Hatály: 2015. X. 29 -

Nemzeti Közszolgálati Egyetem

Informatikai Biztonsági Szabályzat

EGYSÉGES SZERKEZETBEN
a 66/2015. (X. 28.) szenátusi határozat
módosító rendelkezéseivel)

2015.

Tartalom

I. FEJEZET

ÁLTALÁNOS RENDELKEZÉSEK

A Szabályzat célja

1. §

(1) A Nemzeti Közszolgálati Egyetem (a továbbiakban: Egyetem) Informatikai Biztonsági Szabályzat (a továbbiakban : Szabályzat) alapvető célja, hogy az elérhető szolgáltatások használata, alkalmazása során biztosítsa az adatvédelem alkotmányos elveinek, az adatbiztonság követelményeinek érvényesülését, és 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 információvagyon sértetlensége, bizalmassága és rendelkezésre állása biztosított legyen.

(2) Az Egyetem Informatikai Szolgáltató Központja (a továbbiakban: ISZK) az Egyetem összes telephelyére kiterjedő informatikai és kommunikációs hálózatot (a továbbiakban: Hálózat, ha az informatikai és kommunikációs hálózatról általánosságban van szó akkor 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 informatikai és kommunikációs 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. §

(1) 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, illetve mindazok, 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.

(2) A Vezető és Továbbképző Intézetre (a továbbiakban: VTKI) vonatkozó különös (kiegészítő) szabályok külön fejezetben kerülnek meghatározásra.

Értelmező rendelkezések

3. §

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. **Adatfeldolgozó:** Az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely az adatkezelővel kötött szerződése alapján - beleértve a jogszabály rendelkezése alapján történő szerződéskötést is - adatok feldolgozását végzi.
4. **Adatfelelős**: Az a közfeladatot ellátó szerv, amely az elektronikus úton kötelezően közzéteendő közérdekű adatot előállította, illetve amelynek a működése során ez az adat keletkezett.
5. **Adatgazda**: Felelős az általa kezelt adatokért, továbbá jogosult minősítés vagy osztályba sorolás elvégzésére.
6. **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 és megsemmisítése, valamint az adatok további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők rögzítése.
7. **Adatkezelő:** Az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, 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 végrehajtatja.
8. **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).
9. **Asztali munkaállomás**: A felhasználó rendelkezésére bocsátott számítástechnikai eszköz, mely alapvetően a számítógépből, monitorból, billentyűzetből és egérből, illetve más csatlakoztatható számítástechnikai eszközökből (különösen: mikrofon, kamera, scanner, stb.) állhat.
10. **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.
11. **Biztonság**: Az informatikai rendszerekben olyan előírások és szabványok betartását jelenti, amelyek a rendszer működőképességét, az információk rendelkezésre állását, sértetlenségét, bizalmasságát és hitelességét erősítik.
12. **BYOD (Bring Your Own Device – BYOD):** Saját mobileszközök (különösen: notebookok, tabletek, okos telefonok) munkahelyi környezetben való használata.
13. **Csomópont**: Szerver feladatokat ellátó eszközök és aktív eszközök csoportja az informatikai szolgáltatások ellátására.
14. **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 (különösen: uni-nke.hu).

15. **DNS (Domain Name System)**: Az internet neveket és címeket egymáshoz rendelő adatbázis, amely általában külön kiszolgáló gépen fut.
16. **Felhasználó**: Az a természetes személy, aki az egyetemi informatikai infrastruktúrát használja.
17. **Felhasználói azonosító**: Az intézményi címtárban tárolt egyedi azonosításra szolgáló rövid karaktersorozat, amely általában a felhasználó nevéből képződik.
18. **Felhőszolgáltatás, felhőszolgáltató** (angolul "cloud computing")**:** A feladatvégzéshez használt adatállományok, programok, szolgáltatások, stb. fizikailag nem a felhasználó számítógépén, hanem az interneten, egy szolgáltatónál (ún. szerver farmon, valahol a "felhőben") találhatók. Az adatok (e-mailek, címjegyzékek, naptárbejegyzések, és kedvenc linkek) felhőben való tárolásának egyik legnagyobb előnye, hogy bárhonnan könnyen elérhetők, és akkor sem vesznek el, ha a felhasználó számítógépe tönkremegy. Ez egyben a felhőszolgáltatás hátránya is: mivel nem tudható pontosan hol tárolják a fájlt, a felhasználók nem lehetnek biztosak afelől, hogy adataik mindig épségben, hozzáférhetők fognak maradni vagy, hogy illetéktelenek nem férnek hozzá. Éppen ezért a biztonsági kérdések figyelembevételével a felhőszolgáltatás igénybevétele nagy részt bizalmi kérdés is.
19. **Hálózat**: Felhasználói számítógépek és/vagy szerverek közötti adatátvitelt biztosító passzív és aktív eszközökből álló infrastruktúra.
20. **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.
21. **Hitelesség**: Az információ akkor hiteles, ha az elvárt, hozzáértő, megbízható forrásból származik.
22. **Informatikai erőforrások**: A hardver, szoftver eszközök összessége.
23. **Internet**: A világháló.
24. **Intranet**: Az intézményen belüli hálózat és annak szolgáltatásai.
25. **IP telefónia**: Olyan számítógép-hálózati alkalmazás, amely dedikált eszközök (készülék és központ, számítógépes hálózat) segítségével telefonszolgáltatást tesz lehetővé, ez a hagyományos telefonközpontokat felváltó számítógépes rendszer.
26. **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.
27. **Közérdekből nyilvános adat**: A közérdekű adat fogalma alá nem tartozó minden olyan adat, amelynek nyilvánosságra hozatalát, megismerhetőségét vagy hozzáférhetővé tételét törvény közérdekből elrendeli.
28. **Központi címtár**: Az Egyetem dolgozóinak felhasználói adatait tároló LDAP adatbázis.
29. **Központi szolgáltatások**: Levelezés, címtár, fájl kiszolgálás, web szolgáltatás, névszolgáltatás, és más informatikai és kommunikációs szolgáltatások.
30. **LDAP (Light Weight Directory Access Protocol**): Nyílt szabványú címtár struktúra leíró nyelv.
31. **Mobil eszközök**: Notebook, netbook, tablet, palmtop, okostelefon.
32. **NEPTUN kód**: A NEPTUN rendszer szolgáltatásaihoz hozzáférést biztosító betűkből és számokból álló, legalább 6 karakter hosszúságú kód.
33. **NIIFI (Nemzeti Információs Infrastruktúra Fejlesztési Intézet)**: Az Intézet 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.

