghibásodás, rendellenes működés esetén segítséget kérni.
- d) A munkavégzéshez szükségesnek ítélt eszközök, szoftverek beszerzését, telepítését igényelni. Az igény jogosságát a szervezeti egység vezetőjével együttműködve – a műszaki és ellátási igazgatót egyidejűleg tájékoztatva – az InI vezetője bírálja el.
- e) Levelező szolgáltatás és saját elektronikus postafiók használatára. Az InI a felhasználói fiókot az Egyetem rendszerén belül előretelepített kliens programmal, illetve web felületen teszi elérhetővé.
- f) A Hálózat üzemeltetői részéről a személyhez fűződő jogainak tiszteletben tartására, amelytől eltérni csak jogszabály által meghatározott esetekben lehet.
- g) Tájékoztatásra – a lehetőségek függvényében – a Hálózat technikai fejlesztéseiről, problémáiról (tervezett vagy rendkívüli eseményekről).
- h) Tájékoztatásra az esetlegesen vele szemben, az egyetemi Hálózaton foganatosított szankciókról.
- i) A felhasználókra vonatkozó szabályok megismerésére.

---

## 9. § A FELHASZNÁLÓK KÖTELESSÉGEI

---

A Hálózat biztonságos használata érdekében a felhasználó köteles:

- a) Az IBSZ-t megismerni, az abban foglaltakat betartani, valamint együttműködni a Hálózat üzemeltetőivel a benne foglaltak betartatása érdekében.
- b) A Hálózatot annak céljaival megegyezően használni.
- c) A Hálózaton csak a számára engedélyezett erőforrásokat használni.
- d) Tevékenységével az egyetemi hálózaton feladataikat végzők tevékenységét nem zavarni, akadályozni, veszélyeztetni.
- e) A hálózati szolgáltatások igénybevételéhez használatos jelszavait titkosan kezelni, előírt gyakorisággal változtatni, az IBSZ jelszóhasználattal kapcsolatos előírásait betartani (**Tilos** a hozzáférési jogosultságok, jelszavak átruházása, mások jelszavának használata, a hálózat, a levelezőrendszer - a tulajdonos felhatalmazása nélkül - más nevében történő igénybevétele).
- f) Gondoskodni adatainak tőle elvárható védelméről és helyi mentéséről.
- g) A hálózati szolgáltatások, a távfelügyeleti rendszerek működéséhez szükséges programok telepítését lehetővé tenni.
- h) A számára biztosított informatikai és kommunikációs eszközöket működőképességben megőrizni, ellenőrzéskor kérésre bemutatni, a jogviszony megszűnéskor visszaszolgáltatni. A felhasználó a részére biztosított eszközöket, berendezéseket nem bonthatja meg. A hardver és szoftverkörnyezetet - beleértve a számítógépes vírusellenőrzéssel, és vírusirtással kapcsolatos szoftvereket is - nem vagy csak az InI vezetőjének külön engedélyével módosíthatja, az eszközök hálózati és egyéb beállításában működést befolyásoló módosításokat nem végezhet.
- i) Felelősséget vállalni az egyetem tulajdonát képező, informatikai, kommunikációs eszközökben vagy eszközökkel okozott szabályellenes cselekedetekért, károkért. Az ezekből eredő esetleges működési zavar, adatvesztés utáni helyreállítás, javítás költségeit megtéríteni.
- j) USB memóriakulcsok, vagy más külső adathordozók csatlakoztatása után az InI által biztosított számítógépes vírusellenőrző eszközökkel a vírusellenőrzést, vírusirtást végrehajtani.
- k) Meghibásodás, üzemzavar észlelésekor, vírusfertőzés vagy annak gyanúja esetén haladéktalanul értesíteni az InI-t, valamint a számítógép további használatát az InI intézkedéséig felfüggeszteni. A hibaelhárítás folyamán az InI szakembereivel együttműködni, számukra a szükséges információkat megadni.

- l) A Hálózaton, az egyetemi levelező rendszerben és a telefonkönyvben tárolt adatokban (különösen: név, szervezeti egység, beosztás, munkahelyi telefonszám, iroda) történt változásokat (különösen: névváltozás, más szervezeti egységhez történt áthelyezés, telefonszám változás) az InI-nél bejelenteni.
- n) Amennyiben tudomására jut, hogy bárki megsértette a szabályzatban foglaltakat, haladéktalanul tájékoztatni az InI-t és az érintett szervezeti egység vezetőjét.

---

#### 10. § A MEG NEM ENGEDETT TEVÉKENYSÉGEK SZANKCIÓI

---

A szabályzat megsértésének gyanúja esetén a cselekményt ki kell vizsgálni. A vizsgálatra kijelölt háromtagú felelős kivizsgáló bizottságnak (melynek tagjai az érintett szervezeti egység vezetője, jogi igazgató és az InI vezetője vagy az általuk delegált személy) javaslatot kell tennie a szükséges intézkedésekre, amelyekre a következők az irányadók:

- a) A szabályzat gondatlan megszegése esetén az elkövetőt figyelmeztetésben kell részesíteni.
- b) A szabályzat ismételt megszegése szándékos elkövetésnek minősül.
- c) A szabályzat szándékos megsértése esetén az elkövető a Hálózat használatából ideiglenesen vagy véglegesen kizárható, és az eset súlyosságától függően eljárás lefolytatása kezdeményezhető ellene. A Hálózat szolgáltatásait csak az eljárás lefolytatása után és annak eredményétől függően veheti újra igénybe.
- d) Amennyiben a szabályzat megsértéséből következően anyagi kár keletkezett, a felhasználó köteles azt megtéríteni.

---

#### 11. § A HÁLÓZAT FELÉPÍTÉSE

---

(1) Az Egyetem több telephelyes hálózat, melynek felépítése az alábbi:

- a) A Hálózata tűzfalakkal védett, logikailag szegmensekre osztott. Telephelyenként külön-külön szegmensekben működnek a foglalkoztatotti, tantermi illetve a kollégiumokban működő gépek, valamint a több irányba szolgáltatást nyújtó szerver számítógépek. A hálózati működés biztosításához, illetve speciális feladatokhoz további szegmensek is kialakításra kerülhetnek, ez a felépítés a felmerülő igényekhez, szükségletekhez igazodva változtatható.
- b) Az egyes telephelyek logikai felépítése hasonló, a telephelyek közötti forgalom tűzfalakkal szabályozott, a definiált informatikai szolgáltatások elérhetősége minden telephely esetében biztosított.

- c) Az egyes számítógépek, illetve szolgáltatások különböző szegmensekbe történő besorolását az InI vezetője határozza meg.

(2) A Hálózat mindenkor műszaki paramétereit külön dokumentáció tartalmazza.

---

## 12. § A HÁLÓZAT ÜZEMELTETÉSE, ÉPÍTÉSE, BŐVÍTÉSE

---

- (1) Kizárólag az InI jogosult a Hálózat bővítésére, átalakítására. A Hálózatot, a lehetőségeket figyelembe véve az INI az igényeknek megfelelően folyamatosan bővíti, karbantartja. Hálózat vagy hálózatrész építése, módosítása, valamint az Egyetem rendszerén kívüli szolgáltatásokhoz, hálózatokhoz állandó kapcsolat (különösen site-to-site VPN) létesítése külső erőforrások bevonása esetében is csak az InI jóváhagyásával történhet.
- (2) Arra jogosultsággal nem rendelkező személy a kialakított rendszeren nem változtathat, végpontot nem helyezhet át, aktív vagy szerver-feladatokat ellátó eszközt a Hálózatra nem kapcsolhat rá és arról nem kapcsolhat le.

