

Hatály: 2013. VI. 6 – 2013. VII. 25.



Nemzeti Közzolgálati Egyetem

Informatikai és kommunikációs hálózat használatának és üzemeltetésének szabályai

2013.

Tartalom

I. FEJEZET	3
ÁLTALÁNOS RENDELKEZÉSEK	3
A Szabályzat célja	3
A Szabályzat hatálya	3
Értelmező rendelkezések	4
II. FEJEZET	6
A HÁLÓZAT HASZNÁLATA	6
A hálózat használatának alapvető szabályai.....	6
Szolgáltatások a hálózaton	6
Az ISZK kötelezettségei.....	7
Az ISZK jogai	8
A felhasználók jogai.....	8
A felhasználók kötelességei	8
A meg nem engedett tevékenységek szankciói	9
A hálózat felépítése	9
A hálózat üzemeltetése, építése, bővítése	10
A hálózati hardver használatának szabályai	10
A hálózati hibák elhárítása	11
III. FEJEZET	11
A HÁLÓZAT SZOFTVERÜZEMELTETÉSE	11
Támogatott protokollok.....	11
Kritikus adatokat tartalmazó számítógépek használata.....	11
Személyi számítógépek felkészítése a használatra.....	12
Szerverek üzemeltetése	12
A rendszergazdák feladatai	12
Tanszékek és szervezetek informatikai felelőseinek feladatai	13
Távoli munkavégzés.....	13
Adatok elhelyezésének szabályai a belső hálózaton	13
Adatok, információk elhelyezésének szabályai az Egyetem WEB szerverén.....	14
Domain nevek használatának szabályai	15
IV. FEJEZET	15
JOGOSULTSÁGOK ÉS INFORMATIKAI BIZTONSÁG	15
Jogosultságok az Egyetem informatikai hálózatán	15
A jelszavak használatának szabályai	16
Elektronikus levelezés használata az Egyetem hálózatán	17
Szoftverjogtisztaság, szoftverek telepítése, frissítése.....	18
A számítógépes vírusvédelem az Egyetem informatikai hálózatában	18
Katasztrófakezelés, mentés, visszaállítás, szolgáltatásfolytonosság	19
V. FEJEZET	20
ZÁRÓ RENDELKEZÉSEK	20

I. FEJEZET

ÁLTALÁNOS RENDELKEZÉSEK

A Szabályzat célja

1. §

- (1) A Nemzeti Közszerológati Egyetem (a továbbiakban: Egyetem) informatikai és kommunikációs hálózata használatának és üzemeltetésének szabályai (a továbbiakban : Szabályzat) alapvető célja, hogy az elérhető szolgáltatások használata, alkalmazása során biztosítsa az adatvédelem alkotmányos elveinek, az adatbiztonság követelményeinek érvényesülését, s megakadályozza a jogosulatlan hozzáférést, az adatok megváltoztatását és jogosulatlan nyilvánosságra hozatalát. A Szabályzat elő kell, hogy mozdítsa az informatikai és kommunikációs eszközök előírásoknak megfelelő és biztonságos használatát, ezzel támogatva, hogy az Egyetem által kezelt információvagyton sértetlensége, bizalmassága és rendelkezésre állása biztosított legyen.
- (2) Az Egyetem Informatikai Szerológátató Központja (a továbbiakban: ISZK) az Egyetem összes telephelyére kiterjedő informatikai és kommunikációs hálózatot (a továbbiakban: hálózat) 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, illetve a felhasználók között az információáramlás biztosítása, valamint egyéb hálózati szolgáltatások nyújtása a felhasználók számára. A hálózat által nyújtott, a felhasználók által igénybe vehető szolgáltatások körét az ISZK igazgatójával történő egyeztetés alapján az Egyetem főtitkára határozza meg.
- (4) Napjainkban az informatikai és a kommunikációs technológia konvergenciája látványos (különösen: azonos eszközök, berendezések, szabványok, vagy okos telefonok, tabletek, mobil számítástechnikai eszközök használata). A jelen Szabályzat mindkét szakterületre egyaránt érvényes, speciális szabály az adott szakterületre vonatkozó résznél kerül megfogalmazásra.

A Szabályzat hatálya

2. §

Jelen 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, akik oktatási, kutatási, tudományos, adminisztrációs és egyéb feladataikhoz állandó vagy eseti jelleggel vagy szerződés alapján az Egyetem hálózatát használják. Az egyetemi hálózat vonatkozásában az oktatók, a rendszergazdák, a hallgatók, és a felhasználók más csoportjai különböző jogosultságokkal és kötelezettségekkel rendelkezhetnek.

Értelmező rendelkezések

3. §

1. **Adatbiztonság:** Az adatok jogosulatlan megszerzése, módosítása és tönkretétele elleni műszaki és szervezési intézkedések és eljárások együttes rendszere.
2. **Adatfelelős:** Az a közfeladatot ellátó szerv, amely az elektronikus úton kötelezően közzeendő közérdekű adatot előállította, illetve amelynek a működése során ez az adat keletkezett.
3. **Adatgazda:** Felelős az általa kezelt adatokért, továbbá jogosult minősítés vagy osztályba sorolás elvégzésére.
4. **Aktív hálózati eszköz:** Kapcsolók (switch-ek), forgalomirányítók (router-ek), vezeték nélküli hozzáférési pontok (Acces Pointok) és egyéb eszközök, amelyek segítségével a hálózat üzemvitele biztosítható (bridge-ek, tűzfalak).
5. **Asztali munkaállomás:** A felhasználó rendelkezésére bocsátott számítástechnikai eszköz, mely alapvetően a számítógépből, monitorból, billentyűzetből és egérből áll.
6. **Bizalmasság:** Az információ azon jellemzője, hogy csak egy előre meghatározott felhasználói kör (jogosultak) részére hozzáférhető, mindenki más számára titok. A bizalmasság elvesztését felfedésnek nevezzük, mely esetén a bizalmas információ arra jogosulatlanok számára is ismertté, hozzáférhetővé válik.
7. **Biztonság:** Az informatikai rendszerekben olyan előírások és szabványok betartását jelenti, amelyek a rendszer működőképességét, az információk rendelkezésre állását, sértetlenségét, bizalmasságát és hitelességét erősítik.
8. **Csomópont:** Szerver feladatokat ellátó eszközök és aktív eszközök csoportja az informatikai szolgáltatások ellátására.
9. **Domain név:** Tartománynév (műszaki azonosító), amelyet elsősorban a könnyebb megjegyezhetősége miatt, az internetes kommunikációhoz nélkülözhetetlen Internet cím tartományok (IP címek) helyett használnak. Az Internet egy meghatározott részét, tartományát egyedileg leíró megnevezés, a számítógépek (kiszolgálók) azonosítására szolgáló névtartomány (uni-nke.hu).
10. **DNS:** Az internet neveket és címeket egymáshoz rendelő adatbázis, amely általában külön kiszolgáló gépen fut.
11. **Felhasználó:** Az a természetes személy, aki az egyetemi informatikai infrastruktúrát használja.
12. **Felhasználói azonosító:** Az intézményi címtárban tárolt egyedi azonosításra szolgáló rövid karaktersorozat, amely általában a felhasználó nevéből képződik.
13. **Hálózat:** Felhasználói számítógépek és/vagy szerverek közötti adatátvitelt biztosító passzív és aktív eszközökből álló infrastruktúra.
14. **Hálózati rendszergazda:** Az ISZK állományából kijelölt, az egyes kampuszokon, a teljes Egyetem vagy egy-egy kampusz számára szolgáltató szerverek, valamint a hálózati hardverrendszer hardver és szoftver üzemeltetői.
15. **Hitelesség:** Az információ akkor hiteles, ha az elvárt, hozzáértő, megbízható forrásból származik.
16. **Informatikai erőforrások:** A hardver, szoftver eszközök összessége.
17. **Internet:** A világháló.
18. **Intranet:** Az intézményen belüli hálózat és annak szolgáltatásai.

