MAGYAR TESTNEVELÉSI ÉS SPORTTUDOMÁNYI EGYETEM
BUDAPEST

Campus Főigazgató
Dr. Varga Dániel
1123 Budapest, Alkotás u. 42-48., K2, földszint
+36 70 902 0680
varga.daniel@tf.hu

Iktatószám: TE/CF/283/2024

A Magyar Testnevelési és Sporttudományi Egyetem
campus főigazgatójának
2024. évi 2. sz. rendelkezése
az Informatikai Biztonsági Szabályzatról

A Magyar Testnevelési és Sporttudományi Egyetem (a továbbiakban: Egyetem) Szervezeti és Működési Szabályzatának 1. rész (Szervezeti és Működési Rend) 64. § (4) bekezdése alapján – figyelemmel az információs önrendelkezési jogról és információszabadságról szóló 2011. évi CXII. törvény, valamint az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény vonatkozó rendelkezéseire – az informatikai rendszerkörnyezet üzemeltetésének, használatának, továbbá a megfelelő szintű informatikai biztonsági védelem biztosíthatóságának érdekében az alábbi rendelkezést adom ki:

1. §

Az Egyetem Informatikai Biztonsági Szabályzatát az 1. sz. melléklet tartalmazza.

2. §

Jelen rendelkezés 2024. július 22-én lép hatályba, egyúttal a Szenátus 4/2022. (I.27.) számú határozatával elfogadott és többször módosított Informatikai Biztonsági Szabályzat hatályát veszti. A jelen rendelkezésben nem szabályozott kérdésekben a vonatkozó hatályos jogszabályok az irányadók.

3. §

Jelen rendelkezés közzétételre kerül az Egyetem honlapján.

Budapest, 2024. július 19.

Dr. Varga Dániel
campus főigazgató

Magyar Testnevelési és Sporttudományi Egyetem
Campus Főigazgató
Budapest

1. sz. melléklet

MAGYAR TESTNEVELÉSI ÉS SPORTTUDOMÁNYI EGYETEM

Informatikai Biztonsági Szabályzat

2024.

TARTALOM

1. § A SZABÁLYZAT CÉLJA

(1) Az Egyetem Informatikai Biztonsági Szabályzatának (a továbbiakban: Szabályzat) alapvető célja, hogy az elérhető szolgáltatások használata és alkalmazása során biztosítsa az adatvédelem alkotmányos elveinek, az adatbiztonság és informatikai biztonság követelményeinek érvényesülését. Továbbá megfogalmazza az informatikai biztonság létrehozásával és működtetésével kapcsolatos alapelveket, feladatokat és meghatározza a kapcsolódó kötelezettségeket, illetve felelősségeket. Egyúttal célja olyan kontrollkörnyezet kialakítása, amely detektálja és megakadályozza a jogosulatlan hozzáférést, az adatok jogosulatlan megváltoztatását és nyilvánosságra hozatalát. Az Egyetemen működő informatikai rendszerekre specializálva a megelőző kontrollok alkalmazásával csökkenti az informatikai biztonsági kockázatok bekövetkezésének valószínűségét. A Szabályzat további célja, hogy elősegítse 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. § A SZABÁLYZAT HATÁLYA

(1) A szabályzat hatálya kiterjed az Egyetem hálózatát használó felhasználókra és rendszergazdákra, továbbá az informatikai rendszerkörnyezet infrastruktúrájára, azaz a fizikai, infrastrukturális eszközökön kívül az adatok, szoftverek teljes körére, az informatikai biztonsággal összefüggő folyamatokra és feladatokra, az Egyetem teljes területén. Felhasználónak minősülnek az Egyetem foglalkoztatottjai, hallgatói, valamint mindazok, akik oktatási, kutatási, tudományos, adminisztrációs és egyéb feladataikhoz állandó vagy eseti jelleggel, illetve egyéb jogviszony alapján az Egyetem hálózatát használják, beleértve az informatikai rendszerkörnyezet fenntartásáért felelős szolgáltatókat is. A felhasználók különböző jogosultságokkal és kötelezettségekkel rendelkezhetnek.