---

## 13. § AZ EGYETEMI INFORMATIKAI ÉS KOMMUNIKÁCIÓS HÁLÓZAT HASZNÁLATÁNAK SZABÁLYAI

---

A Hálózat használata folyamán az alábbi szabályok betartására kell különös figyelmet fordítani:

- a) Új hálózatrészek építésének tervezését, kivitelezését, a már megépült hálózatrészek módosítását csak az InI vagy felügyeletével az Egyetem által megbízott kivitelező végezheti.
- b) Hálózati aktív eszközöket (repeater, HUB, switch, router, tűzfal) csak az InI csatlakoztathat a Hálózatra vagy köthet le arról. Az aktív eszközök kapcsolatainak megbontására és az eszközök bármilyen konfigurálására csak az InI jogosult.
- c) A Hálózatra bármilyen berendezést csak az InI engedélyével lehet csatlakoztatni. Ha az eszköz adattárolásra is alkalmas, akkor a csatlakoztatás után vírusellenőrzést kell végrehajtani. Az adatok tárolására vonatkozó jelen és más vonatkozó egyetemi szabályzatok és előírások betartására különös figyelmet kell fordítani.
- d) Az InI az engedély kiadását megtagadhatja, ha a csatlakoztatni kívánt berendezés a Hálózat működését, rendeltetésszerű használatát, működési vagy adatvédelmi biztonságát (a továbbiakban: hálózati biztonság) veszélyeztetné.

- e) Saját személyi számítógép csak az InI-nek történő előzetes bejelentés, a gépek alapvető paramétereinek és felhasználójának nyilvántartásba vétele után, az InI által megszabott feltételekkel használható, kivéve az „f” pontban meghatározott eseteket.
- f) Időszakos rendezvények (különösen: konferenciák, gyakorlatok vagy más események) idején, az Egyetem területén működő vezeték nélküli internet szolgáltatást az InI által meghatározott feltételekkel (ideiglenes wifi szegmensek kialakításával), be nem jelentett számítógépekkel is igénybe lehet venni. A használathoz szükséges hitelesítés módszertanát az InI határozza meg.
- g) A WIFI csatlakozást igénybevevő mobil eszközök használatára ugyanazok a szabályok vonatkoznak, mint más számítógépekre. A mobilitásukból adódó nagyobb sebezhetőségekre tekintettel a rajtuk tárolt adatokra és a fizikai biztonságukra nagyobb figyelmet kell fordítani.
- h) A hálózati aktív eszközök feszültségmentesítését (kikapcsolását) áramszünet, természeti csapás (különösen: tűz, vízbetörés vagy más rendkívüli esemény), áraműtés, vagy annak gyanúja, egyértelmű készülék meghibásodás (különösen: füst, látható zárlat vagy más látható műszaki hiba) kivételével csak az InI végezheti.
- i) Az Egyetemen rádiófrekvenciás és mikrohullámú frekvenciatartományban sugárzó infokommunikációs eszközt kizárólag az InI által engedélyezett frekvencián és az engedélyezett időtartamra lehet használni. Az engedélyt a használat előtt legalább 30 nappal írásban kell igényelni.
- j) Saját tulajdonú, vagy más szervezet tulajdonát képező számítógépek Hálózatra kapcsolását csak egyedi esetekben, az InI által elvégzett előzetes ellenőrzés és a használathoz előírt programok telepítése után, az InI engedélyezheti. Az ezzel kapcsolatos részletszabályokat a 28. § tartalmazza.

---

#### 14. § A HÁLÓZATI HIBÁK ELHÁRÍTÁSA

---

A hálózat bármilyen jellegű meghibásodása esetén a hiba elhárítását az InI a lehető leghamarabb, de legkésőbb a bejelentést követő első munkanapon megkezdi. Ha a hiba elhárításához külső segítség szükséges vagy a hiba oka a Hálózaton kívül keletkezett, akkor a hibát bejelenteni, elhárítására intézkedni, a javítást megrendelni csak a meghibásodásban érintett hálózatrész üzemeltetéséért felelős szakemberek jogosultak. Mind a hálózati



meghibásodásról és az ezzel kapcsolatban meg tett intézkedésekről tájékoztatni kell az InI vezetőjét.

---

### III. FEJEZET AZ INFORMATIKAI HÁLÓZAT SZOFTVER ÜZEMELTETÉSE

---

---

#### 15. § TÁMOGATOTT PROTOKOLLOK

---

- (1) Az Egyetem Hálózatának elsődleges protokollja az IP protokoll, támogatottak az IP feletti protokollok. A hálózatban helyileg megengedett, de nem támogatott az IP-n kívüli, szabványos protokollok (NetBEUI/Netbios, NWLink, AppleTalk, IPX) használata.
- (2) Az InI az egyes protokollok, portok, illetve az ezeket használó alkalmazások használatát a működési stabilitás és az adatbiztonság érdekében időlegesen vagy véglegesen, VLAN-onként, telephelyenként vagy az Egyetem teljes hálózatára kiterjedő hatállyal korlátozhatja vagy megtilthatja.

---

#### 16. § KRITIKUS ADATOKAT TARTALMAZÓ SZÁMÍTÓGÉPEK HASZNÁLATA

---

Az adatvédelmi szempontból kritikus adatokat (különösen: tanulmányi, személyügyi, pénzügyi, ügyviteli információkat) tároló számítógépek védelmére fokozott figyelmet kell fordítani. Ha a működtetésük nem teszi kifejezetten szükségessé, akkor az internethez történő csatlakoztatásuk **tilos**. Ezen gépek körét az érintett szervezeti egységek vezetői határozzák meg. Az igényelt, internetkapcsolat nélküli biztonságos belső hálózati kapcsolat biztosítása az InI feladata.

---

#### 17. § SZEMÉLYI SZÁMÍTÓGÉPEK FELKÉSZÍTÉSE A HASZNÁLATRA

---

- (1) Az egyes hálózati szolgáltatások igénybevételére használható, illetve a technikai segítségnyújtással támogatott programok körét az InI a telepítési protokollban határozza meg.
- (2) A folyamatos munkavégzésre kijelölt számítógépeken - az első hálózatra kapcsolás előtt - az előzetes ellenőrzést, a használathoz előírt programok telepítését, a feladatra történő felkészítést, valamint a személyre szabást az InI szakemberei az erre a célra kijelölt, speciálisan kialakított helyiségben hajtják végre.

- (3) Az InI a számítógépeket a telepítési protokoll szerint előre telepített operációs rendszerrel, irodai programcsomaggal, vírusvédelmi szoftverrel és a hálózati szolgáltatások igénybevételére alkalmas programokkal, személyre szólóan felkészítve adja át.
- (4) A számítógép hálózati beállításainak, rendszerlemeinek módosítására, az operációs rendszer és a gépre feltelepített szoftverek konfigurációjának megváltoztatására, szükség szerinti újratelepítésére vagy új programok telepítésére kizárólag az InI, illetve az általa erre felhatalmazott és megfelelően felkészített személyek jogosultak.
- (5) Ha a felhasználó számára átadott számítógép a névre szóló felkészítés után másik felhasználóhoz kerül, akkor az új felhasználó feladata kezdeményezni az InI-nél, hogy a gép szoftver konfigurációja, és a rá vonatkozó hálózati bejegyzések megfelelő módon, az InI által módosításra kerüljenek.