34. **Okostelefon**: Internetezésre és/vagy dokumentumkezelésre is használható mobil telefon.
35. **Passzív eszközök**: Hálózati kábelezés és csatlakozók.
36. **Rendelkezésre állás**: Annak biztosítása, hogy a szükséges információ a szükséges időben az arra jogosultak számára meghatározott formában hozzáférhető, elérhető legyen.
37. **Sértetlenség**: Az információ létének, hitelességének, épségének, önmagában teljességének kritériuma.
38. **Social engineering**: Megtévesztés, az emberek bizalomra való hajlamának manipulatív kihasználása, információgyűjtés számítógépes rendszerekbe történő behatolás érdekében.
39. **Számítógép**: Olyan informatikai eszköz, amelyet a felhasználó a napi munkája során használ, és amellyel igénybe veheti a hálózat szolgáltatásait.
40. **Szerver-feladatokat ellátó eszköz**: Olyan számítógépek, szoftverek, vagy speciális eszközök, amelyek különböző szolgáltatásokat biztosítanak más számítógépek számára.
41. **Szerverhelyiség**: Fokozottan védett, naplózott bejutású, klimatizált, zárt helyiség, ahol a folyamatos működés feltételei az informatikai erőforrások számára biztosítottak.
42. **Szervezeti rendszergazda**: Az egyes egyetemi szervezetek felügyeletében lévő hálózati szolgáltatást nyújtó számítógép adminisztrátora.
43. **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.
44. **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.
45. **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).
46. **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.
47. **WiFi (Wireless Fidelity), 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 szabályzatokban foglaltak szerint lehet használni. A Hálózatot - összhangban NIIFI Felhasználói Szabályzatával - **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 (különösen: rágalmazás, stb.), 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 érzékenységét bántó, zaklató tevékenység (különösen: pornográf, pedofil anyagok közzététele);
c) A hálózati erőforrások, szolgáltatások olyan célra való használata, amely az erőforrás/szolgáltatás eredeti céljától idegen (különösen: hírcsoportokba/levelezési listákra a csoport/lista témájába nem vágó üzenet küldése).
d) Profitszerzést célzó, direkt üzleti célú tevékenység és reklám;
e) Mások munkájának zavarása vagy akadályozása (különösen: kéretlen levelek, hirdetések).
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/szolgáltatások - akár tesztelés céljából történő - illetéktelen szisztematikus próbálgatása (különösen: TCP port scan);
j) A Hálózat erőforrásainak, a hálózaton elérhető adatoknak illetéktelen módosítására, megrongálására, megsemmisítésére vagy bármely károkozásra irányuló tevékenység;
k) Hálózati üzenetek, hálózati eszközök hamisítása: olyan látszat keltése, mintha egy üzenet más gépről vagy más felhasználótól származna (spoofing).
l) A Hálózat bármely szolgáltatásának szándékos, vagy hiányos ismeretekből, nem megfelelő körültekintéssel végzett beavatkozásokból fakadó zavarása, illetve részleges vagy teljes bénítása (leszámítva a rendeltetésszerű használat fenntartásához szükséges, a hálózati rendszergazdák, rendszermérnökök általi tudatos beavatkozásokat).

Központi szolgáltatások az informatikai hálózaton

5. §

Az informatikai hálózaton[1] elérhető központi szolgáltatások

[1] Az 5. §-ban felsorolt szolgáltatások az Egyetemen nem minden esetben és nem minden helyszínen érhetők el.

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) Az egyetemi intranet szerverek üzemeltetése;
f) Domain nevek kezelése;
g) Jelszavas hozzáférés szabályozáson alapuló, védett adattároló területek biztosítása a közös munkavégzéshez a központi szervereken;
h) Biztonságos távoli munkavégzéshez VPN kapcsolat biztosítása;
i) Központi nyomtatás kezelő rendszer (SAFEQ) üzemeltetése;
j) Központi vírusvédelmi és spamszűrő rendszer üzemeltetése;
k) Video Streaming szolgáltatás;
l) Tanulmányi információs rendszer (NEPTUN) elérhetőségének biztosítása;
m) Gazdálkodási rendszer (Forrás SQL);
n) Távoktatási rendszerek (ILIAS, MOODLE) üzemeltetése;
o) Integrált könyvtári rendszer (OLIB);
p) Elektronikus iktatórendszer;
q) Belső adminisztratív rendszerek (Felhasználói ügybejelentő, Kollégiumi elhelyezés igénylő, Közalkalmazotti önéletrajz nyilvántartó rendszer, Nyomdai szolgáltatás igénylő, Rendezvény nyilvántartó, Szenátusi anyagok köröztető rendszere);
r) Személyügyi rendszer (SZENYOR);
s) Közszolgálati egyéni teljesítményértékelési rendszer (TÉR);
t) Vezetői információs rendszer (VIR);
u) Tervkezelő és nyilvántartó rendszer (PlanDoc);
v) Complex jogtár;
w) SPSS statisztikai programcsomag;
x) CorelDRAW grafikai csomag;

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 szabályozatok, 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 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 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 vagy e-mailben, és az esedékesség előtt min. 1 órával belső hálózati üzenet formájában történő bejelentése.
k) Az általános informatikai ismereteken túli, az adott szolgáltatás igénybevételéhez szükséges ismeretek 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 bármely szolgáltatás 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 előretelepített kliens programmal, illetve web felületen 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 foganatosított 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) Az Egyetem Hálózatán csak a számára engedélyezett erőforrásokat használni.
d) Tevékenységével nem zavarni, nem akadályozni, nem veszélyeztetni az egyetemi hálózaton feladataikat végzők tevékenységét.
e) 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.).
f) A hálózati szolgáltatások, a távfelügyeleti rendszerek működéséhez szükséges segédprogramok telepítését lehetővé tenni.
g) Gondoskodni adatainak tőle elvárható védelméről és helyi mentéséről.
h) A számára biztosított informatikai és kommunikációs eszközöket működőképes állapotban megőrizni, leltározáskor és más ellenőrzéskor kérésre bemutatni, a jogviszony/munkaviszony megszűnésekor visszaszolgáltatni (a biztosított eszközöket, berendezéseket nem bonthatja meg, a hardver és szoftverkörnyezetet - beleértve a számítógépes vírusellenőrzéssel, és vírusirtással kapcsolatos szoftvereket is – nem vagy csak az ISZK igazgatójának külön engedélyével módosíthatja, az eszközök hálózati és egyéb beállításaiban működést befolyásoló módosításokat nem végezhet).
i) Felelősséget vállalni az általa szándékosságból, vagy gondatlanságból, vagy a neki felróható módon az általa, a nevében, a felhasználói azonosítójával (különösen: a jelszavak kölcsönadásával vagy nem biztonságos kezelésével, a hozzáférési jogosultságok nem megfelelő kezelésével, a számára biztosított – az egyetem tulajdonát képező - informatikai, kommunikációs eszközökben vagy eszközökkel) okozott szabályellenes cselekedetekért, károkért. Az előbbiekből eredő esetleges működési zavar, adatvesztés utáni helyreállítás, javítás/javíttatás költségeit - a vonatkozó jogszabályokban, és más közjogi szervezetszabályozó eszközökben megfogalmazottak szerint - megtéríteni.
j) Meghibásodás, üzemzavar észlelésekor, vírusfertőzés (vagy annak gyanúja) esetén haladéktalanul értesíteni az ISZK-t, a számítógép további használatát az ISZK informatikusainak intézkedéséig felfüggeszteni. A hibaelhárítás folyamán az ISZK szakembereivel együttműködni, számukra a szükséges információkat megadni.