19. **IP telefónia:** Olyan számítógép-hálózati alkalmazás, amely dedikált eszközök (készülék és központ) segítségével telefonszolgáltatást tesz lehetővé, ez a hagyományos telefonközpontokat felváltó számítógépes rendszer.
20. **Központi címtár:** Az Egyetem dolgozóinak felhasználói adatait tároló LDAP adatbázis.
21. **Központi szolgáltatások:** Levelezés, címtár, fájl kiszolgálás, Web szolgáltatás, névszolgáltatás, és más informatikai és kommunikációs szolgáltatások.
22. **LDAP (Light Weight Directory Access Protocol):** Nyílt szabványú címtár struktúra leíró nyelv.
23. **Mobil eszközök:** Notebook, netbook, tablet, palmtop, okostelefon.
24. **NEPTUN kód:** A rendszer használatához szükséges betűkből és számokból álló legalább 6 karakter hosszúságú kód.
25. **NIFI (Nemzeti Információs Infrastruktúra Fejlesztési Intézet):** Az iroda a teljes magyarországi kutatási, felsőoktatási és közgyűjteményi közösség számára biztosít integrált országos számítógép-hálózati infrastruktúrát, valamint erre épülő kommunikációs, információs és kooperációs szolgáltatásokat, élvonalbeli alkalmazási környezetet, és tartalom-generálási illetve tartalom-elérési hátteret.
26. **Okostelefon:** Internetezésre és/vagy dokumentumkezelésre is használható mobil telefon.
27. **Passzív eszközök:** Hálózati kábelezés és csatlakozók.
28. **Rendelkezésre állás:** Annak biztosítása, hogy a szükséges információ a szükséges időben az arra jogosultak számára meghatározott formában hozzáférhető, elérhető legyen.
29. **Sértetlenség:** Az információ létének, hitelességének, épségének, önmagában teljességének kritériuma.
30. **Számítógép:** Olyan informatikai eszköz, amelyet a felhasználó a napi munkája során használ, és amellyel igénybe veheti a hálózat szolgáltatásait.
31. **Szerver-feladatokat ellátó eszköz:** Olyan számítógépek, szoftverek, vagy speciális eszközök, amelyek különböző szolgáltatásokat biztosítanak más számítógépek számára.
32. **Szerverhelyiség:** Fokozottan védett, naplózott bejutású, klimatizált, zárt helyiség, ahol a folyamatos működés feltételei az informatikai erőforrások számára biztosítottak.
33. **Szervezeti rendszergazda:** Az egyes egyetemi szervezetek felügyeletében lévő, az ISZK igazgató engedélyével működő, hálózati szolgáltatást nyújtó számítógép adminisztrátora.
34. **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.
35. **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.
36. **VPN szolgáltatás:** Speciális hálózati elérés, amely az Egyetem hálózatához titkosított, és hitelesített kapcsolatot tesz lehetővé a világ bármely részéről.
37. **WEB adminisztrátor:** Az Egyetem WEB szerverét működtető, az Egyetem honlapjának felügyeletét ellátó személyek. A WEB-es adat- és tartalomszolgáltatást az Egyetem szerveiből kijelölt felelősök végzik.
38. **WiFi, WLAN:** Szabványos vezeték nélküli adatátviteli technika. A szabad frekvenciatartományt használó rendszer átviteli sebessége nagymértékben függ a rádióhullámok terjedési környezetétől (akadályok, távolság). A legtöbb notebook, laptop, palmtop számítógép gyárilag rendelkezik ilyen kapcsolódási lehetőséggel.

II. FEJEZET

A HÁLÓZAT HASZNÁLATA

A hálózat használatának alapvető szabályai

4. §

Az Egyetem hálózatát csak Magyarország hatályos jogszabályaiban és a vonatkozó szabályozókban foglaltak szerint lehet használni. A hálózat - összhangban NIIFI Felhasználói Szabályzatával - nem használható különös tekintettel az alábbi tevékenységekre :

- a) a mindenkor hatályos magyar jogszabályokba ütköző cselekmények előkészítése vagy végrehajtása, így különösen mások személyiségi jogainak megsértése (különösen: rágalmozás), tiltott haszonszerzésre irányuló tevékenység (különösen: piramisjáték), szerzői jogok megsértése (különösen: szoftver nem jogszerű tárolása, terjesztése);
- b) profitszerzést célzó, direkt üzleti célú tevékenység és reklám;
- c) a hálózat, a kapcsolódó hálózatok, illetve ezek erőforrásainak rendeltetésszerű működését és biztonságát megzavaró, veszélyeztető tevékenység, ilyen információknak és programoknak a terjesztése;
- d) a hálózatot, a kapcsolódó hálózatokat, illetve erőforrásaikat indokolatlanul, túlzott mértékben, pazarló módon igénybevevő tevékenység (különösen: levélbombák, hálózati játékok, kéretlen reklámok);
- e) a hálózat erőforrásaihoz, a hálózaton elérhető adatokhoz történő illetéktelen hozzáférés, azok illetéktelen használata, gépek/szolgáltatások - akár tesztelés céljából történő - illetéktelen szisztematikus próbálgatása (különösen: TCP port scan);
- f) a hálózat erőforrásainak, a hálózaton elérhető adatoknak illetéktelen módosítására, megromlására, megsemmisítésére vagy bármely károkozásra irányuló tevékenység;
- g) másokra nézve sértő, vallási, etnikai, politikai vagy más jellegű érzékenységet bántó, zaklató tevékenység (különösen: pornográf vagy pedofil anyagok közzététele);
- h) hálózati üzenetek, hálózati eszközök hamisítása: olyan látszat keltése, mintha egy üzenet más gépről vagy más felhasználótól származna (spoofing).