---

#### 18. § SZERVEREK ÜZEMELTETÉSE

---

- 1) Az InI által üzemeltetett számítógépeken kívül szerverek, informatikai szolgáltatások elindítása, ilyen szolgáltatást nyújtó számítógépek Hálózatra kapcsolása az InI-vel való előzetes egyeztetés után történhet.
- 2) Az Egyetem szervereinek felügyelete - beleértve az operációs rendszerek karbantartását, frissítését is - az egyetemi rendszergazdák feladata.

---

#### 19. § TÁVOLI MUNKAVÉGZÉS

---

- (1) Az InI a szervezeti egységek vezetőinek javaslata alapján lehetővé teszi a kijelölt felhasználók részére a Hálózat bizonyos részeinek távoli elérését. A távoli munkavégzés során is be kell tartani a jelen szabályzat előírásait, különös tekintettel az illetéktelen hozzáférés megakadályozására. A távoli hozzáférés esetében minimális biztonsági követelmény, hogy a hitelesítés során használt jelszót és az adatforgalmat titkosítani szükséges.
- (2) A Hálózatra a távoli munkavégzés során VPN és DIRECTACCESS szolgáltatás segítségével csatlakoztatott eszközök fokozott védelme, karbantartása, vírusvédelme és az illetéktelen hozzáférés megakadályozása a felhasználó kiemelt kötelessége.

---

## 20. § ADATOK ELHELYEZÉSÉNEK SZABÁLYAI A HÁLÓZATON

---

- (1) Az InI a több felhasználó által közösen használt adatok biztonságos, illetéktelen hozzáféréstől védett elhelyezésére a szervereken szükség szerint tárhelyet biztosít. A tárterülethez történő hozzáférés beállítása az adatokért felelős szervezeti egység vezetőjének írásos igénye alapján történik.
- (2) A felhasználók a tevékenységükkel kapcsolatosan keletkezett adatokat a hálózati szervereken a számukra kijelölt könyvtárakban helyezhetik el. Ez a tárterület kizárólag e tevékenységekkel kapcsolatos adatok tárolására használható. A könyvtárak elnevezésének egyértelműen utalnia kell a tárolt adattartalomra. A tárterületek adattartalmáért a jogosult felhasználó felel.
- (3) A fájlok elérési útvonalának a teljes hossza maximum 256 karakter lehet, amelybe a könyvtárstruktúrát alkotó könyvtárak nevei, a fájlnev és a kiterjesztés is kötelezően beleértendő.
- (4) A Hálózat tárterületével történő gazdálkodás az InI feladata és felelőssége.

---

## 21. § ADATOK, INFORMÁCIÓK ELHELYEZÉSÉNEK SZABÁLYAI AZ EGYETEM WEB SZERVERÉN

---

- (1) Az Egyetem internetes megjelenítését biztosító web szervereit az InI üzemelteti, felel azok működőképességéért. Az egyetemi honlap tartalomkezelő rendszerének üzemeltetését az Egyetemmel erre a feladatra szerződött partner végzi. A kijelölt tartalmi honlapfelelős végzi a honlap tartalmak feltöltését.
- (2) Az egyetemi honlap egységes megjelenéséért, tartalmáért az Egyetemi kommunikációért és sajtómegjelenésért felelős szervezeti egysége felelős.
- (3) A honlapon csak publikus, közérdekű és közérdekből nyilvános adatok jeleníthetők meg.
- (4) Az egyes szervezeti egységekre vonatkozó információk tartalmáért, pontosságáért, naprakészségéért az adott szervezeti egység vezetője a felelős.
- (5) Az egyetemi honlapon történő adat/információ megjelenítésnél szigorúan be kell tartani a személyes és közérdekű adatok védelmére és biztonságára vonatkozó jogszabályokban meghatározott előírásokat.

---

## 22. § DOMAIN NEVEK HASZNÁLATÁNAK, TANÚSÍTVÁNYOK IGÉNYLÉSÉNEK SZABÁLYAI

---

- (1) Az Egyetem által használt internetes megjelenést szolgáló domain nevek igénylésére, kezelésére kizárólag az InI jogosult. Új domain név, SSL kapcsolatot igénylő szerver és felhasználói tanúsítvány, lejárt helyett új tanúsítvány igénylése esetén az InI vezetőjéhez kell fordulni.
- (2) Az Egyetem életével kapcsolatos események hivatalos internetes megjelentetésére elsődleges forrásként az ezeken a domain neveken belül működtetett web felületek szolgálnak.

---

## IV. FEJEZET JOGOSULTSÁGOK ÉS INFORMATIKAI BIZTONSÁG

---

---

### 23. § JOGOSULTSÁGOK AZ EGYETEM INFORMATIKAI HÁLÓZATÁN

---

- (1) A Hálózaton nyújtott szolgáltatások igénybevétele kötelező felhasználói azonosításhoz – az egyedi számítógépeken és a hálózati kapcsolatokhoz is érvényes felhasználói azonosító és jelszó használatához (hitelesítéshez) – kötött.
- (2) Az Egyetem kollégiumaiban és a rendezvények idejére biztosított hálózatokban nem kötelező az egyetemi felhasználói azonosítás. Ezekből a hálózati szegmensekből csak internet elérés biztosítható, más központi szolgáltatás nem érhető el.
- (3) Hálózat hozzáférési jogosultságok kiosztása:
  - a) A felhasználók és a rendszergazdák jogosultságait az illetékes szervezeti egységek vezetőinek, illetve az adatgazdák írásos igényei alapján az InI határozza meg.
  - b) A jogosultságok kiosztásakor alapelveként kell kezelni, hogy minden funkcióhoz illetve feladathoz csak az ellátásához feltétlenül szükséges és elégséges mértékű jogosultságot kell biztosítani.
  - c) A Hálózathoz felhasználói hozzáférési jog mindenkit megillet, aki az intézménnyel hallgatói vagy foglalkoztatási jogviszonyban áll, és aláírásával igazolta, hogy az IBSZ tartalmát megismerte, annak betartását vállalja.
  - d) Az InI hozzáférési jogosultságot adhat az Egyetemmel jogviszonyban nem álló felhasználónak is (különösen: vendég-oktató, rendezvény résztvevője).

- e) A felhasználótól a jogosultsági szintjének megfelelő jogot megtagadni csak indokolt esetben lehet. A jogosultsági szintnek megfelelő szabályok betartása a Hálózatba nem kötött eszközök használata esetén is kötelező.
- f) Biztonsági okokból és a későbbi visszakereshetőség, elemzések elvégzése érdekében - a szervereken - a Hálózatba történő sikeres és sikertelen belépési kísérletek valamint hálózati forgalmi adatok is rögzítésre, naplózásra kerülnek.
- g) Ha jogosulatlan hozzáférés történt, vagy a jogosulatlan hozzáférés gyanúja merül fel, a jelszót azonnal meg kell változtatni.