k) 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.
l) Az egyetemi Hálózaton, levelező rendszerben, telefonkönyvben tárolt adataiban (név, szervezeti egység, beosztás, munkahelyi telefonszám) történt változásokat (különösen: névváltozás, más szervezeti egységhez történt áthelyezés) az ISZK-nál bejelenteni.
m) Az Egyetem Hálózatáról értesítésben, intézkedésben vagy egyéb kiadványban közzé tenni kívánt e-mail címet vagy bárminemű tartalmak hálózatos elérhetőségi útvonalát illetékes rendszergazdákkal egyeztetni az ütközések elkerülése, a technikai megvalósíthatóság és a nyilvánosságra hozhatóság, közölhetőség ellenőrzése érdekében.
n) Amennyiben tudomására jut, hogy bárki megsértette a Szabályzatban foglaltakat, haladéktalanul tájékoztatni az ISZK-t és az adott szervezeti egység vezetőjét.

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. Az Egyetem informatikai Hálózatának szolgáltatásait csak az eljárás lefolytatása után és annak eredményétől függően veheti igénybe.
d) A szándékos elkövető – a fentieken túl, amennyiben kimutatható anyagi kár is keletkezett - köteles megtéríteni az általa okozott károkat a vonatkozó jogszabályok és más közjogi szervezetszabályozó eszközök 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. Telephelyenként külön-külön zónákban működnek az oktatói-dolgozói, tantermi illetve a kollégiumokban működő gépek, valamint a több irányba szolgáltatást nyújtó szerver számítógépek. A hálózati működés biztosításához, illetve speciális feladatokhoz további zónák is kialakításra kerültek/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 zónákba történő besorolását a hálózati rendszergazdák javaslatainak figyelembe vételével az ISZK igazgatója határozza meg.

(2) A Hálózat mindenkori 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, valamint az Egyetem rendszerén kívüli szolgáltatásokhoz, hálózatokhoz állandó kapcsolat (különösen site-to-site VPN) létesítése külső erőforrások (különösen: pályázat, és más jellegű támogatások) bevonása esetében is csak az ISZK igazgatójának 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.

Az egyetemi informatikai és kommunikációs Hálózat 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: számítógépeket, perifériákat – nyomtató, scanner külső adattárolók - fax, okostelefon, stb.) csak az ISZK engedélyével szabad csatlakoztatni. Ha az eszköz adattárolásra is alkalmas, akkor a csatlakoztatás után vírusellenőrzést kell végrehajtani, illetve az adatok tárolására vonatkozó jelen és más vonatkozó egyetemi szabályzatok és előírások betartására különös figyelmet kell fordítani..

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, kivéve az alábbi „f” pontban felsorolt eseteket.

f) Időszakos rendezvények (különösen: konferenciák, gyakorlatok vagy más 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 bizalmas és 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. Részletesebben lásd a Saját eszközök használata (BYOD), 29.§-ban.
i) A hálózati aktív eszközök feszültségmentesítését (kikapcsolását) áramszünet, természeti csapás (különösen: tűz, vízbetörés vagy más rendkívüli esemény), áramütés, 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 legalább 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 a meghibásodásban érintett hálózatrész üzemeltetéséért felelős szakemberek jogosultak. Mind a hálózati meghibásodásról és a tett intézkedésekről tájékoztatni kell az ISZK igazgatóját.

III. FEJEZET

AZ INFORMATIKAI HÁLÓZAT SZOFTVER ÜZEMELTETÉSE

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 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.

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 egyes hálózati szolgáltatások igénybevételére használható, illetve a technikai segítségnyújtással támogatott programok körét az ISZK az érvényes telepítési protokollban határozza meg.

(2) A folyamatos munkavégzésre kijelölt számítógépeken - az első hálózatra kapcsolás előtt - az előzetes ellenőrzést, a használathoz előírt programok telepítését, valamint a feladatra történő felkészítést, a személyre-szabást az ISZK szakemberei az ISZK helyiségeiben hajtják végre.

(3) 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.

(4) Ha a felhasználó számára kiadott számítógép a névre szóló felkészítés után másik felhasználóhoz kerül, akkor az új felhasználó feladata kezdeményezni az ISZK-nál, hogy a gép szoftver konfigurációja, és a rá vonatkozó hálózati bejegyzések megfelelő módon, az ISZK szakemberei által módosításra kerüljenek.

(5) A számítógép hálózati beállításainak, rendszerelemeinek módosítására, az operációs rendszer és a gépre feltelepített szoftverek konfigurációjának megváltoztatására, szükség szerinti újratelepítésére vagy új programok telepítésére csak az ISZK szakemberei, illetve az általuk erre felhatalmazott és megfelelően felkészített személyek jogosultak.

(6) A VTKI-n üzemeltetett számítógépek használatra történő felkészítésére vonatkozó különös szabályok külön fejezetben kerülnek szabályozásra.

Szerverek üzemeltetése

18. §

1) Az Egyetemen kívülre, az Egyetem egésze vagy egy-egy kampusza számára szolgáltatást nyújtó szerverek felügyelete - beleértve az operációs rendszereik karbantartását, frissítését is - a kijelölt egyetemi rendszergazdák és az együttműködésre hivatalosan felkért vagy kijelölt személyek feladata.

2) Az ISZK által üzemeltetett számítógépeken kívül szerverek, informatikai szolgáltatások elindítása, ilyen szolgáltatást nyújtó számítógépek Hálózatra kapcsolása az ISZK igazgatójával történt egyeztetés után történhet.

A rendszergazdák feladatai

19. §

A rendszergazda részletes felelősségét és hatáskörét a munkaköri leírása tartalmazza, amely magába foglalja az alábbiakat:

a) Az egyetemi Hálózat biztonsági kockázatának minimalizálása.
b) Az üzemeltetési feladatokat veszélyeztető és akadályozó tényezők felismerése és jelentése.
c) Az informatikai szabályok betartása és betartatása.
d) A hálózati rendszergazdák feladata a felelősségi és hatáskörükbe tartozó 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 felügyelt szerverek, informatikai rendszerek katasztrófa és mentési terveinek elkészítése, az adatállományok rendszeres mentése, az esetlegesen bekövetkező katasztrófák következményeinek felszámolásával kapcsolatos tevékenységek begyakorlása.

Tanszékek és más egyetemi szervezeti egységek 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, információcsere az ISZK szakembereivel, 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 az Egyetem informatikai Hálózatán

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 munkaállomásokon tárolt adatok hálózaton keresztül történő megosztását (különös tekintettel a mobil eszközökre) az ISZK nem támogatja.