Szolgáltatások a hálózaton

5. §

Az ISZK jelenleg az alábbi szolgáltatásokat nyújtja a hálózaton¹:

- a) Vezetékes és vezeték nélküli internet hozzáférés;
- b) Analóg, Digitális és IP telefon szolgáltatás;
- c) Elektronikus levelezés (belső hálózati és távoli hozzáféréssel);
- d) Az egyetem on-line megjelenését biztosító web szerverek üzemeltetése;
- e) Tanulmányi információs rendszer (NEPTUN) elérhetőségének biztosítása;
- f) Gazdálkodási rendszer (Forrás SQL) adminisztrációja
- g) Távközponti rendszerek (ILIAS, MOODLE) üzemeltetése;
- h) Elektronikus iktatórendszer;
- i) Jelszavas hozzáférés szabályozáson alapuló, védett adattároló területek biztosítása a közös munkavégzéshez a központi szervereken;
- j) Központi nyomtatás kezelő rendszer (SAFEQ) üzemeltetése;
- k) Biztonságos távoli munkavégzéshez VPN kapcsolat biztosítása;
- l) Központi vírusvédelmi és spamszűrő rendszer üzemeltetése;

¹ Az ISZK az egyetemen nem minden esetben és nem minden helyszínen nyújtja – az 5. § (1) bekezdésben felsoroltak közül – az összes szolgáltatást teljes körűen.

- m) Belső adminisztratív rendszerek (Szenátusi anyagok kezelése, Óratartás, Felhasználói ügybejelentő, Rendezvény nyilvántartó, Nyomdai szolgáltatás igénylő, Kollégiumi elhelyezés igénylő);
- n) Complex jogtár;
- o) SPSS statisztikai programcsomag;

Az ISZK kötelezettségei

6. §

A biztonságos hálózati szolgáltatások nyújtása érdekében az ISZK kötelezettségei:

- a) Az oktatás, kutatás, tudományos munka, valamint az Egyetem működését biztosító egyéb rendszerek informatikai kiszolgálása, a belső hálózati szolgáltatásokat, valamint az Egyetem internetes megjelenését, kapcsolattartását biztosító rendszerek folyamatos üzemeltetése.
- b) A hálózat üzembiztosságának fenntartása, a hatályos szabályozók, korlátozások betartásával elhelyezett adatok védelme.
- c) A hálózat folyamatos karbantartása, fejlesztése, a lehetőségek mértékében a felmerülő igényekhez igazítása, az új technikai lehetőségek alkalmazhatóságának megteremtése.
- d) A rendszerbe állításra tervezett új informatikai és kommunikációs eszközök, rendszerek szolgáltatásainak, rendszerbe illeszthetőségének vizsgálata, döntés meghozatala az alkalmazhatóságukról, vagy alkalmazásuk kizárásáról, illetve az elavultak kivonásáról.
- e) A felhasználók részéről felmerült, az alapvető irodai informatikai és kommunikációs eszközökön és rendszereken túli igények elbírálása, a jogos igények lehetőség szerinti kielégítése, az adott szakterület vezetőjével egyeztetve javaslat tétele az adott feladat ellátására alkalmas más eszköz, rendszer használatára.
- f) A felhasználók személyi számítógépeinek (asztali és hordozható gépek) felkészítése, a napi munkához szükséges programok, programrendszerek telepítése és konfigurálása, működési zavar, meghibásodás, rendellenes működés esetén a hibaelhárítás lehető leggyorsabb, de maximum 2 munkanapon belül történő megkezdése.
- g) Szankciók alkalmazása a biztonsági előírásokat megsértő felhasználókkal szemben és a szankciókkal sújtott felhasználók haladéktalan tájékoztatása. Az alkalmazott szankciókról tájékoztatni kell a munkahelyi vezetőt, akinek azt jóvá kell hagynia. Tekintettel arra, hogy a szabályok megszegése az egész intézmény informatikai rendszerének, s így mások munkájának biztonságát is veszélyeztetheti, ezért az ISZK indokolt esetben azonnali kitiltást is alkalmazhat. A szankciók alkalmazása ellen a hallgató a tanszékvezetőnél, a dolgozó 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. 30 nap után a levelező rendszer a naplókat automatikusan törli.
- i) A kommunikációs rendszerek viszonylatában a jogszabályokban meghatározott nyilvántartások, naplók vezetése, amelyeket a jogszabályokban meghatározott esetekben, törvényes megkeresés alapján az illetékes hatóságoknak kiszolgáltat.
- j) A hálózat működéséhez, karbantartásához időközönként szükséges, előre tervezhető üzemszünetek, leállások 2 nappal a tervezett időpont előtt az Egyetem honlapján, és az esedékesség előtt min. 1 órával belső hálózati üzenet formájában történő bejelentése.
- k) A hálózati szolgáltatások használatához szükséges alapismertetek nyújtása.

Az ISZK jogai

7. §

Az ISZK jogosult:

- a) A hálózat által nyújtott szolgáltatások körének, az egyes szolgáltatások igénybe vételi feltételeinek meghatározására. A hálózati biztonság érdekében az egyes szolgáltatások használatát felhasználói azonosításhoz (autentikációhoz) 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 és intézkedés a zavar, illetve veszélyhelyzet megszüntetésére.

A felhasználók jogai

8. §

A hálózat használata folyamán a felhasználó jogosult:

- a) A munkavégzéshez szükséges programokkal ellátott, egy vagy több személy használatára beállított, felkészített számítógép(ek), kommunikációs eszközök használatára.
- b) A munkavégzéshez szükséges mértékben – a használatra vonatkozó, aláírással elfogadott 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 szakterület vezetőjével együttműködve az ISZK bírálja el).
- e) Levelező szolgáltatás és saját elektronikus postafiók használatára. Az ISZK a felhasználói fiókot az Egyetem rendszerén belül, illetve WEB felületen előretelepített kliens programmal teszi elérhetővé.
- f) A hálózat üzemeltetői részéről a személyhez fűződő jogainak tiszteletben tartására, amelytől eltérni csak törvény 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 fogánosított szankciókról.
- i) A felhasználókra vonatkozó szabályok megismerésére.

A felhasználók kötelességei

9. §

A hálózat biztonságos használata érdekében a felhasználó köteles:

- a) A Szabályzatot megismerni, az abban foglaltakat betartani, valamint együttműködni a hálózat üzemeltetőivel a benne foglaltak betartatása érdekében.
- b) Az egyetemi hálózatot annak céljaival megegyezően használni.
- c) tevékenységével nem zavarni, nem akadályozni, nem veszélyeztetni az egyetemi hálózaton feladataikat végzők tevékenységét.
- d) A hálózati szolgáltatások igénybevételéhez használatos jelszavait titkosan kezelni, előírt gyakorisággal változtatni, a Szabályzat jelszóhasználattal kapcsolatos előírásait

betartani (Tilos a hozzáférési jogosultságok, jelszavak kölcsönadása, átruházása, mások jelszavának elkérése, a hálózat, a levelező szolgáltatás - a tulajdonos felhatalmazása nélkül - más nevében történő igénybevétele.).