(2) A TF Gyakorló Sportiskolai Általános Iskola és Gimnáziumra (a továbbiakban: Gyakorló Iskola) vonatkozó különös szabályok az V. fejezetben kerülnek meghatározásra. A Gyakorló Iskolára vonatkozó különös szabályok hatálya kiterjed a Gyakorló Iskola valamennyi szervezeti egységére, foglalkoztatottjára, az általa

üzemeltetett belső támogató rendszerek felhasználóira, adataira, továbbá a Gyakorló Iskola teljes informatikai infrastruktúrájára.

3. § A SZABÁLYZAT FELÉPÍTÉSE

(1) A Szabályzat az informatikai és információbiztonságra vonatkozó szabályozás általános kereteit határozza meg, ahhoz további, kontrollpontokat részletező eljárásrendek tartoznak az alábbiak szerint:

1. Logikai hozzáférési Eljárásrend
2. Incidens és biztonsági eseménykezelési Eljárásrend
3. Mentési és archiválási Eljárásrend
4. Működésfolytonossági és katasztrófa elhárítási Eljárásend

4. § ÉRTELMEZŐ RENDELKEZÉSEK

1. **Adatbiztonság**: Az adatok jogosulatlan megszerzése, módosítása és tönkretétele elleni műszaki és szervezési intézkedések, illetve eljárások együttes rendszere.
2. **Adatfeldolgozás**: Az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől feltéve, hogy a technikai feladatot az adatokon végzik.
3. **Adatgazda**: Felelős az általa kezelt adatokért, továbbá jogosult az adatok minősítésének vagy osztályba sorolásának elvégzésére.
4. **Adatkezelés**: Az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése, megsemmisítése, valamint az adatok további felhasználásának megakadályozása, az adatokkal kapcsolatos fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők rögzítése.
5. **Adatkezelő**: Az a személy, aki vagy amely önállóan vagy másokkal együtt az adatok kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az általa megbízott adatfeldolgozóval végrehajtatja.

6. **Adatátviteli hálózat**: Felhasználói számítógépek, illetve szerverek közötti adatátvitelt biztosító passzív elemekből és aktív eszközökből álló infrastruktúra.
7. **Adatvédelem**: Az informatikai/információs rendszerek adatvesztés elleni védelmének, valamint az adatok folyamatos rendelkezésre állását biztosító szabályzatoknak, folyamatoknak és megoldásoknak az együttes rendszere.
8. **Aktív hálózati eszköz**: Kapcsolók (switch-ek), forgalomirányítók (router-ek), vezeték nélküli hozzáférési pontok (Acces Pointok) és egyéb eszközök, amelyek segítségével a hálózat folyamatos üzemvitele biztosítható.
9. **Bizalmasság**: Az információ azon jellemzője, hogy csak egy előre meghatározott felhasználói kör (jogosultak) részére hozzáférhető, mindenki más számára titok. A bizalmasság elvesztése esetén a bizalmas információ arra jogosulatlanok számára is ismertté, hozzáférhetővé válik.
10. **Biztonság**: Az informatikai rendszerekben olyan előírások és szabványok betartását jelenti, amelyek a rendszer működőképességét, az információk rendelkezésre állását, sértetlenségét, bizalmasságát és hitelességét erősítik.
11. **BYOD (Bring Your Own Device – BYOD):** Saját mobileszközök (különösen: notebookok, tabletek, okos telefonok) munkahelyi környezetben való használata.
16. **Felhasználó**: Az a természetes személy, aki az egyetemi informatikai infrastruktúrát használja.
17. **Felhasználói azonosító**: Az egyetemi címtárban tárolt egyedi azonosításra szolgáló rövid karaktersorozat, amely általában a felhasználó teljes nevéből képződik, a hallgatók esetében ide tartozik a NEPTUN kód is.
18. **Domain név**: tartománynév (műszaki azonosító), amely elsősorban a könnyebb megjegyezhetősége miatt, az internetes kommunikációhoz nélkülözhetetlen Internet cím tartományok (IP címek) helyett használatos. Az Internet egy meghatározott részét, tartományát egyedileg leíró megnevezés, a számítógépek (kiszolgálók) azonosítására szolgáló névtartomány (különösen: tf.hu).
19. **DNS (Domain Name System)**: Az internet neveket és címeket egymáshoz rendelő adatbázisa, amely általában külön kiszolgáló gépen fut.
20. **Felhőszolgáltatás, felhőszolgáltató:** A feladatvégzéshez használt adatállományok, programok, szolgáltatások, stb. fizikailag nem a felhasználó számítógépén, hanem az interneten, egy szolgáltatónál találhatók. Az adatok (e-mailek, címjegyzékek, naptárbejegyzések és kedvenc linkek) felhőben való