(2) A fájlok elérési útvonalának a teljes hossza maximum 256 karakter lehet, amelybe a könyvtárstruktúrát alkotó könyvtárak nevei, a fájlnév és a kiterjesztés (.XXX) is beleértendő (S:\könyvtár\alkönyvtárA\alkönyvtárAB\alkönyvtárABC\irat.doc). A megnevezésekben kerülni kell az ékezetes magyar magánhangzók - legfőképpen az í, Í, ő, Ő, ú, Ú, ű, Ű - használatát, mivel egyes rendszerek nem tudják helyesen kezelni ezeket a karaktereket.

(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) A Hálózat tárterületével történő gazdálkodás az ISZK feladata és felelőssége. Az Egyetem tulajdonában lévő eszközök (vagyontárgyak) – úgymint a Hálózat és más számítástechnikai eszközök - csak az egyetem tulajdonát képező adatok tárolására használhatók. A Hálózaton tárolt nem közérdekű (különösen: magánjellegű) vagy az aktualitásukat veszített közérdekű tartalmakat (különösen: videók, fényképek, és más hasonló jellegű adatállományok), amennyiben a munkavégzést akadályozzák akár azonnal, ellenkező esetben a tulajdonos értésítését követő 24 óra elteltével az ISZK hálózati rendszergazdája jogosult törölni.

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. A kijelölt tartalmi honlapfelelősök végzik a honlap tartalmak feltöltését.

(2) Az egyetemi honlap egységes megjelenéséért, tartalmáért - az érvényes rektori utasításnak megfelelően - az Egyetem kommunikációért és sajtómegjelenésért felelős szervezeti egység vezetője felel.

(3) A honlapon csak publikus, közérdekű és közérdekből nyilvános adatok jeleníthetők meg. Minősített adatok, információk megjelenítése **tilos.**

(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) Az egyetemi honlapon történő adat/információ megjelenítésnél szigorúan be kell tartani a személyes és közérdekű, valamint a minősített adatok védelmére és biztonságára vonatkozó jogszabályokban és más közjogi szervezetszabályozó eszközökben (különösen a hatályos NKE Etikai kódexben és a biztonsági szabályzatokban) meghatározott előírásokat.

(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 Rendszerfejlesztési Osztály szakemberei segítséget nyújtanak.

Domain nevek használatának, tanúsítványok igénylésének szabályai

24. §

(1) Az Egyetem által használt, illetve az Egyetem életével kapcsolatos, internetes megjelenést szolgáló domain nevek igénylésére, kezelésére kizárólag az ISZK jogosult. Új domain név és SSL kapcsolatot igénylő szerver és felhasználói tanúsítványok, lejárt tanúsítványok helyett újak igénylése esetén az ISZK igazgatójához kell fordulni.

(2) 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 Egyetem informatikai Hálózatán nyújtott szolgáltatások igénybevétele kötelező felhasználói azonosításhoz – az egyedi számítógépeken és a hálózati kapcsolatokhoz is érvényes felhasználói azonosító és jelszó használatához (autentikációhoz) - köthető.

(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.

(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 alapelvként 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) Biztonsági okokból és a későbbi visszakereshetőség, elemzések elvégzése érdekében - a szervereken - az egyetemi Hálózatba történő sikeres és sikertelen belépési kísérletek 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, 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 Iroda,[2] 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, Forrás SQL, Neptun).	ISZK Igazgatója, egyetemi szervezeti egység vezetője

[2] Módosította a 66/2015. (X. 28.) szenátusi határozat.

A jelszavak használatának szabályai

26. §

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

a) **Tilos** a felhasználóra jellemző, könnyen kitalálható (különösen: vezetéknév, keresztnév, saját gyermekek, ismert kedvenc személy, kedvenc háziállatok, stb.) jelszavakat választani.
b) **Tilos** a login nevet jelszóként használni.
c) **Tilos** azonos vagy az abc-ben, a billentyűzeten egymást követő számokból vagy betűkből álló jelszót használni.
d) 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) A hálózati belépésre jogosító jelszót kötelező - az egyéb jelszavakat ajánlott rendszeresen, de legalább - 90 naponta újra cserélni.

(2) A felhasználók a Hálózathoz, rendszerekhez történő hozzáférést biztosító jelszavakat - első alkalommal – az illetékes rendszergazdáktól lezárt borítékban kapják meg, vagy a felügyeletükben a felhasználók saját maguknak állítják be. A borítékban kiadott jelszavakat az első belépést követően azonnal módosítani kell.

(3) Az elfelejtett, lejárt jelszavak helyett új jelszavak kiadása elsősorban csak személyesen, az illetékes rendszergazdánál az első alkalommal történt jelszavak kiadásához hasonlóan történik.

(4) Az Egyetem Hálózatához történő hozzáférés - jelszó igénylés - jogosultságának ellenőrzése érdekében a rendszergazda kérheti a felhasználó egyetemi belépőkártyáját, vagy az érvényes „személyazonosításra alkalmas hatósági igazolványát” (személyazonosító igazolványát, vagy útlevelét, vagy kártyaformátumú vezetői engedélyét).

(5) Telefonon csak abban az esetben lehet jelszó módosítást kérni, ha illetékes informatikus szakember jelen van és telefonon igazolni tudja a felhasználó személyazonosságát és a jelszó módosítás jogosságát. Minden más esetben tilos a telefonon történő jelszókérés, és közlés.

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

Internet és elektronikus levelezés használata az Egyetem informatikai Hálózatán

27. §

(1) Az Egyetem Hálózatán biztosított internetelérés és levelezés a munkavégzést, az egyetemi célokat hivatott szolgálni, éppen ezért elsősorban az Egyetemen történő oktatással, kutatással, társadalmi élettel, munkaköri feladatokkal kapcsolatos feladatok felelősségteljes végzése támogatott.

(2) Az előző pontban leírt célok elérése érdekében és szükség esetén - különösen biztonsági okokból, a Hálózat terheltségének csökkentése érdekében, stb. – egyes honlapok, külső levelező rendszerek elérése tiltásra kerülhet.

(3) Az ISZK az Egyetem állománya számára biztosítja az interneten keresztüli elektronikus levelezés lehetőségét. A szükséges e-mail címeket az ISZK-tól az erre a célra

rendszeresített igénylő lap kitöltésével lehet igényelni. Az igénylő lap kitöltésével és aláírásával a felhasználó elismeri jelen Szabályzat ismeretét és az abban tartalmazottak betartását.

(4) Az illetékes rendszergazda egységes algoritmussal - a benyújtott igénylőlap alapján, a felhasználó nevéből, amelytől csak indokolt esetben, a felhasználóval történő egyeztetés után térhet el - 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.

(5) Az egyetemi Hálózat szolgáltatásai használatának jogosultsága a jogviszony megszűnéséig tart. Az illetékes rendszergazdák 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.

(6) 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.

(7) Az Egyetem működésével kapcsolatos levelezéshez, kiadványokban történő megjelentetéshez csak a hivatalos egyetemi e-mail címek használhatók.

(8) 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.