- e) Gondoskodni adatainak tőle elvárható védelméről és helyi mentéséről.
- f) Felelősséget vállalni az általa vagy a neki felróható módon (különösen a belépési jogosultság nem megfelelő kezelésével) a felhasználói azonosítójával elkövetett szabályellenes cselekményért.
- g) Az általa vagy neki felróható módon a nevében okozott kárt, az esetleges működési zavar, adatvesztés utáni (különösen: a jelszó kölcsönadása vagy nem biztonságos kezelése, informatikai eszköz szándékos vagy gondatlan rongálása) helyreállítás költségeit megtéríteni.
- h) Az Egyetem hálózatán csak a számára engedélyezett erőforrásokat használni.
- i) A számára biztosított hardver és szoftver környezetet (beleértve a számítógépes vírusellenőrzéssel és vírusirtással kapcsolatos szoftvereket is), kommunikációs eszközöket megőrizni (a biztosított eszközöket, berendezéseket nem bonthatja meg, a hálózati beállításokban a működést befolyásoló módosítást nem végezhet).
- j) A hálózati szolgáltatások, a távfelügyeleti rendszerek működéséhez szükséges segédprogramok telepítését lehetővé tenni.
- k) Haladéktalanul tájékoztatni az ISZK-t és az adott szervezeti egység vezetőjét, amennyiben tudomására jut, hogy bárki megsértette a Szabályzatban foglaltakat.
- l) A hibaelhárítás folyamán az ISZK szakembereivel együttműködni, számukra a szükséges információkat megadni.
- m) USB memóriakulcsok vagy más külső adathordozók csatlakoztatása után az ISZK által biztosított számítógépes vírusellenőrző eszközökkel a vírusellenőrzést, vírusirtást végrehajtani, amelyhez (szükség esetén) az ISZK szakemberei segítséget nyújtanak.

A meg nem engedett tevékenységek szankciói

10. §

A Szabályzat megsértésének gyanúja esetén a cselekményt ki kell vizsgálni, és a vizsgálatra kijelölt legalább három tagú felelős (kivizsgáló) bizottságnak 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.
- d) A szándékos elkövető – a fentieken túl, amennyiben kimutatható anyagi kár is keletkezett - köteles megtéríteni az általa okozott károkat a vonatkozó jogszabályok és belső szabályzatok előírásai szerint
- e) Ha az elkövetett cselekmény kimeríti a Btk. valamely törvényi tényállását, akkor a vizsgálatért felelős személy köteles az elkövető felelősségre vonását kezdeményezni.

A hálózat felépítése

11. §

(1) Az Egyetem hálózata több telephelyes, több településre kiterjedő hálózat. A hálózat logikai felépítése az alábbiak szerint valósult meg:

- a) Az Egyetem hálózata tűzfalakkal védett, logikailag zónákra osztott. Külön-külön zónákban működnek az oktatói-dolgozói, tantermi illetve a kollégiumokban működő számítógépek, valamint a több irányba szolgáltatást nyújtó szerver számítógépek.

- 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 zónákba történő besorolását a hálózati rendszergazdák javaslatainak figyelembe vételével az ISZK igazgatója határozza meg.
- (2) A hálózat mindenkor műszaki paramétereit külön dokumentáció tartalmazza.

A hálózat üzemeltetése, építése, bővítése

12. §

- (1) Kizárólag az ISZK jogosult a hálózat bővítésére, átalakítására. A hálózatot, a lehetőségeket figyelembe véve az ISZK az igényeknek megfelelően folyamatosan bővíti, karbantartja. Hálózat vagy hálózatrész építése, módosítása külső erőforrások (különösen: pályázat és más jellegű támogatások) bevonása esetében is csak ISZK illetékes vezetőjének jóváhagyásával történhet.
- (2) Illetéktelen személy a kialakított rendszeren nem változtathat, végpontot át nem helyezhet, és aktív vagy szerver-feladatokat ellátó eszközt a hálózatra nem kapcsolhat rá és nem kapcsolhat le.

A hálózati hardver használatának szabályai

13. §

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 ISZK szakemberei, vagy felügyeletükkel az ISZK által megbízott kivitelező végezheti.
- b) Hálózati aktív eszközöket (repeater, HUB, switch, router, tűzfal) csak az ISZK szakemberei vagy megbízottjaik csatlakoztathatnak vagy köthetnek le a hálózatról. Az aktív eszközök kapcsolatainak megbontására, az eszközök bármilyen eszközzel történő átkonfigurálására csak az ISZK szakemberei vagy megbízottjaik jogosultak.
- c) A hálózatra bármilyen berendezést (különösen: számítógép, nyomtató, fax, telefon) csak az ISZK engedélyével szabad csatlakoztatni.
- d) Az ISZK az engedély kiadását megtagadhatja, ha a csatlakoztatni kívánt berendezés a hálózat működését, rendeltetésszerű használatát, működési vagy adatvédelmi biztonságát (a továbbiakban: hálózati biztonság) veszélyeztetné.
- e) A hallgatói zónákban (különösen: könyvtárban, kollégiumban, konferenciákon vagy az Egyetem más helyszínein) saját személyi számítógép az ISZK-n történt előzetes bejelentés, a gépek alapvető paramétereinek és felhasználójának nyilvántartásba vétele után, az ISZK által megszabott feltételekkel használható.
- f) Időszakos rendezvények (különösen: konferenciák, gyakorlatok vagy események) idején az Egyetem területén működő vezeték nélküli, WiFi, internet szolgáltatást az ISZK által meghatározott feltételekkel (ideiglenes zónák kialakításával), be nem jelentett számítógépekkel is igénybe lehet venni. Az igénybevevők körét, a használathoz szükséges autentikáció módszerét az ISZK határozza meg.
- g) A WIFI csatlakozást igénybevevő mobil eszközök használatára ugyanazok a szabályok vonatkoznak, mint más számítógépekre. A mobilitásukból adódó nagyobb sebezhetőségükre tekintettel a rajtuk tárolt adatokra és a fizikai biztonságukra nagyobb figyelmet kell fordítani. Mobil eszközökön minősített adatok tárolása tilos. Mobil eszközökön minősített adatok tárolása tilos, azokon csak nyilvános adatok tárolása engedélyezett

- h) Saját tulajdonú, vagy más szervezet tulajdonát képező számítógépek hálózatra kapcsolását egyedi esetekben, az ISZK szakemberei által elvégzett előzetes ellenőrzés és a használathoz előírt programok telepítése után, az ISZK igazgatója engedélyezheti.
- i) 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 ISZK szakemberei végezhetik.
- j) Az Egyetemen rádiófrekvenciás és mikrohullámú frekvenciatartományban sugárzó infokommunikációs eszközt kizárólag az ISZK illetékes vezetője által engedélyezett frekvencián, az engedélyezett időtartamra lehet használni és használata előtt 30 nappal kell igényelni.
- k) Szolgálati mobiltelefonok használatának állandó illetve ideiglenes engedélyezését az Egyetem rektorának intézkedése szabályozza, ennek felügyeletét és működtetését az ISZK végzi.