(4) Hálózat hozzáférési jogosultságok szintjei az Egyetem informatikai Hálózatán:

Szint	Jogosultak	Jogok	Felelős
Külső	Vendégoktató, kutató, tanfolyami, rendezvény résztvevő	Internet elérés, WiFi használat	Szervezeti egység vezetője
Alap	Egyetem hallgatói, foglalkoztatottjai	Egyéni azonosítás alapján lehetővé válik az oktatáshoz, tanuláshoz, munkához szükséges adatok, programok, levelezés, valamint az Internet elérése.	Szervezeti egységek vezetői
Adminisztrátor	Adminisztrációval kapcsolatos munkakörök	Alapszint + hozzáférés az adminisztrációs, dokumentációs rendszerekhez, szervezeti egység közös lemezterületéhez.	Szervezeti egység vezetője
Oktató, kutató	Az Egyetem oktatói, kutatói	Alapszint + hozzáférés az oktatói, kutatói rendszerekhez, a szervezeti egység közös lemezterületéhez, a hallgatókkal kapcsolatos adminisztrációs adatokhoz.	Szervezeti egységek vezetői
Tanulmányi	Tanulmányi Hivatal foglalkoztatottjai a jogosultsági szintnek megfelelően	Alapszint + teljes körű hozzáférés a Neptun rendszer adminisztratív moduljaihoz. Hozzáférés a szervezeti egység közös lemezterületéhez.	Tanulmányi hivatalvezető

Gazdasági	Gazdasági Igazgatóság foglalkoztatottjai a jogosultsági szintnek megfelelően	Alapszint + hozzáférés a gazdálkodással és a foglalkoztatottakkal kapcsolatos rendszerekhez.	Gazdasági Igazgató
Jogi	Jogi Igazgatóság foglalkoztatottjai a jogosultsági szintnek megfelelően	Alapszint + hozzáférés a szervezeti egység közös lemezterületéhez valamint a jogtár adatbázis rendszerekhez.	Jogi Igazgató
Humánpolitikai	HR Iroda és a Gazdasági Igazgatóság bérügyi feladatokkal foglalkozó munkatársai a jogosultsági szintnek megfelelően	Alapszint + hozzáférés a szervezeti egység közös lemezterületéhez valamint a foglalkoztatottakkal kapcsolatos rendszerekhez.	HR Irodavezető, Gazdasági Igazgató
Rendszergazda (hálózati, szerverüzemeltető, szoftverüzemeltető, szervezeti)	Informatikai Iroda rendszergazdái	Korlátlan jog a rendszergazda által felügyelt rendszerekhez (különösen: munkaállomások hálózat, storage, szerverek, adatbázisok, mentési rendszer, egyetemi szervezet által felügyelt szerver).	Informatikai Irodavezető
Alkalmazás rendszergazda	Egy adott alkalmazás informatikai rendszergazda	Korlátlan jog az adott alkalmazáshoz. (különösen: Email rendszer, Poszeidon, Moodle, Learning Age, KIRA, SAP NEPTUN Gazdálkodási Modul, SAP NEPTUN HR Modul, Neptun, JAM, Unipoll). <sup>2</sup>	Informatikai irodavezető, egyetemi szervezeti egység vezetője

<sup>2</sup> Módosította a Szenátus 35/2019. (V. 30.) határozata, hatályos 2019. május 31-től.

---

## 24. § A JELSZAVAK HASZNÁLATÁNAK SZABÁLYAI

---

- (1) A felhasználói jelszavak generálásának és átadásának bizalmasan kell történnie. A jelszavak kiválasztásánál a következő alapvető szabályokat kell betartani:
- a) A jelszó hossza nem lehet rövidebb nyolc karakternél, tartalmaznia kell legalább kettő számjegyet, valamint legalább kettő betűt. A jelszavak használatakor ajánlott a számok, valamint a kis és nagybetűk keverése, továbbá olyan jelszavak használata, amelyek nem találhatók ki könnyen a felhasználó személyes adataiból
  - b) A hálózati belépésre jogosító jelszót kötelező - az egyéb jelszavakat ajánlott rendszeresen, de legalább - 90 naponta újra cserélni.
  - c) **Tilos** a login nevet jelszóként használni.
  - d) **Tilos** a jelszót nyilvános helyen kiírva tartani (különösen: a monitoron).
  - e) **Tilos** azonos vagy az abc-ben, a billentyűzeten egymást követő számokból vagy betűkből álló jelszót használni.
- (2) Az (1) bekezdésben meghatározottak jogellenes megszegésével okozott kárért a felhasználó kártérítési felelősséggel tartozik.

---

## 25. § INTERNET ÉS ELEKTRONIKUS LEVELEZÉS HASZNÁLATA

---

- (1) A Hálózaton biztosított internetelérés és levelezés a munkavégzést, az egyetemi célokat hivatott szolgálni.
- (2) Az előző bekezdésben leírt célok elérése érdekében és szükség esetén – különösen biztonsági okokból, a Hálózat terheltségének csökkentése érdekében – egyes honlapok, külső levelező rendszerek elérése tiltásra kerülhet.
- (3) Az InI a felhasználók számára biztosítja az interneten keresztüli elektronikus levelezés lehetőségét. A szükséges e-mail címeket az erre a célra rendszeresített igénylőlap kitöltésével lehet igényelni, melynek aláírásával a felhasználó kötelezettséget vállal a jelen szabályzatban foglaltak betartására.
- (4) A hálózati szolgáltatások használatának jogosultsága a jogviszony megszűnéséig tart. Az illetékes rendszergazdák az Egyetemi kilépő lap benyújtásakor, az azon megjelölt határidővel (ami fősabályként a jogviszony megszűnésének a napja, indokolt eset-

ben az azt követő 30. nap) gondoskodnak a volt foglalkoztatott hálózati jogosultságainak megszüntetéséről, törléséről. Egyedi méltánylást igénylő esetben – a rektor vagy a kancellár a hozzáférés meghosszabbításáról rendelkezhet.

- (5) Az Egyetem működésével kapcsolatos levelezéshez, kiadványokban történő megjelenítéshez csak a hivatalos egyetemi e-mail cím használható és jeleníthető meg.
- (6) Az InI a tf.hu tartományban az egyes szervezeti egységek számára, illetve az Egyetem működésével kapcsolatos speciális feladatokra tematikus e-mail címet biztosíthat. Ezeknek az e-mail címeknek utalniuk kell a szervezeti egységre vagy az adott feladatra. **Tilos** ilyen célra a saját személyes e-mail címeket használni.
- (7) A felhasználók a Hálózat és a levelezőrendszer használata folyamán különösen az alábbi szabályokat kötelesek betartani:
  - a) Az egyetemi e-mail címek - a személyhez kötéstől függetlenül - a munkavégzést, az egyetemi célokat hivatottak szolgálni.
  - b) A felhasználó az egyetem címjegyzék felhasználásával, szervezeti egységeknek szóló körlevelet csak a vezetőjének írásbeli engedélyével küldhet. Az Egyetem életével, eseményeivel kapcsolatos széles körű tájékoztatás a JAM rendszeren keresztül történhet. Az InI kötelessége, hogy az Egyetem érdekeit sértő tartalmakat a lehető legrövidebb időn belül törölje. Ha az InI a kérdésben önállóan nem tud dönteni, akkor köteles a problémát a rektornak vagy a kancellárnak azonnal jelezni és döntésüket haladéktalanul végrehajtani.
  - c) Az Egyetem levelezőrendszere a nyílt interneten, web felületen is elérhető (web-mail). A levelező rendszer web felületen történő használata csak megbízható környezetben ajánlott.
  - d) Ha a felhasználó a postafiókjába 3 hónapon keresztül nem lép be, a postafiók – a tartalmának változatlanul hagyása mellett – zárolásra kerül, de továbbra is fogadja a leveleket. További 3 hónap elteltével a levelek fogadása megszűnik. Újabb 3 hónap elteltével a felhasználói e-mail cím és a postafiók a tartalmával együtt törlésre kerül.
  - e) **Tilos** minden olyan üzenetküldés, amelyet a nemzetközi hálózatok írott és íratlan szabályai (netikett) tiltanak.