tárolásának előnye, hogy bárhonnan könnyen elérhetők és akkor sem vesznek el, ha a felhasználó számítógépe használhatatlanná válik.

21. **Hálózati tűzfal**: Olyan kiszolgáló eszköz (számítógép vagy program), amelyet a lokális és a külső hálózat közé, a csatlakozási pontra telepítenek annak érdekében, hogy az illetéktelen behatolásokat megakadályozzák. Ezzel együtt lehetővé teszi a kifelé irányuló forgalom, tartalom ellenőrzését is.
22. **Információbiztonság:** Az információbiztonság az információ bizalmasságának, sértetlenségének és rendelkezésre állásának megőrzése. A hozzá kapcsolódó intézkedések alatt pedig az adatok sérülése, megsemmisülése, jogosulatlan megszerzése, módosítása és tönkretétele elleni műszaki és szervezési intézkedések és eljárások együttesét értjük.
23. **Központi címtár**: Az Egyetem foglalkoztatottjainak felhasználói adatait tároló adatbázis.
24. **Közérdekű adat**: Az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv, vagy személy kezelésében lévő és tevékenységére vonatkozó vagy közfeladatának ellátásával összefüggésben keletkezett, a személyes adat fogalma alá nem eső, bármilyen módon vagy formában rögzített információ vagy ismeret, függetlenül kezelésének módjától, önálló vagy gyűjteményes jellegétől. Így különösen a hatáskörre, illetékességre, szervezeti felépítésre, szakmai tevékenységre, annak eredményességére is kiterjedő értékelésére, a birtokolt adatfajtákra, és a működést szabályozó jogszabályokra, valamint a gazdálkodásra, a megkötött szerződésekre vonatkozó adat.
25. **Közérdekből nyilvános adat**: A közérdekű adat fogalma alá nem tartozó minden olyan adat, amelynek nyilvánosságra hozatalát, megismerhetőségét vagy hozzáférhetővé tételét törvény közérdekből elrendeli.
26. **Megtévesztés (Social engineering)**: az emberek bizalomra való hajlamának manipulatív kihasználása, információgyűjtés számítógépes rendszerekbe történő behatolás érdekében.
27. **Mobil eszközök**: Notebook, tablet, mobiltelefon, stb.
28. **Munkaállomás**: A felhasználó rendelkezésére bocsátott számítástechnikai eszköz, amely alapvetően hordozható vagy asztali számítógépből és a hozzá tartozó kiegészítőkből, illetve más, a hálózathoz vagy a munkaállomáshoz

csatlakoztatható számítástechnikai eszközökből (különösen: mikrofon, kamera, scanner, tablet, telefon stb.) állhat.

29. **NEPTUN kód**: A NEPTUN rendszer szolgáltatásaihoz hozzáférést biztosító betűkből és számokból álló, legalább 6 karakter hosszúságú kód.
34. **Passzív eszközök**: Hálózati kábelezés, rendezők és csatlakozók.
35. **Rendelkezésre állás**: Annak biztosítása, hogy a szükséges információ a szükséges időben az arra jogosultak számára meghatározott formában hozzáférhető és elérhető legyen.
36. **Szerverhelyiség**: Fokozottan védett, naplózott bejutású, klimatizált, zárt helyiség, ahol a folyamatos működés feltételei az informatikai erőforrások számára biztosítottak.
37. **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 korlátozódjon az esetleges kár.
38. **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).
39. **WEB adminisztrátor**: Az Egyetem honlapjának felügyeletét ellátó személy.
40. **WiFi, WLAN**: Szabványos vezeték nélküli adatátviteli technika.