A hálózati hibák elhárítása

14. §

A hálózat bármilyen jellegű meghibásodása esetén a hiba elhárítását az ISZK szakemberei legkésőbb a bejelentést követő első munkanapon megkezdik. Amennyiben a hiba elhárításához külső segítség szükséges vagy a hiba oka az Egyetem hálózatán kívül keletkezett, a hibát bejelenteni, elhárítására intézkedni, a javítást megrendelni csak az ISZK kijelölt szakemberei jogosultak.

III. FEJEZET

A HÁLÓZAT SZOFTVERÜZEMELTETÉSE

Támogatott protokollok

15. §

- (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) használata.
- (2) Az ISZK az egyes protokollok, portok, illetve 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.

Kritikus adatokat tartalmazó számítógépek használata

16. §

Az adatvédelmi szempontból kritikus adatokat (különösen: személyügyi, pénzügyi, ügyviteli információkat) tároló számítógépek védelmére fokozott figyelmet kell fordítani. Amennyiben a működésük nem teszi szükségessé, az internethez történő csatlakoztatásuk tilos. Ezen gépek körét az érintett szervezetek vezetői határozzák meg. Az igényelt, internetkapcsolat nélküli biztonságos belső hálózati kapcsolat biztosítása az ISZK feladata.

Személyi számítógépek felkészítése a használatra

17. §

- (1) Az Egyetem alkalmazottainak a számítógépeket az ISZK az érvényes telepítési protokoll szerint előre telepített operációs rendszerrel, irodai programcsomaggal, vírusvédelmi szoftverrel és a hálózati szolgáltatások igénybevételére alkalmas programokkal, személyre szólóan felkészítve adja át.
- (2) Ha a felhasználó számára kiadott számítógép a névre szóló felkészítés után másik felhasználóhoz kerül, az új felhasználó feladata kezdeményezni a szervezeti egysége vezetőjénél, aki az ISZK-nál igényli, hogy a gép szoftver konfigurációja, a rá vonatkozó hálózati bejegyzések megfelelő módon, az ISZK szakemberei által módosításra kerüljenek.
- (3) A számítógép hálózati beállításainak, rendszerlemeinek módosítására, az operációs rendszer és a gépre az ISZK által feltelepített szoftverek konfigurációjának megváltoztatására, szükség szerinti újratelepítésére csak az ISZK szakemberei, illetve az általuk erre felhatalmazott és megfelelően felkészített személyek jogosultak.
- (4) A folyamatos munkavégzésre kijelölt számítógépeken - az első hálózatra kapcsolás előtt - az előzetes ellenőrzést, a használathoz előírt programok telepítését, valamint a feladatra, személyre történő felkészítést az ISZK szakemberei az ISZK helyiségeiben hajtják végre.
- (5) Az egyes hálózati szolgáltatások igénybevételére használható, illetve a technikai segítségnyújtással támogatott programok körét az ISZK az érvényes telepítési protokollban határozza meg.

Szerverek üzemeltetése

18. §

- (1) Az Egyetemen kívülre, az Egyetem egésze vagy egy-egy kampusza számára szolgáltatást nyújtó szerver számítógépeket az ISZK üzemelteti. A szerverek felügyelete a kijelölt egyetemi rendszergazdák, a szerverek operációs rendszereinek karbantartása a rendszergazdák és velük együttműködve az ISZK igazgatója által felkért vagy kijelölt személyek feladata.
- (2) Az ISZK által üzemeltetett gépeken kívül szervergépek, informatikai szolgáltatások elindítása, ilyen szolgáltatást nyújtó számítógépek hálózatra kapcsolása az ISZK igazgatójának írásos engedélye nélkül tilos. Indokolt esetben ilyen jellegű szolgáltatás elindítását – kijelölt, felelős szervezeti rendszergazda felügyelete mellett – az ISZK igazgatója az egyetemi rendszergazdák javaslatainak figyelembe vételével engedélyezheti.

A rendszergazdák feladatai

19. §

A rendszergazda részletes felelősségét és hatáskörét a munkaköri leírása tartalmazza. A rendszergazdák feladatai:

- a) Az egyetemi hálózat biztonsági kockázatának minimalizálása.
- b) Az üzemeltetési feladatokat veszélyeztető és akadályozó tényezők felismerése és jelentése.
- c) Az informatikai szabályok betartása és betarttatása.
- d) A hálózati rendszergazdák feladata az Egyetemen működő, szerverszolgáltatást nyújtó számítógépek (a továbbiakban szerverek), valamint a hálózati aktív eszközök hardver és szoftver felügyelete, napi működésének biztosítása.
- e) A szervezeti rendszergazdák feladata az egyes egyetemi szervezetek kezelésében lévő, az ISZK igazgató engedélyével működő, hálózati szolgáltatást nyújtó számítógépek

üzemeltetése, az általuk üzemeltetett szerverek működésének biztosítása, valamint a hálózati rendszergazdák által megszabott üzemeltetési feltételek betartása, betartatása. A szervezeti rendszergazdákat a megfelelő szakismerettel rendelkező személyek közül, az adott egyetemi szervezet vezetőjének javaslata alapján az ISZK igazgatója jelöli ki.

- f) A WEB adminisztrátor feladata az Egyetem WEB szerverének üzemeltetése, az Egyetem honlapjának technikai felügyelete.
- g) A felügyelt szerverek, informatikai rendszerek katasztrófa és mentési terveinek elkészítése, az adatállományok rendszeres mentése, az esetlegesen bekövetkező katasztrófák következményeinek felszámolásával kapcsolatos tevékenységek begyakorlása.

Tanszékek és szervezetek informatikai felelőseinek feladatai

20. §

- (1) Az Egyetem valamennyi, informatikai eszközöket alkalmazó szervezeténél informatikai felelőst, kapcsolattartót (a továbbiakban: kapcsolattartó) kell kijelölni. A kapcsolattartó lehetőség szerint legalább alapvető informatikai ismeretekkel rendelkező személy legyen.
- (2) A kapcsolattartók feladata a hálózat működését érintő ügyekben a kapcsolattartás az ISZK szakembereivel, információszolgáltatás az ISZK számára, hibák bejelentése, üzemeltetéssel, tervezett leállásokkal kapcsolatos értesítések továbbítása az ISZK-tól a felhasználók felé.
- (3) A kijelölt kapcsolattartókat az ISZK-nál be kell jelenteni, ahol róluk elérhetőségükkel együtt naprakész nyilvántartást kell vezetni.