- f) **Tilos** olyan adatok, levelek továbbítása, amelyben bármelyik, a feladó azonosítására szolgáló információ hamis, értve ezalatt az elektronikus levél szándékosan hamis feladóval történő küldését is, továbbá a feladó vagy a küldő eltitkolását, hamisított fejlécű IP csomagok vagy üzenetek küldését.
  - g) **Tilos** a levelezőrendszeren biztonsági szempontból érzékeny adatot továbbítani, illetéktelen személy részére hozzáférhetővé tenni.
  - h) **Tilos** olyan tartalmú levelet küldeni, amely bármilyen más személy, csoport vagy társaság személyes, illetve üzleti érdekeit sértheti vagy veszélyeztetheti.
  - i) **Tilos** másokra nézve sértő, vallási, etnikai, politikai vagy más jellegű érzékenységet bántó, zaklató tevékenység közzététele.
  - j) **Tilos** lánclevelet, kéretlen reklámokat (spam) küldeni.
  - k) **Tilos** az illegális tartalmak terjesztése és olyan tartalmú üzenetek küldése, amely a másik felhasználó rendszerének megsemmisítését célozza, vagy működését hátrányosan befolyásolja.
- (10) Az Egyetem fenntartja a jogot arra, hogy a vonatkozó jogszabályok betartásával a felhasználók internet forgalmát, annak tartalmát figyelemmel kísérje és naplózza, a veszélyt rejtő internetes honlapok elérését letiltja. A naplózásra a Hálózat biztonságos és rendeltetés szerinti használatának, optimális leterheltségének, sebességének kialakítása és fenntartása érdekében kerülhet sor.

---

## 26. § MEGTÉVESZTÉS (SOCIAL ENGINEERING)

---

A Hálózat biztonságát legegyszerűbben a social engineering (megtévesztés) módszerrel lehet veszélyeztetni. Ez a módszer az emberek manipulálására, segítőkészségére, gyanútlanosságára, hiszékenységére alapozva teszi lehetővé a bizalmas információk megszerzését, továbbá teret nyithat a rendszerekbe történő bejutásnak és az azokban történő károkozásnak. Nagy körültekintést és óvatosságot igényel az e módszerből eredő veszélyek elkerülése, melynek kockázata az alábbi szabályok betartásával csökkenthető:

- a) Ismeretlen, nem megbízható helyről származó, idegen adathordozót (különösen: CD, DVD, pendrive, külső meghajtó) nem javasolt a számítógéphez csatlakoztatni.

- b) Ismeretlen címről érkező, egyetemi viszonylatban nem megszokott tárgyú gyanús e-mailt, és csatolmányait nem szabad megnyitni, mert vírusokkal fertőzhetik meg a számítógépet és a Hálózatot.
- c) Az e-mailekben (még ismerőstől származó levélben is) szereplő linkekre csak nagy körültekintéssel szabad kattintani, mivel rosszindulatú kódokat tartalmazó honlapokra irányíthatja át a felhasználó számítógépet. Léteznek olyan manipulált weboldalak, amelyek internetes címe csak egy-két karakterben tér el a megnyitni szándékozott honlap címétől és megjelenésükben szinte teljes mértékben megegyeznek velük, de károkozási szándékkal, csalók készítették őket.
- d) Az időszakosan nem használt számítógépet minden esetben ki kell kapcsolni vagy jelszó védelemmel zárolni kell azt.
- e) A nyomtatókból a lehető legrövidebb időn belül el kell távolítani a kinyomtatott iratokat, illetve az ezzel a funkcióval rendelkező nyomtatókon lehetőség szerint alkalmazni kell a biztonságos nyomtatás funkciót.

---

### 27. § SAJÁT ESZKÖZÖK HASZNÁLATA (BYOD)

---

- (1) A felhasználók saját tulajdonú elsősorban mobil vagy esetleg más asztali számítástechnikai eszközeinek az Egyetemen történő használatára vonatkozó szabályok:
- a) A saját eszköz egyetemi célokra (munkavégzésre) történő használatát a szervezeti egység vezetőjének javaslatára, indokolt esetben az InI – a megbízható hálózati működéshez és a védelemhez szükséges programok (különösen: vírusirtó program) által történt előzetes ellenőrzés, valamint a nyilvántartásba vétel után – engedélyezheti az alábbi feltételekkel:
- Az InI megvizsgálja, hogy az érintett felhasználó rendelkezik-e a biztonságos számítógép használathoz nélkülözhetetlen ismeretekkel.
  - A saját eszközhöz az InI számára mindenkor hozzáférést kell biztosítani a megbízható hálózati működés és a védelem szükséges feltételeinek ellenőrzése céljából.
  - A saját eszközön az operációs rendszer, biztonsági csomag, irodai rendszerek utolsó biztonsági frissítése kötelezően használandó, ezért aktiválni szükséges ezek automatikus frissítés funkcióját.

- A saját eszközön tárolt egyetemi adatok biztonságáért az eszköz tulajdonosa teljes körű felelősséggel tartozik.
- Saját eszközt a Hálózathoz, internethez csatlakoztatni csak biztonságos körülmények megléte esetén lehet. A vezeték nélküli (WiFi, bluetooth) kapcsolat csak biztonságos körülmények között használható.
- A saját eszközön tárolt adatoknak a Hálózatra történő rendszeres mentésére fokozott figyelmet kell fordítani.

b) Időszakos rendezvényeken (különösen: konferenciákon, gyakorlatokon, stb.) külön engedély nélkül lehet a saját mobil eszközöket használni.

(2) Különös figyelemmel kell lenni a munkatársak saját eszközeinek (BYOD) biztonságos használatára, amellyel nem sérthetők sem a személyes, sem az egyetemi érdekek. Vítás esetekben az egyetemi érdekek elsőbbséget élveznek és a saját eszközök használatát az egyetemi Hálózat biztonságának veszélyeztetése esetén figyelmeztetés nélkül azonnal meg lehet tiltani.

---

## 28. § KÖZÖSSÉGI HÁLÓZATOK HASZNÁLATA

---

(1) Az Egyetem használja az internetes közösségi oldalakat is tevékenységének széleskörű megismertetésére, társadalmi elfogadottságának növelésére, oktatási portfóliójának a továbbtanulás előtt álló középiskolások közötti népszerűsítésére.

(2) A felhasználóknak az Interneten történő megnyilatkozásaik esetében is figyelemmel kell lenniük a személyes és közérdekű adatok védelmére és biztonságára vonatkozó jogszabályokban előírtakra, ugyanis ezek a megnyilatkozások nem csak a kinyilvánítójuk, hanem az Egyetem jó hírnévére is befolyással lehetnek és akár jogi következményekkel is járhatnak.

(4) A felhasználók megnyilatkozásaik során személyes identitásukat nem elfedve kötelesek képviselni a véleményüket, amelyért felelősséggel tartoznak. **Tilos** az Egyetemmel kapcsolatosan az egyetemi polgárokhoz méltatlan vélemények nyilvános közlése.

---

## 29. § SZOFTVERJOGTISZTASÁG, SZOFTVEREK TELEPÍTÉSE, FRISSÍTÉSE

---

(1) Az egyetemi számítógépekre csak az Egyetem által megvásárolt, jogtiszt szoftverek telepíthetők.

- (2) Az egyetemi munkaállomásokon telepített operációs rendszerek, irodai szoftverek frissítése az interneten keresztül automatikusan történik. A frissítési folyamat felhasználói beavatkozást nem igényel.