(9) A felhasználók az Egyetem Hálózatának, levelező szolgáltatásának használata folyamán különösen az alábbi szabályokat kötelesek betartani, figyelembe venni:

a) Az egyetemi levelező rendszeren létrehozott e-mail címek - a személyhez kötéstől függetlenül - a munkavégzést, az egyetemi célokat hivatottak szolgálni, éppen ezért elsősorban 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 üzemeltetésért felelős rendszergazdák az üzemeltető egyetemi szervezet vezetőjének engedélyével jogosultak.
e) Biztonsági és adatvédelmi okokból a beérkező levelek feltétel nélküli átirányítása csak az „uni-nke.hu” fő domain alatt üzemelő szerverekre engedélyezett, minden más levelező szerverre/domainre tiltott.
f) Az Egyetem levelező rendszere a nyílt interneten, web felületen is elérhető. A levelező rendszer web felületen történő használata biztonsági okokból nagy körültekintést követel meg. Használata csak megbízható környezetben ajánlott.

g) Amennyiben a felhasználó a postafiókjába 3 hónapon keresztül nem lép be, a postafiók - tartalmának változatlanul hagyása mellett - zárolásra kerül. A postafiók fogadja a leveleket, de a felhasználó nem tud belépni. További 3 hónap elteltével a fiók már leveleket sem fogad. Újabb 6 hónap (összesen 12 hónap) elteltével, a zárolás feloldására irányuló kérés hiányában, az felhasználói e-mail cím és a postafiók a tartalmával együtt törlésre kerül.
h) **Tilos** minden olyan üzenetküldés, amelyet a nemzetközi hálózatok írott és íratlan szabályai (netikett) tiltanak.
i) **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.
j) **Tilos** a nyílt levelező rendszeren minősített adatot továbbítani.
k) **Tilos** a nyílt levelező rendszeren biztonsági szempontból érzékeny (különösen: minősített, és más nem publikus) anyagot illetéktelen személy részére hozzáférhetővé tenni.
l) **Tilos** a levelező rendszeren keresztül olyan tartalmú levelet küldeni, amely bármilyen más személy, csoport vagy társaság személyes, illetve üzleti érdekeit sértheti vagy veszélyeztetheti.
m) **Tilos** másokra nézve sértő, vallási, etnikai, politikai vagy más jellegű érzékenységet bántó, zaklató tevékenység (különösen: pornográf, pedofil vagy hasonló jellegű anyagok) közzététele.
n) **Tilos** a levelező rendszeren lánclevelet, kéretlen reklámokat (spam) küldeni, rémhíreket terjeszteni.
o) **Tilos** az illegális tartalmak terjesztése vagy olyan tartalmú üzenetek küldése, ami másik felhasználó (hardver, szoftver) rendszerének megsemmisítését célozza, vagy működését hátrányosan befolyásolja.

(10) 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, és rendeltetés szerinti használatának, optimális leterheltségének, sebességének kialakítása, fenntartása érdekében) a felhasználók internet forgalmát, tartalmát figyelemmel kísérje és naplózza, a veszélyes internetes honlapok elérését letiltsa.

(11) 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.

Social engineering (megtévesztés)

28. §

Az informatikai Hálózat biztonságát legegyszerűbben, legolcsóbban a social engineering (még nincs általánosan elfogadott magyar megfelelője, leggyakrabban pszichológiai manipulációként kerül hivatkozásra, illetve legegyszerűbben megtévesztésnek lehet nevezni) módszerrel lehet veszélyeztetni. Ez a módszer az emberek manipulálására, segítőkészségére, gyanútlanságára, hiszékenységére alapozva teszi lehetővé a bizalmas

információk megszerzését, majd a rendszerekbe történő bejutást és károkozást. Nagy körültekintést és óvatosságot igényel az e módszerekből eredő veszélyek elkerülése. Az alábbi szabályok betartásával csökkenthető a social engineeringből fakadó veszélyeztetettség (az alább felsoroltak nem teljes körűek, mivel nap mint nap újabb és kifinomultabb módszerek jelennek meg):

a) Ismeretlen, nem megbízható helyről származó, idegen adathordozót (különösen: CD, DVD, pendrive, külső meghajtó) tilos a számítógéphez csatlakoztatni, mert behatolást elősegítő programokat tartalmazhatnak.
b) Ismeretlen címről érkező, egyetemi viszonylatban nem megszokott tárgyú (különösen értesítő nagy nyereményről, örökségről, rendkívül kedvező áron elérhető vásárlásról, vagy segítség kérése beteg gyermek gyógyításához, stb. témájú) gyanús e-mailt, és csatolmányait nem szabad megnyitni, mert vírusokkal fertőzhetik meg a számítógépet és a Hálózatot. (Az e-mailek és csatolmányaik rosszindulatú kódokat tartalmazhatnak.)
c) Az e-mailekben (még ismerőstől származó levélben is) szereplő linkekre csak nagy körültekintéssel szabad kattintani, mivel rosszindulatú kódokat tartalmazó honlapokra irányíthatja át a 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) Egyetemi e-mail címmel csak az egyetemi feladatokhoz szorosan kapcsolódó ismert, szakmai honlapokra engedélyezett regisztrálni és a belépési jelszónak az Egyetemen használt jelszótól különböző jelszót kell megadni. Minden más honlapon **tilos** az egyetemi, hivatalos e-mail cím használata.
e) Minden jelszóval védett információs rendszerhez különböző jelszót kell használni. Azonos jelszavak használata nemcsak a felhasználók, hanem a rendszerbe rossz szándékkal behatolók dolgát is nagy mértékben megkönnyíti.
f) Tilos könnyen hozzáférhető helyen felírva (különösen: képernyőn) tárolni a jelszavakat. Ha bármi okból, mégis felírva kell azokat tárolni, akkor biztonságos, zárt helyen a leragasztás mentén aláírt, zárt borítékban.
g) Az ISZK és más szervezetek informatikusai, a rendszergazdák sosem kérik telefonon vagy e-mailen keresztül megadni a jelszavakat, legfeljebb csak a felhasználó által az azonnali módosítását. Ha valaki ezt kéri, ez gyanús és értesíteni kell az ISZK-t.
h) Az aktuálisan nem használt számítógépet ki kell kapcsolni vagy jelszó védetten zárolni kell azt.
i) A jogtalan hozzáférés, információvesztés, és rongálás elkerülése érdekében alkalmazni kell a „tiszta asztal, tiszta képernyő” szabályt, azaz az aktuális feladathoz csak a legszükségesebb anyagokat kell az asztalon hozzáférhetően, a képernyőn láthatóan tartani. Munkaidőn túl az iratokat az íróasztalokon nem lehet tárolni, el kell zárni azokat. Külön figyelmet kell fordítani és messzemenően be kell tartani az információk/adatok minősítésére vonatkozó előírásokat.
j) A nyomtatókról azonnal el kell távolítani a kinyomtatott iratokat, illetve a korszerű hálózati nyomtatókon lehetőség szerint alkalmazni kell a biztonságos nyomtatás funkciót, amely keretében a felhasználó megadja a saját azonosítóját, majd a nyomtatón ugyanezt beüti és megjelennek a nyomtatandó dokumentumok – így biztosítható, hogy a felhasználó jelenléte és felügyelete mellett történjen a nyomtatás.
k) A fölöslegessé vált, idejét múlt iratokat nem kell tárolni, amint lehetőség van rá iratmegsemmisítőn le kell zúzni azokat. A nyílt iratokat is tilos kukába dobni.