Távoli munkavégzés

21. §

- (1) Az ISZK a munkahelyi vezetők javaslatai alapján lehetővé teszi a kijelölt felhasználók részére az egyetemi hálózat bizonyos részeinek távoli, otthoni elérését. Az otthoni, távoli munkavégzés során is be kell tartani a biztonsági rendszabályokat, különös tekintettel az illetéktelen hozzáférés megakadályozására. A távoli hozzáférés esetében minimális biztonsági követelmény, hogy a hitelesítés során használt jelszó a hálózaton titkosított formában haladjon, valamint az adatforgalmat is titkosítani kell.
- (2) Az Egyetem hálózatára a távoli munkavégzés során VPN segítségével csatlakoztatott eszközök fokozott védelme, karbantartása, vírusvédelme, az illetéktelen hozzáférés megakadályozása a felhasználó kötelessége.

Adatok elhelyezésének szabályai a belső hálózaton

22. §

- (1) A több felhasználó által közösen használt adatok biztonságos, illetéktelen hozzáféréstől védett elhelyezésére az ISZK a szervereken szükség szerint tárhelyet biztosít. A tárterülethez történő hozzáférés beállítása az adatokért felelős személy írásos igénye alapján történik. A személyi számítógépeken tárolt adatok megosztását ISZK nem támogatja.
- (2) A szerveren tárolt adatok (fájlok) és a tárolásukra használt könyvtárak nevei esetében – az anyagok biztonsági mentéseinek lehetővé tétele érdekében – maximum 24 karakter hosszú nevek használhatók. Az elnevezésekben kerülni kell az ékezetes betűk használatát. Az egymásból nyíló (egymásba ágyazott) könyvtárak száma („mélysége”) nem haladhatja meg a 8-at.

- (3) A felhasználók a tanulmányi, oktatói, munkahelyi tevékenységükkel kapcsolatosan keletkezett adatokat a hálózati szervereken a számukra kijelölt könyvtárakban helyezhetik el. Ez a tárterület csak e tevékenységekkel kapcsolatos adatok tárolására használható. A könyvtárak elnevezéseinek, felhasználásuk céljainak, hozzáférési jogosultsági rendszerének beállítása az adatfelelős és a rendszergazda közös feladata. A könyvtárak elnevezésének egyértelműen utalnia kell a benne elhelyezett tartalomra. A területek adattartalmáért a jogosult felhasználók és a terület adatgazdája felel.
- (4) A hálózati szervereken és a munkaállomásokon minősített dokumentumok kezelése, tárolása tilos. Erre a célra kizárólag a minősítésnek megfelelően akkreditált helyiségekben elhelyezett munkaállomásokat lehet igénybe venni.
- (5) Nem közérdekű tartalmakat, magánjellegű információkat, a felhasználók csak a saját eszközeiken tárolhatják. A hálózati tárterülettel történő gazdálkodás az ISZK feladata és felelőssége. A hálózaton tárolt nem közérdekű tartalmak (különös tekintettel a magánjellegű dokumentumokra, videókra, fényképekre, és más hasonló jellegű adatállományokra) az ISZK hálózati rendszergazdája egy kör e-mailben előzetesen megjelölt határidőt követő napon jogosult törölni.
- (6) Amennyiben a felhasználó az általa elhelyezett adatok elérési útját, vagy e-mail címet, értesítésben, intézkedésben vagy egyéb kiadványban kívánja közzétenni - az ütközések elkerülése és a technikai megvalósíthatóság érdekében - köteles előzetesen egyeztetni az illetékes rendszergazdákkal.

Adatok, információk elhelyezésének szabályai az Egyetem WEB szerverén

23. §

- (1) Az Egyetem rektorának az egyetemi honlap működtetéséről szóló utasításában foglaltaknak megfelelően, az Egyetem internetes megjelenítését biztosító WEB szervereit az ISZK üzemelteti, felel azok működőképességéért, és végzi a honlap tartalmak feltöltését.
- (2) Az egyetemi honlap egységes megjelenéséért, tartalmáért az Egyetem Kommunikációs és Sajtóosztálya felelős, a hatályos rektori utasításokkal összhangban.
- (3) A honlapon minősített és az üzleti titok kategóriájába tartozó adatok, információk nem jeleníthetők meg.
- (4) Az egyes egyetemi szervezetekre vonatkozó információk tartalmáért, pontosságáért, naprakészségéért az adott szervezet vezetője a felelős.
- (5) A tartalomszolgáltatásért, a cikkek beküldéséért, azok tartalmi, formai teljességéért és helyességéért az adott szervezet vezetője a felelős.
- (6) A honlap karbantartását, archiválását, visszatöltését, szerkezeti összefüggéseinek, formai egységességének biztosítását a WEB adminisztrátorok végzik. A tartalmi vagy esztétikai szempontból nem megfelelő vagy tartalmilag elavult lapok megjelenítését a WEB adminisztrátorok - a Kommunikációs és Sajtóosztállyal, az ISZK igazgatójával, valamint az érintett szervezet vezetőjével történt egyeztetés után - elutasíthatják, törölhetik.
- (7) A honlap aktualizálásához szükséges adatforgalmat (le- és feltöltést) a WEB adminisztrátorok által meghatározott módon kell végezni.
- (8) Az egyes szervezeti egységek számára, a saját honlaprész kezeléséhez, az általuk megadott információk WEB felületen történő megjelenítéséhez – igény esetén – az ISZK szakemberei segítséget nyújtanak.
- (9) Amennyiben a felhasználó a WEB szerveren közzétett információ elérési útját (URL) értesítésben, intézkedésben vagy más kiadványban kívánja közzétenni - az ütközések elkerülése és a technikai megvalósíthatóság érdekében - köteles előzetesen egyeztetni az illetékes WEB adminisztrátorral.

Domain nevek használatának szabályai

24. §

Az Egyetem által használt, illetve az Egyetem életével kapcsolatos, internetes megjelenést szolgáló domain nevek igénylésére, kezelésére kizárólag az ISZK jogosult. Új domain név igény felmerülése esetén az ISZK-hoz kell fordulni. Az Egyetem életével kapcsolatos események hivatalos internetes megjelentetésére elsődleges forrásként az ezeken a domain neveken belül üzemelő Web felületek szolgálnak.