---

### 30. § A SZÁMÍTÓGÉPES VÍRUSVÉDELEM

---

- (1) A számítógép vírussal vagy más rosszindulatú programmal, történő fertőződése súlyos biztonsági kockázat. Az Egyetem hálózatában az InI által központilag biztosított és felügyelt több szintű vírusvédelmi rendszer működik. Ha ennek ellenére valamilyen számítógép, felhasználói munkaállomás vírussal fertőződik, az InI – a vírusmentesítés és az ellenőrzések idejére, a fertőzés terjedésének megakadályozása érdekében - kizárhatja azt a hálózati forgalomból. A felhasználó ilyen esetben köteles a mielőbbi vírusmentesítés érdekében együttműködni az InI illetékes munkatársaival.
- (2) Több munkaállomás számítógépes vírusfertőzése esetén a vírusmentesítés és az ellenőrzések idejére, a fertőzés terjedésének megakadályozása érdekében az InI jogosult az adott hálózati szegmens izolálására vagy kizárására
- (3) A felhasználóknak be kell tartaniuk a vírusvédelemre vonatkozó elemi szabályokat és az ide vonatkozó egyéb rendelkezéseket.
- (4) A vírusvédelmi rendszer frissítése központilag, felhasználói beavatkozás nélkül történik, amelyet a vírusvédelmi rendszer szervergépe hajt végre. A szerver elérhetlensége esetén a munkaállomások vírusvédelmi rendszerének frissítése az interneten keresztül történik.

---

### 31. § KATASZTRÓFAKEZELÉS, MENTÉS, VISSZAÁLLÍTÁS, A SZOLGÁLTATÁS FOLYTONOSSÁGA

---

Rendkívüli események által okozott károk elkerülésére, enyhítésére, az esetleges bekövetkezésük utáni teendőkről az adott rendszer felelősénél elérhető helyreállítási, mentési tervek állnak rendelkezésre, melyek elkészítése, karbantartása, tárolása az adott rendszer felelősének a feladata.

---

## V. FEJEZET A BERUHÁZÁSI PROGRAMIRODÁRA VONATKOZÓ KÜLÖNÖS SZABÁLYOK

---

---

### 32. § AZ V. FEJEZET HATÁLYA

---

- (1) A BPI esetében az informatikai és kommunikációs Hálózat üzemeltetése e fejezetben foglalt eltérésekkel történik.
- (2) A BPI tevékenységének informatikai támogatása külső szolgáltató által valósul meg.
- (3) Jelen speciális szabályozás hatálya kiterjed a BPI valamennyi foglalkoztatottjára és jelen szabályzat alapján érintett szerződéses partnereire, továbbá a BPI teljes számítástechnikai infrastruktúrájára. Ez magába foglalja a BPI használatában lévő valamennyi számítógépet (szerverek és személyi számítógépek), a perifériákat, a hálózati erőforrásokat és szolgáltatásokat, a szoftvereket, azok üzemeltetését, továbbá a mindezekon kezelt adatokat és információkat.
- (4) A BPI felhasználói által igénybe vehető informatikai és kommunikációs szolgáltatások körét – az InI-t is érintő szolgáltatások esetében – az InI-vel történő előzetes egyeztetés alapján, a BPI illetékes vezetője határozza meg.

---

### 33. § FELADATMEGOSZTÁS AZ INI ÉS BPI KÖZÖTT

---

- (1) A BPI által használt informatikai alapinfrastruktúra:
  - a) A BPI működését biztosító informatikai rendszerek informatikai kiszolgálása és a BPI tevékenységi körébe tartozó informatikai rendszerek üzemeltetése a BPI felelősségi körébe tartozik.
  - b) A BPI által használt ingatlanban az internet kapcsolat, a hálózati, a vezeték nélküli hálózati és a kommunikációs hálózati infrastruktúra kialakítása és üzemeltetése a BPI felelősségi körébe tartozik.
  - c) A BPI IP telefónia (asztali telefonkészülékek) igényeinek ellátása a BPI felelősségi körébe tartozik.
  - d) A BPI használatában lévő, BPI igényei szerint kialakított virtuális hálózati szegmens üzemeltetése, üzembiztosságának fenntartása az InI felelősségi körébe tartozik.

- e) A BPI használatában lévő virtuális hálózati szegmens folyamatos karbantartása, fejlesztése, a lehetőségek mértékében a felmerülő igényekhez igazítása, az új technikai lehetőségek alkalmazhatóságának megteremtése - a BPI-vel előzetesen egyeztetve - az InI felelősségi körébe tartozik.
  - f) A BPI hálózati szegmens üzemzavarának esetében az InI köteles a hibaelhárítást a bejelentést követően haladéktalanul megkezdeni. Munkaszüneti nap esetében az azt követő első munkanap kezdetén köteles az InI a hibaelhárítást megkezdeni.
- (2) Általános szabályok a BPI által használt informatikai eszközökön:
- a) A BPI által használt informatikai eszközök működéséhez szükséges szoftverek telepítése és jogtisztasága a BPI felelősségi körébe tartozik.
  - b) A BPI által használt informatikai eszközök és adatok vírusvédelme a BPI felelősségi körébe tartozik.
  - c) A BPI által használt informatikai eszközök és szoftverek nyilvántartása a BPI felelősségi körébe tartozik.
- (3) A BPI által üzemeltetett informatikai rendszerek:
- a) A BPI rendszerbe állításra tervezett, az egyetemi rendszereket globálisan érintő informatikai és kommunikációs eszközeinek, rendszerek szolgáltatásainak, rendszerbe illeszthetőségének vizsgálata, döntés meghozatala az alkalmazhatóságukról, vagy alkalmazásuk kizárásáról, illetve az elavultak kivonásáról – az InI-vel törőntént előzetes egyeztetés után, és egyetértésével – a BPI felelősségi körébe tartozik.
  - b) A BPI által nyújtott hálózati szolgáltatások körének, az egyes szolgáltatások igénybe vételi feltételeinek meghatározása, a hálózati biztonság érdekében az egyes szolgáltatások használatának felhasználói azonosításhoz kötése, a felhasználók körének szűkítése, korlátozása a BPI felelősségi körébe tartozik.
  - c) Speciális szaktudást igénylő feladatoknál külső informatikai szolgáltató igénybevétele a BPI felelősségi körébe tartozik. Azokban az esetekben, amelyek befolyással lehetnek az InI felelősségi területeire, előzetes InI-BPI egyeztetés szükséges.
- (4) A BPI foglalkoztatottjai, partnerei által használt irodai és munkavégzéshez szükséges informatikai környezet:

- a) A BPI felhasználóinak az elektronikus – a tf.hu domain alatt üzemeltetett - levelezéssel kapcsolatos postafiókok, címek, hozzáférések biztosítása az InI felelősségi körébe tartozik. A BPI felhasználói számára is mérvadóak és követendőek a jelen szabályzatban az elektronikus levelezéssel kapcsolatosan megfogalmazott általános szabályok.
  - b) A BPI saját Microsoft infrastruktúrájának üzemeltetése a BPI felelősségi körébe tartozik.
  - c) A BPI saját Microsoft infrastruktúráját használó (szerver és kliens) számítógépek támogatása a BPI felelősségi körébe tartozik.
  - d) A BPI felhasználók számára központi tárhelyet biztosítása, annak struktúrájának, hozzáféréseinek és jogosultsági szintjeinek beállítása a BPI felelősségi körébe tartozik.
  - e) A BPI felelősségi körébe tartozó informatikai és hálózati erőforrások jogosultságainak szabályozása a BPI felelősségi körébe tartozik.
  - f) A BPI felhasználók személyi számítógépeinek (asztali és hordozható gépek egyaránt) felkészítése, a napi munkához szükséges programok, programrendszerek telepítése és konfigurálása a BPI felelősségi körébe tartozik. Az olyan esetekben, amelyek befolyásolhatják az InI feladatkörét, előzetes InI-BPI megállapodás szükséges.
  - g) A BPI felhasználók számítógépein a helyi rendszergazdai jogosultságokról való döntés a BPI felelősségi körébe tartozik.
  - h) A BPI felhasználók saját tulajdonú, vagy más szervezet tulajdonát képező számítógépek Hálózatra kapcsolásnak engedélyezése – szükség esetén az InI-vel történő előzetes egyeztetés után – a BPI felelősségi körébe tartozik.
  - i) A BPI felhasználók számára a távoli munkavégzéshez (VPN kapcsolat) használt erőforrások biztosítása az InI felelősségi körébe tartozik.
- (5) A BPI által használt informatikai eszközök:
- a) A BPI használatában, kezelésében lévő informatikai eszközök beszerzése a Műszaki és Ellátási Igazgatóság feladatkörébe tartozik.