Saját eszközök használata (BYOD)

29. §

(1) A felhasználók saját elsősorban mobil vagy esetleg más asztali számítástechnikai eszközeinek az Egyetemen történő használata:

a) Egyetemi célokra (munkavégzésre) történő használatát a munkavállaló munkahelyi vezetőjének javaslatára az ISZK igazgatója – a megbízható hálózati működéshez és a védelemhez szükséges programok (különösen: vírusirtó program) ISZK által történt telepítése és nyilvántartásba vétele után – engedélyezheti az alábbi feltételekkel:

- A mobil eszközön tárolt egyetemi (munkahelyi) adatok biztonságáért az eszköz tulajdonosa teljes körű felelősséggel tartozik.
- A mobil eszközön az operációs rendszer, biztonsági csomag, irodai rendszerek utolsó biztonságos frissítése használható, ezért javasolt aktivizálni ezek automatikus frissítés funkcióját. (A biztonsági frissítéseket a programgyártók ingyenesen teszik elérhetővé.)
- Mobil eszközön bizalmas és minősített adatok tárolása **tilos**, azokon csak nyilvános adatok tárolása engedélyezett!
- Az eszközt számítástechnikai hálózathoz, internethez csatlakoztatni csak biztonságos körülmények szabad. A vezetéknélküli - WiFi, bluetooth - kapcsolat csak biztonságos körülmények között használható, ezután kikapcsolásuk ajánlott (nyilvános helyeken – különösen szórakozóhelyek, üzletek, állomások területén elérhető hálózatok használata nem ajánlott).
- A mobil eszköz biztonságos használatára különösen nagy figyelmet kell fordítani. Ezek az eszközök a mobilitásukból eredően, könnyen hozzáférhetőek, eltulajdoníthatóak. A rajtuk tárolt adatok (különösen: WiFi, bluetooth kapcsolaton keresztül) akár a tulajdonos, a használó tudtán kívül is lemásolhatók. Amennyiben a biztonsági esemény (különösen: az egyetemi adatok illetéktelen másolása, vagy a hitelessége, bizalmassága, sértetlensége egyéb módon sérül, stb.) az eszköz tulajdonosának gondatlanságából, vagy neki felróható módon (különösen: program frissítések kikapcsolása, az eszköz gondatlan tárolása, szállítása, stb.) következik be, az így okozott károkért teljes körű felelősséggel tartozik.
- A saját eszközön történő egyetemi feladatokkal kapcsolatos munkavégzéshez szükséges adatokat külön könyvtárban (könyvtár rendszerben) kell tárolni, amely kialakításához – kérés, szükség esetén - az ISZK szakemberei segítséget nyújtanak, illetve az eszközt érintő biztonsági esemény/incidens esetén az ISZK szakemberei részére hozzáférést kell biztosítani. Egyúttal ki kell jelölni az egyetemi Hálózatra történő mentések helyét.
- A munkahelyi célokra létrehozott könyvtárak egyetemi Hálózatra történő rendszeres mentésére fokozott figyelmet kell fordítani. A Hálózatra történő mentés a felhasználó kötelessége.
- A munkaviszony és a hozzáférési engedély megszüntetése után az egyetemi munkavégzéssel kapcsolatos adatokat, és az egyetemi licenszek alapján telepített programokat az eszközről visszaállíthatatlanul törölni kell, amit végezhet az ISZK illetékes szakembere, vagy az eszköz tulajdonosa, használója. A visszaállíthatatlan törlést végző személy írásos nyilatkozatot tesz a végrehajtásról.
- Az ilyen eszközök bármely célú (saját otthoni, vagy munkahelyi) használatánál az adatok biztonsága érdekében az Egyetem vonatkozó biztonsági előírásait kell érvényesíteni.

b) Időszakos rendezvényeken (különösen: konferenciákon, gyakorlatokon, stb.) külön erre a célra, az adott időtartamra létrehozott zónákban 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. Vitás esetekben az egyetemi érdekek elsőbbséget élveznek és a saját eszközök használatát – indokolt esetben – az egyetemi Hálózat biztonságának veszélyeztetése esetén - akár figyelmeztetés nélkül azonnal, más esetekben 24 órával korábban történt figyelmeztetés után, fel lehet függeszteni, meg lehet tiltani, akadályozni, vagy egyes hálózati szolgáltatások elérhetőségét korlátozni.

Felhőszolgáltatások igénybevétele

30. §

(1) Informatikai értelemben a felhő tulajdonképpen nem más, mint maga az internet vagy egy kommunikációs hálózat. Ezért a felhőalapú számítástechnika (angolul: cloud computing) az internet (vagy nagyobb cégek esetében a belső, intranet hálózat) felhasználásával nyújtott szolgáltatások összességét jelenti. Amikor egy cloud szolgáltatást igénybe vesz egy felhasználó, akkor a szolgáltatójának erőforrásait használja, miközben az adatai részben vagy teljes mértékben távoli adatközpontokban kerülnek eltárolásra, feldolgozásra. A felhőszolgáltatások újabb biztonsági kockázatokat jelentenek, amelyeket a használatuk során figyelembe kell venni.

(2) A felhőszolgáltatások igénybevétele legfőképpen magán célokra javasolt. Az egyetemi célú igénybevételét az ISZK nem támogatja, de az egyetemi Hálózatról történő elérését jelenleg nem is tiltja. Az Egyetem informatikai és kommunikációs Hálózatáról történő használatánál az alábbiakat kell figyelembe venni:

a) Bármely külső szolgáltató tárhely szolgáltatásának igénybevételénél az Egyetem - internet használatára vonatkozó - biztonsági rendszabályainak betartása kötelező.
b) Minősített adatok tárolása csak az arra rendszeresített számítógépek és hálózatok tárolóin engedélyezett. **Tilos** az Egyetem működése szempontjából érzékeny és bizalmas adatok külső szolgáltatónál történő tárolása. Csak a személyes és nyíltan hozzáférhető adatok külső tárolása engedélyezett.
c) A felhőszolgáltatók tárhely hozzáférése más személyekkel – különösen nem az egyetemen dolgozó munkatársakkal - történő megosztásainál figyelembe kell venni, hogy milyen jellegű adatokhoz férhet hozzá az illető személy, illetve a felhőszolgáltatáshoz való illetéktelen hozzáférés esetén milyen adatszivárgás, káresemény történhet.

Közösségi hálózatok

31. §

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

(2) Az Egyetem rendelkezik több internetes közösségi honlapon saját fórummal, amelyek az Egyetem életével kapcsolatos események hivatalos internetes megjelentetésére, véleményformálásra szolgálnak.