IV. FEJEZET

JOGOSULTSÁGOK ÉS INFORMATIKAI BIZTONSÁG

Jogosultságok az Egyetem informatikai hálózatán

25. §

- (1) Az Egyetem dolgozóinak túlnyomó többsége napi munkája során hálózatba kötött munkaállomáson végzi feladatait. Az egyetemi hálózat használatakor, a központi szolgáltatások igénybevétele esetében a felhasználói azonosítás kötelező. Érvényes felhasználói azonosító és jelszó nélkül senki nem kapcsolódhat sem a hálózatra, sem a különálló számítógépekre.
- (2) Az érvényes felhasználói azonosítóval rendelkező felhasználó az azonos jogosultsági körbe tartozó bármely hálózati munkaállomáson (a speciális feladatra kijelöltek kivételével) bejelentkezhet a hálózatra, ha ennek korlátozását illetékes vezető nem kéri, illetve nem rendeli 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 ISZK igazgatója határozza meg.
 - b) A jogosultságok kiosztásakor alapelveként kell kezelni, hogy minden funkcióhoz illetve feladathoz csak az ellátásához szükséges és elégséges mértékű jogosultságot kell biztosítani.
 - c) Az Egyetem hálózatához felhasználói hozzáférési jog mindenkit megillet, aki az intézménnyel hallgatói vagy foglalkoztatási jogviszonyban áll, és aláírásával igazolta, hogy a Szabályzat tartalmát megismerte, annak betartását vállalja.
 - d) Hozzáférési jogosultság adható 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) Az ISZK gondoskodik a hozzáférések naplózásáról, így regisztrálható a sikertelen hozzáférési kísérlet is. Ha jogosulatlan hozzáférés történt, vagy a jogosulatlan hozzáférés gyanúja merül fel, a jelszót azonnal meg kell változtatni.

(4) A hálózati hozzáférési jogosultságok szintjei:

Szint	Jogosultak	Jogok	Felelős
Külső	Vendégoktató, kutató, tanfolyami, rendezvény résztvevő	Internet elérés, WiFi használat	Szervezeti egység vezetője
Alap	Egyetem hallgatói, dolgozói	Egyéni azonosítás alapján lehetővé válik az oktatáshoz, tanuláshoz, munkához szükséges adatok, programok, levelezés, valamint az Internet elérése.	Karok és 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.	Karok és szervezeti egységek vezetői
Tanulmányi	Központi Tanulmányi Hivatal, Kari Tanulmányi Osztályok	Alapszint + teljes körű hozzáférés a Neptun rendszer adminisztratív moduljaihoz.	Oktatási Rektorhelyettes, illetékes tanulmányi vezető
Gazdasági	Gazdasági Főigazgatóság dolgozói a jogosultsági szintnek megfelelően	Alapszint + hozzáférés a gazdálkodással és a dolgozókkal kapcsolatos rendszerekhez.	Gazdasági Főigazgató
Humánpolitikai	Humánerőforrás Iroda dolgozói a jogosultsági szintnek megfelelően	Alapszint + hozzáférés a dolgozókkal kapcsolatos rendszerekhez.	Főtitkár
Rendszergazda (hálózati, szervezeti)	ISZK, egyetemi szervezetek rendszergazdái	Korlátlan jog a rendszergazda által felügyelt rendszerekhez (különösen: hálózat, storage, szerverek, adatbázisok, mentési rendszer, egyetemi szervezet által felügyelt szerver).	ISZK Igazgatója, egyetemi szervezet vezetője
Alkalmazás rendszergazda	Egy adott alkalmazás informatikai rendszergazda	Korlátlan jog az adott alkalmazáshoz. (különösen: AVIR, Gólya felvételi rendszerhez, Forrás SQL, Neptun).	ISZK Igazgatója

A jelszavak használatának szabályai

26. §

(1) A felhasználói jelszavak generálásának, átadásának bizalmasan kell történnie. A jelszavak kiválasztásánál a következő alapvető szabályokat kell betartani:

- Tilos a felhasználóra jellemző, könnyen kitalálható (különösen: vezetéknev, keresztnév) jelszavakat választani.
- Tilos a login nevet jelszóként használni.
- Tilos azonos számokból vagy betűkből álló jelszót használni.
- A jelszó hossza nem lehet rövidebb nyolc karakternél, tartalmaznia kell legalább kettő számjegyet, valamint legalább kettő betűt. Ajánlott a számok, kis és nagybetűk keverése jelszavak használatakor.

- e) Tilos a jelszót nyilvános helyen kiírva tartani (különösen: monitorra ragasztva).
- f) Kötelező a jelszót legalább 90 naponta újra cserélni.

(2) A fenti előírások jogellenes megszegésével okozott kárért a felhasználó teljes körű kártérítési felelősséggel tartozik.

Elektronikus levelezés használata az Egyetem hálózatán

27. §

- (1) Az ISZK az Egyetem állománya számára biztosítja az interneten keresztüli elektronikus levelezés lehetőségét. A szükséges e-mail címeket az ISZK-tól az igénylő lap kitöltésével lehet igényelni. Az igénylő lap kitöltésével és aláírásával a felhasználó elismeri jelen Szabályzat ismeretét és az abban tartalmazottak betartását.
- (2) Az illetékes rendszergazda - a benyújtott igénylőlap alapján, a felhasználó nevéből - egységes algoritmussal határozza meg az e-mail címet, valamint gondoskodik a címek nyilvántartásáról, karbantartásáról. A hallgatók e-mail fiókneve a hallgató Neptun kódja. A rendelkezésre álló tárhely nagyságát, a küldhető, illetve fogadható levelek méretét a technikai lehetőségek függvényében az ISZK határozza meg.
- (3) Az egyetemi hálózat szolgáltatásai használatának jogosultsága a jogviszony megszűnéséig tart. Az ISZK illetékes rendszergazdái az Egyetemi elhagyási lap benyújtásakor, az azon megjelölt határidővel (ami főszabályként a jogviszony megszűnésének a napja) gondoskodnak a volt dolgozó hálózati jogosultságainak megszüntetéséről, törléséről. Egyedi méltánylást igénylő esetben – a szakterületért felelős magasabb vezető javaslatára – az ISZK igazgatója a hozzáférést meghosszabbíthatja.
- (4) A jogviszony megszűnése után az egyetemi postafiók (levelezési cím) fenntartása, a használható postafiók méretének meghatározása a kilépő dolgozó szervezeti vezetőjének jóváhagyásával, és az ISZK igazgatóval történt egyeztetés után, egyedi elbírálás alapján történik.
- (5) Az Egyetem működésével kapcsolatos levelezéshez, kiadványokban történő megjelentetéshez csak a hivatalos egyetemi e-mail címek használhatók.
- (6) Az ISZK az egyes egyetemi szervezeteknek, illetve bizonyos, az Egyetem működéséhez kötődő speciális feladatok számára külön (kijelölt felelősökhöz kötött) szervezeti vagy (adott feladathoz létrehozott) tematikus e-mail címet biztosít. Ezeknek az e-mail címeknek utalniuk kell a tulajdonos szervezetre, vagy az adott feladatra. Tilos ilyen célra a saját személyes e-mail címeket használni.
- (7) A felhasználók az Egyetem hálózatának, levelező szolgáltatásának használata folyamán különösen az alábbi szabályokat kötelesek betartani, figyelembe venni:
 - a) Csak az Egyetemen történő oktatással, kutatással, társadalmi élettel, munkaköri feladatokkal kapcsolatos üzenetek továbbíthatók.
 - b) A központi levelezés során a felhasználó levelezési forgalma (a kommunikációban részt vevő felhasználók felhasználói azonosítói, az igénybe vett szolgáltatás típusa, a kommunikáció dátuma, kezdő és záró időpontja) naplózásra kerül (a levelek tartalma nem kerül rögzítésre).
 - c) Az Egyetem címjegyzékeinek felhasználásával, szervezeti egységeknek szóló körlevelet csak a saját szervezeti egysége vezetőjének engedélyével küldhet ki.
 - d) Az Egyetem informatikai rendszerének működésével kapcsolatos technikai jellegű tájékoztatás egyetemi, kari szintű körlevelek küldésére az ISZK igazgatója és a rendszergazdák külön engedély nélkül jogosultak.
 - e) Tilos minden olyan üzenetküldés, amelyet a nemzetközi hálózatok szabályai tiltanak.
 - f) Tilos az Egyetem hálózatában olyan adatok, levelek továbbítása, amelyben bármelyik, a feladó azonosítására szolgáló információ hamis, ide értve az elektronikus levél