I. FEJEZET AZ EGYETEM INFORMATIKAI RENDSZEREINEK HASZNÁLATA

5. § ALAPVETŐ SZABÁLYOK

(1) Az Egyetem informatikai rendszereit és szolgáltatásait csak a hatályos jogszabályokban és a vonatkozó szabályozókban foglaltak szerint lehet használni. Az eszközöket és szolgáltatásokat **TILOS** használni az alábbi tevékenységekre, illetve ilyen tevékenységekre irányuló próbálkozásokra, kísérletekre:

a) A mindenkor hatályos magyar jogszabályokba ütköző, büntetőjogi következményekkel járó cselekmények előkészítése vagy végrehajtása, mások személyiségi jogainak megsértése, tiltott haszonszerzésre irányuló tevékenység, szerzői jogok megsértése (különösen: szoftver és médiatartalom nem jogszerű megszerzése, tárolása, terjesztése);

b) Másokra nézve sértő, vallási, etnikai, politikai vagy más jellegű érzékenységet bántó, zaklató tevékenység (különösen: pornográf, pedofil anyagok közzététele);

c) Az informatikai erőforrások, szolgáltatások olyan célra való használata, amely az erőforrás vagy a szolgáltatás eredeti céljától idegen (különösen: hírcsoportokba/levelezési listákra a csoport vagy lista témájához nem tartozó üzenet küldése);

d) Profitszerzést célzó, direkt üzleti célú tevékenység és reklámtevékenység;

e) Mások munkájának zavarása vagy akadályozása (különösen: kéretlen levelek, hirdetések küldése);

f) A hálózati erőforrások magáncélra való túlzott mértékű használata;

g) Az informatikai adathálózatot, a kapcsolódó hálózatokat, illetve erőforrásaikat indokolatlanul, túlzott mértékben, pazarló módon igénybevevő tevékenység (különösen: hálózati játékok, torrent, kriptobányászat, streaming tevékenység, illegális tartalmak hostolása);

h) Az informatikai rendszerek és szolgáltatások rendeltetésszerű működését és biztonságát megzavaró, veszélyeztető tevékenység, ilyen információknak és programoknak a terjesztése;

i) Az informatikai rendszereken és szolgáltatásokon keresztül elérhető adatokhoz történő illetéktelen és jogosulatlan hozzáférés, azok illetéktelen használata vagy kompromittálása; egyetemi informatikai eszközök vagy szolgáltatások sérülékenységének illetéktelen és szisztematikus tesztelése vagy azzal történő visszaélés;

j) Az informatikai rendszereken és szolgáltatásokon keresztül elérhető adatoknak illetéktelen módosítására, megrongálására, megsemmisítésére vagy bármely károkozásra irányuló tevékenység folytatása;

k) Az informatikai rendszerkörnyezet bármely szolgáltatásának szándékos, vagy hiányos ismeretekből, nem megfelelő körültekintéssel végzett beavatkozásokból fakadó zavarása, illetve részleges vagy teljes bénítása.

6. § KÖZPONTI SZOLGÁLTATÁSOK AZ INFORMATIKAI HÁLÓZATON

(1) Az Egyetem által biztosított informatikai szolgáltatások:

a) Vezetékes és vezeték nélküli internet hozzáférés;

b) Központi címtárszolgáltatás;

c) Elektronikus levelezés (belső hálózati és távoli hozzáféréssel);

d) Az egyetem on-line megjelenését biztosító weboldalak és webes szolgáltatások;

e) Jelszavas hozzáférés szabályozáson alapuló, védett adattároló területek a közös munkavégzéshez a központi szervereken;

f) Távoli munkavégzés biztosítása biztonságos adatkapcsolaton keresztül;

g) Központi nyomtatási szolgáltatás;

h) Központi vírusvédelmi, spamszűrési, tűzfalas és egyéb védelmi szolgáltatások;

i) Az Egyetem oktatási tevékenységéhez kapcsolódó audiovizuális, e-learning és kollaborációs szolgáltatások;

j) Az Egyetem adminisztrációs működtetését kiszolgáló ügyviteli rendszerek működésének biztosítása.