(3) Internetes közösségi és más nyilvános oldalakon történő megnyilatkozások esetében is figyelemmel kell lenni a személyes és közérdekű adatok védelmére és biztonságára vonatkozó jogszabályokban és más közjogi szervezetszabályozó eszközökben (különösen a hatályos NKE Etikai kódexben és a biztonsági szabályzatokban) meghatározottakra,

ugyanis ezek a megnyilatkozások nem csak a kinyilvánítójuk, hanem az Egyetem jó hírnevére is befolyással lehetnek és akár jogi következményekkel is járhatnak.

(4) Az Egyetem vezetése elvárja, hogy az Egyetem alkalmazottai és hallgatói megnyilatkozásaik folyamán személyes identitásukat nem elfedve képviseljék véleményüket, amelyért felelősséggel tartoznak. Az Egyetem tevékenységében esetlegesen meglévő hiányosságokat, a belső vitákat nem a nyilvános, hanem a belső fórumokon kell megvitatni. Tilos az Egyetemmel, a vezetésével, munkatársaival, hallgatóival kapcsolatosan az Egyetem alkalmazottaihoz, hallgatóihoz méltatlan (különösen valótlan, fenyegető, obszcén, vulgáris, stb.) vélemények nyilvános közlése. Az interneten megjelenő véleménynyilvánítások kapcsán minden megnyilatkozónak szem előtt kell tartania, hogy ami az interneten egyszer megjelenik, az a későbbiekben már nem, vagy csak rendkívüli erőfeszítésekkel törölhető.

Szoftverjogtisztaság, szoftverek telepítése, frissítése

32. §

(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 jogtiszta 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

33. §

(1) A számítógép számítógépes vírussal vagy más rosszindulatú programmal, történő fertőződése 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 – a vírusmentesítés és az ellenőrzések idejére, a fertőzés terjedésének megakadályozása érdekében - 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 elérhetetlensége esetén a munkaállomások vírusvédelmi rendszerének frissítése az interneten keresztül történhet.

Katasztrófakezelés, mentés, visszaállítás, szolgáltatásfolytonosság

34. §

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

V. FEJEZET

A VEZETŐ- ÉS TOVÁBBKÉPZÉSI INTÉZETRE VONATKOZÓ KÜLÖNÖS SZABÁLYOK

Az V. fejezet hatálya

35. §

(1) A VTKI esetében az informatikai és kommunikációs Hálózat üzemeltetése e fejezetben foglalt eltérésekkel történik.

(2) A VTKI Informatika fő tevékenysége a közszolgálati tisztviselők továbbképzéséről szóló 273/2012. számú kormányrendelet által előírt elektronikus továbbképzési rendszer, valamint a VTKI által bonyolított uniós programok informatikai fejlesztéseinek megvalósítása, az azokban létrejött informatikai rendszerek biztonságos és nagy rendelkezésre állású üzemeltetése, az ehhez szükséges fejlesztő és kiszolgáló személyzet informatikai igényeinek megvalósítása, valamint az ehhez tartozó beszerzések lebonyolítása.

(3) A VTKI tevékenységének támogatására szerződött partner az Apertus Nonprofit Kft., amelynek tulajdonosi jogait a Nemzeti Közszolgálati Egyetem gyakorolja. Jelen szabályozásban az Apertus Nonprofit Kft. tevékenységének azon része érintett, amely az egyetemi Hálózatban, illetve a VTKI tevékenységének támogatására kerül elvégzésre.

(4) A speciális szabályok célja e tevékenységekhez tartozó feladatok, folyamatok meghatározása.

(5) A VTKI Hálózata által nyújtott, a VTKI felhasználói által igénybe vehető informatikai és kommunikációs szolgáltatások körét az ISZK-t is érintő szolgáltatások esetében az ISZK igazgatójával történő előzetes egyeztetés alapján a VTKI Igazgatói Iroda informatikai és telekommunikációs feladatokat ellátó irodavezető-helyettese határozza meg.

(6) Jelen speciális szabályozás hatálya kiterjed a VTKI valamennyi szervezeti egységére, dolgozóira, az általa üzemeltetett belső támogató rendszerek felhasználóira, valamint a VTKI-val szerződéses viszony alapján állandó, vagy rendszeres munkavégzést folytató külső dolgozókra, illetve a VTKI (és az Egyetem) támogatására végzett feladatok körében a szerződéses partner cégek, így az Apertus Nonprofit Kft. munkatársaira is.

(7) Jelen fejezet hatálya a VTKI teljes számítástechnikai infrastruktúrájára kiterjed. Ez magába foglalja a VTKI használatában lévő valamennyi számítógépet (szerverek és személyi számítógépek), a perifériákat, a hálózati erőforrásokat és szolgáltatásokat, a szoftvereket, azok üzemeltetését, továbbá a mindezeken kezelt adatokat és információkat.

(8) A VTKI Informatikai Egység alatt a VTKI Igazgatói Iroda Informatikai és Telekommunikációs Egységét, valamint az ennek az egységnek a támogatására szerződött partnereket –, így az Apertus Nonprofit Kft.-t is – értjük. A VTKI Informatikai Vezetője ezen egység vezetője.

Feladatmegosztás az ISZK és VTKI között

36. §

(1) A VTKI által használt informatikai alapinfrastruktúra:

a) A VTKI működését biztosító informatikai rendszerek informatikai kiszolgálása és a VTKI tevékenységi körébe tartozó informatikai rendszerek üzemeltetése a VTKI felelősségi körébe tartozik.

b) Az egyetemi campusokon[3] az internet kapcsolat kialakítása az NKE által igénybevett szolgáltatón keresztül történik, a kapcsolattartás és meghibásodások kezelése az ISZK felelősségi körébe tartozik. Az egyetemi campusokon a hálózati, a vezeték nélküli hálózati és a kommunikációs hálózati infrastruktúra kialakítása az ISZK felelősségi körébe tartozik
c) Az egyetemi campusokon kívül[4] az internet kapcsolat, a hálózati, a vezeték nélküli hálózati és a kommunikációs hálózati infrastruktúra kialakítása a VTKI felelősségi körébe tartozik.
d) A VTKI IP telefónia (asztali telefonkészülékek) igényeinek ellátása az ISZK felelősségi körébe tartozik.
e) A VTKI használatában lévő, VTKI igényei szerint kialakított virtuális hálózati szegmens üzemeltetése, üzembiztosságának fenntartása az ISZK felelősségi körébe tartozik.
f) A VTKI használatában lévő virtuális hálózati szegmens folyamatos karbantartása, fejlesztése, a lehetőségek mértékében a felmerülő igényekhez igazítása, az új technikai lehetőségek alkalmazhatóságának megteremtése - a VTKI-val előzetesen egyeztetve - az ISZK felelősségi körébe tartozik.
g) A VTKI hálózati szegmens üzemzavarának esetében az ISZK köteles a hibaelhárítást a bejelentést követően haladéktalanul megkezdeni. Munkaszüneti nap esetében az azt követő első munkanap kezdetén köteles az ISZK a hibaelhárítást megkezdeni.