- b) A BPI a kiszolgáló szervereit az elhelyezésére szolgáló bérelt ingatlan szervertermében helyezi el és az őrzéséről saját maga gondoskodik. A szerverek biztonságos üzemeltetéséhez szükséges feltételeket a BPI biztosítja.
- (6) Szankciók alkalmazása a biztonsági előírásokat megsértő BPI felhasználókkal szemben és a szankciókkal sújtott felhasználók haladéktalan tájékoztatása a BPI felelősségi körébe tartozik. A foganatosított szankciókról, és a szankciókkal sújtott személyekről a BPI haladéktalanul köteles írásban vagy e-mailben tájékoztatni az InI-t.

---

### 34. § BPI FELHASZNÁLÓK KÖTELESSÉGEI

---

A BPI felhasználók kötelességei vonatkozásában a jelen szabályzatban megfogalmazott általános szabályok az irányadók, azzal a kivétellel, hogy a BPI felhasználói az informatikai eszközök és Hálózat használata folyamán tapasztalt bármiféle meghibásodás, rendellenesség, a vonatkozó biztonsági szabályzatokban megfogalmazottak megsértése esetén elsőként a BPI informatikusait kell, hogy értesítsék. Az Egyetem informatikai és kommunikációs Hálózatával kapcsolatos hibaelhárítás folyamán a BPI-nek az InI-vel együtt kell működnie.

---

## VI. FEJEZET A GYAKORLÓ ISKOLÁRA VONATKOZÓ KÜLÖNÖS SZABÁLYOK

---

---

### 35. § A VI. FEJEZET HATÁLYA

---

- (1) A Gyakorló iskola esetében az informatikai és kommunikációs Hálózat üzemeltetése az e fejezetben foglalt eltérésekkel történik.
- (2) A speciális szabályok célja e tevékenységekhez tartozó feladatok, folyamatok meghatározása.
- (3) Jelen speciális szabályozás hatálya kiterjed a Gyakorló Iskola valamennyi szervezeti egységére, foglalkoztatottjára, az általa üzemeltetett belső támogató rendszerek felhasználóira, továbbá a Gyakorló Iskola teljes számítástechnikai infrastruktúrájára. Ez magába foglalja a Gyakorló Iskola használatában lévő valamennyi számítógépet (szerverek és személyi számítógépek), a perifériákat, a hálózati erőforrásokat és szolgáltatásokat, a szoftvereket, azok üzemeltetését, továbbá a mindezekben kezelt adatokat és információkat.



- (4) A Gyakorló Iskola hálózata által nyújtott, a Gyakorló Iskola felhasználói által igénybe vehető informatikai és kommunikációs szolgáltatások körét az InI-t is érintő szolgáltatások esetében az InI-vel történő előzetes egyeztetés alapján a Gyakorló Iskola igazgatója határozza meg.

---

### 36. § FELADATMEGOSZTÁS AZ INI ÉS GYAKORLÓ ISKOLA KÖZÖTT

---

- (1) A Gyakorló Iskola által használt informatikai alpinfrastruktúra:
- a) A Gyakorló Iskola működését biztosító informatikai rendszerek informatikai kiszolgálása és a Gyakorló Iskola tevékenységi körébe tartozó informatikai rendszerek üzemeltetése a Gyakorló Iskola felelősségi körébe tartozik.
  - b) Az egyetemi campusokon az internet kapcsolat kialakítása az TE által igénybevett szolgáltatón keresztül történik, a kapcsolattartás és meghibásodások kezelése az InI felelősségi körébe tartozik. Az egyetemi campusokon a hálózati, a vezeték nélküli hálózati és a kommunikációs hálózati infrastruktúra kialakítása az InI felelősségi körébe tartozik.
  - c) A Gyakorló Iskola használatában lévő, Gyakorló Iskola igényei szerint kialakított virtuális hálózati szegmens üzemeltetése, üzembiztosságának fenntartása az InI felelősségi körébe tartozik.
  - d) A Gyakorló Iskola használatában lévő virtuális hálózati szegmens folyamatos karbantartása, fejlesztése, a lehetőségek mértékében a felmerülő igényekhez igazítása, az új technikai lehetőségek alkalmazhatóságának megteremtése - a Gyakorló Iskolával előzetesen egyeztetve - az InI felelősségi körébe tartozik.
  - e) A Gyakorló Iskola hálózati szegmens üzemzavarának esetében az InI köteles a hibaelhárítást a bejelentést követően haladéktalanul megkezdeni. Munkaszüneti nap esetében az azt követő első munkanap kezdetén köteles az InI a hibaelhárítást megkezdeni.
- (2) Általános szabályok a Gyakorló Iskola informatikai eszközeinek használatára vonatkozóan:
- a) A Gyakorló Iskola által használt informatikai eszközök működéséhez szükséges szoftverek telepítése és jogtisztasága a Gyakorló Iskola felelősségi körébe tartozik.

- b) A Gyakorló Iskola által használt informatikai eszközök és adatok vírusvédelme a Gyakorló Iskola felelősségi körébe tartozik.
  - c) A Gyakorló Iskola által használt informatikai eszközök és szoftverek nyilvántartása a Gyakorló Iskola felelősségi körébe tartozik.
- (3) A Gyakorló Iskola által üzemeltetett informatikai rendszerek:
- a) A Gyakorló Iskola rendszerbe állításra tervezett, az egyetemi rendszereket globálisan érintő informatikai és kommunikációs eszközeinek, rendszerek szolgáltatásainak, rendszerbe illeszthetőségének vizsgálata, döntés meghozatala az alkalmazhatóságukról, vagy alkalmazásuk kizárásáról – az InI-vel történt előzetes egyeztetés után – a Gyakorló Iskola felelősségi körébe tartozik.
  - b) A Gyakorló Iskola által nyújtott hálózati szolgáltatások körének, az egyes szolgáltatások igénybe vételi feltételeinek meghatározása, a hálózati biztonság érdekében az egyes szolgáltatások használatának felhasználói azonosításhoz kötése, a felhasználók körének szűkítése, korlátozása a Gyakorló Iskola felelősségi körébe tartozik.
  - c) Speciális szaktudást igénylő feladatoknál külső informatikai szolgáltató igénybevétele a Gyakorló Iskola felelősségi körébe tartozik. Azokban az esetekben, amelyek befolyással lehetnek az InI felelősségi területeire, előzetes InI - Gyakorló Iskola egyeztetés szükséges.
- (4) A Gyakorló Iskola felhasználói által használt, munkavégzéshez szükséges informatikai környezet:
- a) A Gyakorló Iskola felhasználóinak az elektronikus – a tfgyakorlo.hu domain alatt üzemeltetett - levelezéssel kapcsolatos postafiókok, címek, hozzáférések biztosítása az InI felelősségi körébe tartozik. A Gyakorló Iskola felhasználói számára is mérvadók és követendőek a jelen szabályzatban az internet használatával és elektronikus levelezéssel kapcsolatosan meghatározott általános szabályok.
  - b) A Gyakorló Iskola saját Microsoft infrastruktúrájának üzemeltetése a Gyakorló Iskola felelősségi körébe tartozik.
  - c) A Gyakorló Iskola saját Microsoft infrastruktúráját használó (szerver és kliens) számítógépek támogatása a Gyakorló Iskola felelősségi körébe tartozik.