szándékosan hamis feladóval történő küldését, a feladó vagy a küldő eltitkolását, hamisított fejlécű IP csomagok, üzenetek küldését.

- g) Tilos a nyílt levelező rendszeren minősített adatot továbbítani.
 - h) Tilos a nyílt levelező rendszeren biztonsági szempontból érzékeny (különösen: üzleti titkot képező) anyagot illetéktelen személy részére továbbítani.
 - i) Tilos a levelező rendszeren keresztül olyan tartalmú levelet küldeni, amely bármilyen más személy, csoport vagy társaság személyes, illetve üzleti érdekeit sértheti vagy veszélyeztetheti.
 - j) Tilos másokra nézve sértő, vallási, etnikai, politikai vagy más jellegű érzékenységet bántó, zaklató tevékenység (különösen: pornográf, pedofil vagy hasonló jellegű anyagok) közzététele.
 - k) Tilos a levelező rendszeren lánclevelet küldeni, rémhíreket terjeszteni.
 - l) Tilos az illegális tartalmak terjesztése vagy olyan tartalmú üzenetek küldése, ami másik felhasználó (hardver, szoftver) rendszerének megsemmisítését célozza, vagy működését hátrányosan befolyásolja.
- (8) A hálózatot használó munkaállomások alaphelyzetben (a speciális rendeltetésű számítógépek kivételével) rendelkeznek internet eléréssel. Az Egyetem fenntartja a jogot arra, hogy a vonatkozó törvények betartásával, és az azoktól kapott felhatalmazás alapján - különös tekintettel a Büntető Törvénykönyvben és az elektronikus hírközlésről szóló 2003. évi C törvényben foglaltakra - az egyetemi hálózat használata folyamán (a hálózat biztonságos, rendeltetés szerinti használatának fenntartása érdekében) a felhasználók internet forgalmát, tartalmát figyelemmel kísérje és naplózza.
- (9) A számítógépek és a hálózat felhasználásánál a jelen intézkedésben nem szabályozott kérdésekben a hatályos magyar jogszabályok irányadóak, különös tekintettel a Polgári Törvénykönyv és a Büntető Törvénykönyv, valamint a szerzői jogról szóló törvény vonatkozó rendelkezéseire. A hatályos jogszabályok rendelkezéseinek nem vagy nem kellő ismerete nem jelent mentesítést a megsértésük miatt kilátásba helyezett szankciók alkalmazása alól.

Szoftverjogtisztaság, szoftverek telepítése, frissítése

28. §

- (1) A szoftverek jogtisztaságának kérdése kiterjed a beszerzés, az üzemeltetés, a licencelés kérdéseire és megfelel a jogi, a pénzügyi és technikai követelményeknek.
- (2) A számítógépekre csak jogtiszt szoftverek telepíthetők.
- (3) A telepített szoftverek (és hardverek) nyilvántartását a Novell Zenworks Inventory teszi lehetővé.
- (4) Az Egyetem belső és tantermi zónáiban üzemelő felhasználói munkaállomásokon telepített operációs rendszerek, irodai szoftverek frissítése - jelenleg - az interneten keresztül automatikusan történik. A frissítési folyamat felhasználói beavatkozást nem igényel.

A számítógépes vírusvédelem az Egyetem informatikai hálózatában

29. §

- (1) A számítógép számítógépes vírussal vagy más rosszindulatú programmal, történő fertőzése súlyos biztonsági kockázat. Az Egyetem hálózatában az ISZK által központilag biztosított, felügyelt több szintű vírusvédelmi rendszer működik. Ha ennek ellenére valamelyik számítógép, felhasználói munkaállomás vírussal fertőződik, az ISZK kizárhatja azt a hálózati forgalomból (a belső hálózatot, az internetet, és a levelezést beleértve). A felhasználó ilyen esetben köteles a mielőbbi vírusmentesítés érdekében együttműködni az ISZK munkatársaival.

- (2) Több munkaállomás számítógépes vírusfertőzése esetén a vírusmentesítés és az ellenőrzések idejére, a fertőzés terjedésének megakadályozása érdekében az ISZK 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 az Egyetem belső és tantermi zónáiban üzemelő felhasználói munkaállomásokon. A szerver elérhetlensége esetén a munkaállomások vírusvédelmi rendszerének frissítése az interneten keresztül történhet.

Katasztrófakezelés, mentés, visszaállítás, szolgáltatásfolytonosság

30. §

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

V. FEJEZET

ZÁRÓ RENDELKEZÉSEK

31. §

- (1) A Szabályzat felügyeletével megbízott személy évente egyszer (szeptember 1-ig) köteles a Szabályzatot áttekinteni, a szükséges mértékben aktualizálni, függetlenül attól, hogy az adott időszakban történt-e változás vagy sem. A Szabályzat változásainak, aktuális változatának kihirdetése az ISZK feladata. 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) A Szabályzat összhangban áll a hatályos jogszabályokkal, valamint az Egyetem internetszolgáltatójának szabályaival, azok hatályosságát nem érinti. A Szabályzatban nem szabályozott kérdésekben a hatályos jogszabályok irányadók.
- (3) A Szabályzatban foglaltak megsértése esetén a Szabályzat nem ismerete nem mentesít a jogkövetkezmények alól.
- (4) Jelen Szabályzatot a Szenátus 92/2013. (VI. 5.) számú határozatával fogadta el.
- (5) A Szabályzat az elfogadását követő napon lép hatályba.