(2) Általános szabályok a VTKI által használt informatikai eszközökön:

a) A VTKI által használt informatikai eszközök működéséhez szükséges szoftverek beszerzése, telepítése és jogtisztasága a VTKI felelősségi körébe tartozik.
b) A VTKI által használt informatikai eszközök és adatok vírusvédelme a VTKI felelősségi körébe tartozik.
c) A VTKI által használt informatikai eszközök és szoftverek nyilvántartása a VTKI felelősségi körébe tartozik.

(3) A VTKI által fejlesztett és üzemeltetett informatikai rendszerek:

a) A VTKI 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 ISZK Igazgatójával történt előzetes egyeztetés után, és egyetértésével – a VTKI felelősségi körébe tartozik.
b) A VTKI 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 VTKI felelősségi körébe tartozik.
c) Speciális szaktudást igénylő feladatoknál külső informatikai szolgáltató igénybevétele a VTKI felelősségi körébe tartozik. Azokban az esetekben, amelyek befolyással lehetnek az ISZK felelősségi területeire, előzetes ISZK-VTKI megállapodás szükséges.

(4) A VTKI munkatársai, partnerei (felhasználói) által használt irodai és munkavégzéshez szükséges informatikai környezet:

[3] Érintett egyetemi campusok: Ludovika tér, Hungária krt, KTK kampusz Ménesi út, RTK kampusz Farkasvölgyi út, VTKI Kelenhegyi út, HHK Szolnok Kilián út-Repülőtér
[4] Egyetemi campuson kívül telephely jelen Szabályzat hatálybalépésekor: Mohai út/Petzvál u., Naphegy tér, Adyliget

a) A VTKI felhasználóinak az elektronikus levelezéssel kapcsolatos postafiókok, címek, hozzáférések biztosítása a VTKI felelősségi körébe tartozik. A VTKI felhasználói számára is mérvadóak és követendőek a jelen Szabályzat 27. §-ában megfogalmazott, az internet használatával és elektronikus levelezéssel kapcsolatos általános szabályok.
b) A VTKI saját Microsoft infrastruktúrájának üzemeltetése a VTKI felelősségi körébe tartozik.
c) A VTKI saját Microsoft infrastruktúráját használó (szerver és kliens) számítógépek támogatása a VTKI felelősségi körébe tartozik.
d) A VTKI felhasználók számára központi tárhelyet biztosítani, annak struktúráját, hozzáféréseit és jogosultsági szintjeit beállítani a VTKI felelősségi körébe tartozik.
e) A VTKI felelősségi körébe tartozó informatikai és hálózati erőforrások jogosultságainak szabályozása a VTKI felelősségi körébe tartozik. Az Egyetem informatikai Hálózatán való jogosultságok tekintetében - a VTKI felhasználók esetében is - a jelen Szabályzat 25. §-ában foglaltak követendőek.
f) A VTKI felhasználók személyi számítógépeinek (asztali és hordozható gépek) felkészítése, a napi munkához szükséges programok, programrendszerek telepítése és konfigurálása a VTKI felelősségi körébe tartozik. Az olyan esetekben, amelyek kapcsolódnak, és befolyásolhatják az ISZK területeit, előzetes ISZK-VTKI megállapodás szükséges.
g) A VTKI felhasználók számítógépein a helyi rendszergazdai jogosultságokról való döntés a VTKI felelősségi körébe tartozik.
h) A VTKI felhasználók saját tulajdonú, vagy más szervezet tulajdonát képező számítógépek Hálózatra kapcsolásnak engedélyezése – szükség esetén az ISZK Igazgatójával történt előzetes egyeztetés után, és egyetértésével – a VTKI felelősségi körébe tartozik.
i) A VTKI felhasználók számára a távoli munkavégzéshez (VPN kapcsolat) használt erőforrások biztosítása az ISZK felelősségi körébe tartozik.

(5) A VTKI által használt informatikai eszközök:

a) A VTKI használatában, kezelésében lévő informatikai eszközök beszerzése a VTKI felelősségi körébe tartozik.
b) A VTKI a belső igényeinek, tevékenységi körébe tartozó feladatainak, valamint uniós projektjeinek informatikai fejlesztéseit kiszolgáló szervereit az egyetem Hungária körúti szervertermében helyezi el, az őrzését az ISZK végzi, a szerverek biztonságos üzemeltetéséhez szükséges feltételeket az ISZK biztosítja, a szerverszobába történő bejutást az Üzemeltetési Szabályzat részletezi. A jelölt szerverpark üzemeltetése a VTKI felelősségi körébe tartozik.

(6) Szankciók alkalmazása a biztonsági előírásokat megsértő VTKI felhasználókkal szemben és a szankciókkal sújtott felhasználók haladéktalan tájékoztatása a VTKI felelősségi körébe tartozik. A foganatosított szankciókról, és a szankciókkal sújtott személyekről a VTKI Informatikai Vezetője haladéktalanul köteles írásban vagy e-mailben tájékoztatni az ISZK Igazgatóját.

(7) A VTKI felelősségi körébe tartozó feladatokkal kapcsolatos döntési, felelősségi és az azokra korlátozott belső szabályozási jogköröket a VTKI Informatikai Vezetője gyakorolja.

VTKI felhasználók kötelességei

37. §

A VTKI felhasználók kötelességei vonatkozásában a 9. §-ban megfogalmazottak a követendőek, azzal a kivétellel, hogy a VTKI felhasználói az informatikai eszközök és

Hálózat használata folyamán tapasztalt bármiféle meghibásodás, rendellenesség, a vonatkozó biztonsági szabályzatokban megfogalmazottak megsértése esetén elsőként a VTKI informatikusait, rendszergazdáit kell, hogy értesítsék. Az Egyetem informatikai és kommunikációs Hálózatával kapcsolatos hibaelhárítás folyamán az ISZK szakembereivel kell együttműködniük.

VI. FEJEZET

ZÁRÓ RENDELKEZÉSEK

38. §

(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 vonatkozó hatályos jogszabályokkal, valamint az Egyetem internetszolgáltatójának szabályaival, azok hatályosságát nem érinti. A Szabályzatban nem szabályozott kérdésekben a vonatkozó hatályos jogszabályok irányadók.

(3) A Szabályzatban foglaltak megsértése esetén a Szabályzat nem ismerete nem mentesít a jogkövetkezmények alól.

(4) Jelen Szabályzatot a Szenátus 31./2015. (II. 18.) számú határozatával fogadta el.

(5) A Szabályzat az elfogadását követő napon lép hatályba.

(6) A 92/2013. (VI. 5.) számú szenátusi határozattal elfogadott, 2013. június 6-án hatályba lépett Informatikai és kommunikációs hálózat használatára és üzemeltetésére vonatkozó szabályzat jelen Szabályzat hatálybalépésével egyidejűleg hatályát veszti.