- d) A Gyakorló Iskola felhasználói, illetve honlapja számára központi tárhely biztosítása, annak struktúrájának, hozzáféréseinek és jogosultsági szintjeinek beállítása a Gyakorló Iskola felelősségi körébe tartozik.
  - e) A Gyakorló Iskola felelősségi körébe tartozó informatikai és hálózati erőforrások jogosultságainak szabályozása a Gyakorló Iskola felelősségi körébe tartozik. Az Egyetem informatikai Hálózatán való jogosultságok tekintetében - a Gyakorló Iskola felhasználók esetében is - a jelen szabályzatban rögzített általános szabályok az irányadók.
  - f) A Gyakorló Iskola felhasználók személyi számítógépeinek (asztali és hordozható gépek egyaránt) felkészítése, a napi munkához szükséges programok, programrendszerek telepítése és konfigurálása a Gyakorló Iskola felelősségi körébe tartozik. Az InI feladatkörét érintő esetekben előzetes egyeztetés szükséges a Gyakorló Iskola és az InI között.
  - g) A Gyakorló Iskola felhasználók számítógépein a helyi rendszergazdai jogosultságokról való döntés a Gyakorló Iskola felelősségi körébe tartozik.
  - h) A Gyakorló Iskola felhasználók saját tulajdonú informatikai eszközei hálózatra kapcsolásának engedélyezése – szükség esetén az InI-vel történő előzetes egyeztetés után, és egyeztetésével – a Gyakorló Iskola felelősségi körébe tartozik.
  - i) A Gyakorló Iskola felhasználók számára a távoli munkavégzéshez (VPN kapcsolat) használt erőforrások biztosítása az InI felelősségi körébe tartozik.
- (5) A Gyakorló Iskola által használt informatikai eszközök:
- a) A Gyakorló Iskola használatában, kezelésében lévő informatikai eszközök beszerzése a Műszaki és Ellátási Igazgatóság felelősségi körébe tartozik.
  - b) A Gyakorló Iskola a belső igényeinek, tevékenységi körébe tartozó feladatainak kiszolgáló szervereit az egyetem Diana utcai telephelyének szervertermében helyezi el, az őrzését a Gyakorló Iskola végzi, a szerverek biztonságos üzemeltetéséhez szükséges feltételeket a Gyakorló Iskola biztosítja. A szerverpark üzemeltetése a Gyakorló Iskola felelősségi körébe tartozik.
- (6) Szankciók alkalmazása a biztonsági előírásokat megsértő Gyakorló Iskola felhasználókkal szemben és a szankciókkal sújtott felhasználók haladéktalan tájékoztatása a

Gyakorló Iskola felelősségi körébe tartozik. A foganatosított szankciókról, és a szankciókkal sújtott személyekről a Gyakorló Iskola illetékes vezetője haladéktalanul köteles írásban vagy e-mailben tájékoztatni az InI-t.

---

### 37. § GYAKORLÓ ISKOLA FELHASZNÁLÓINAK KÖTELESSÉGEI

---

A Gyakorló Iskola felhasználók kötelességei vonatkozásában a jelen szabályzatban megfogalmazottak a követendők, azzal a kivétellel, hogy a Gyakorló Iskola felhasználói az informatikai eszközök és Hálózat használata folyamán tapasztalt bármiféle meghibásodás, rendellenesség, a vonatkozó biztonsági szabályzatokban megfogalmazottak megsértése esetén elsőként a Gyakorló Iskola informatikusát kell, hogy értesítsék. A Hálózattal kapcsolatos hibaelhárítás folyamán az InI-vel együtt kell működni.

---

## VII. FEJEZET KOCKÁZATKEZELÉS

---

---

### 38. § KOCKÁZATMENEDZSMENT

---

- (1) Annak érdekében, hogy az Egyetemnél az informatikai biztonság érvényesítése során a kockázatarányos védelem elve érvényesüljön az informatikai biztonsági kérdésekkel kapcsolatosan folyamatosan alkalmazni kell a kockázatkezelési szabályokat.
- (2) A kockázatmenedzsment célja, hogy az információk bizalmasságát, sértetlenségét, valamint rendelkezésre állását veszélyeztető kockázati tényezők azonosításával, a kockázatok csökkentésével biztosítsa az informatikai biztonság növelését, szinten tartását.
- (3) A teljes körű kockázatfelmérést jelentős változás esetén (technológia, ill. szolgáltatás be-, illetve kivezetése), de legalább két évente kell végrehajtani az informatikai rendszer minden elemére vonatkozóan.
- (4) A felmerült kockázatok kezelésére (csökkentésére) akcióterveket kell készíteni, melyeknek a feltárt kockázatok függvényében az alábbiakat kell tartalmazniuk:
  - a) javaslatokat a technikai eszközök megváltoztatására, vagy fejlesztésére (pl.: új védelmi eszközök alkalmazása, vagy a jelenlegi átkonfigurálása);
  - b) javaslatokat az érvényben lévő szabályozás megváltoztatására;
  - c) javaslatokat a személyi állományra vonatkozóan;

- d) a kockázatok tudatos felvállalását, ha a védelmi intézkedés közvetlen és közvetett anyagi vonzata nagyobb vagy közel azonos, mint a fenyegetettség által elszenvedhető közvetlen és közvetett anyagi kár.

---

## VIII. FEJEZET VEGYES ÉS ZÁRÓ RENDELKEZÉSEK

---

---

### 39. § VEGYES ÉS ZÁRÓ RENDELKEZÉSEK

---

- (1) Az InI vezetője évente egyszer (szeptember 1-ig bezárólag) köteles a szabályzatot áttekinteni és amennyiben szükséges, akkor annak módosítását kezdeményezni. Az egyes szervezeti egységek vezetői kötelesek gondoskodni arról, hogy minden informatikai és kommunikációs szolgáltatást nyújtó és igénybe vevő szervezeti egység és alkalmazott megismerje a jelen szabályzatot.
- (2) Az IBSZ összhangban áll a vonatkozó hatályos jogszabályokkal. A IBSZ-ben nem szabályozott kérdésekben a vonatkozó hatályos jogszabályok az irányadók.
- (3) Az IBSZ-ben foglaltak megsértése esetén az IBSZ nem ismerete nem mentesít a jogkövetkezmények alól.
- (4) Jelen szabályzatot a Szenátus 74/2017. (X. 19.) számú határozatával fogadta el. Az IBSZ az elfogadását követő napon lép hatályba.

Budapest, 2017. október 19.

Prof. Dr. h. c. Mocsai Lajos s.k.  
rektor

Egyetértek:

Dr. Genzwein Ferenc s.k.  
kancellár