7. § AZ INFORMATIKAI IRODA FELADATAI ÉS KÖTELEZETTSÉGEI

(1) Az Informatikai Iroda feladata:

a) az oktatást, a tudományos kutatást, valamint az Egyetem működését biztosító valamennyi rendszer informatikai kiszolgálása, a belső hálózati szolgáltatásokat, valamint az Egyetem internetes megjelenését, kapcsolattartását biztosító informatikai rendszerkörnyezet folyamatos üzemeltetése;

b) a kiszolgáló informatikai rendszerek üzembiztosságának fenntartása, a Szabályzat, valamint az informatikai működéssel kapcsolatos hatályos szabályzók betartása és betartatása;

c) az informatikai rendszerkörnyezet karbantartása, fejlesztése, a felmerülő igényekhez történő igazítása, valamint az újabb technikai lehetőségek alkalmazhatóságának megteremtése;

d) az új informatikai és kommunikációs eszközök, rendszerek szolgáltatásainak rendszerbe illeszthetőségének vizsgálata, a vonatkozó döntések meghozatalának előkészítése az alkalmazhatóságukról és gondoskodás a megvalósításról;

e) a felhasználók részéről felmerülő igények elemzése, rangsorolása és javaslattétel a döntéselőkészítésben;

f) a felhasználók személyi számítógépeinek (asztali és hordozható) felkészítése, a napi munkához szükséges programok, programrendszerek telepítése és konfigurálása, működési zavar, meghibásodás, rendellenes működés esetén a hibaelhárítás;

g) az Egyetem által nyújtott informatikai szolgáltatások részleges vagy teljes korlátozása, valamint indokolt esetben a megfelelő (fegyelmi, etikai, stb.) eljárás kezdeményezése a biztonsági előírásokat megsértő felhasználókkal szemben foglalkoztatottak esetén közvetlen munkahelyi vezetőik, hallgatók esetén tanulmányi ügyintézőik egyidejű tájékoztatása mellett. Az intézkedéssel szemben a hallgató a Tanulmányi Hivatal vezetőjénél, a foglalkoztatott a közvetlen munkahelyi vezetőjénél élhet panasszal;

h) az informatikai és kommunikációs rendszerek esetében a jogszabályokban, valamint az Egyetem Adatvédelmi és adatbiztonsági Szabályzatban meghatározott adatok, nyilvántartások, naplók vezetése és célhoz kötött kezelése, amelyeket meghatározott esetekben, a vonatkozó jogszabályoknak megfelelő adatvédelmi vagy büntetőjogi eljáráshoz kapcsolódó megkeresés alapján az illetékes hatóságoknak kiszolgáltathat;

j) az informatikai rendszerkörnyezet működéséhez, karbantartásához időközönként szükséges, előre tervezhető üzemszünetek, leállások előzetes egyeztetése, az érintettek értesítése, valamint a publikusan elérhető szolgáltatások részleges vagy teljes kiesése esetén tájékoztató információ elhelyezése;

k) biztonságtudatosító és központilag nyújtott szolgáltatások általános vagy speciális használatához kapcsolódó felhasználói oktatóanyagok, leírások, dokumentációk készítése és elérhetővé tétele;

l) a szervezeti egységek vezetői által meghatározott, adatvédelmi vagy információbiztonsági szempontból kritikus adatokat (különösen: tanulmányi, személyügyi, pénzügyi, ügyviteli információkat) tároló munkaállomások számára védett hálózati szegmens biztosítása;

m) információbiztonsági és adatvédelmi incidensek kivizsgálása, valamint megelőző, monitorozó és korrektív tevékenységek végzése az incidensek előfordulásának csökkentése érdekében.

8. § AZ INFORMATIKAI IRODAVEZETŐ INFORMATIKAI BIZTONSÁGGAL ÖSSZEFÜGGŐ JOGAI

(1) Az Informatikai Irodavezető informatikai biztonsággal összefüggő feladatai esetében jogosult:

a) az Egyetem által nyújtott szolgáltatások körének, az egyes szolgáltatások igénybe vételi feltételeinek meghatározására. Az informatikai biztonság érdekében bármely szolgáltatás használatát felhasználói azonosításhoz kötheti;

b) az informatikai rendszerek és kezelt adatok biztonsága érdekében a Szabályzat előírásait megsértő felhasználók hozzáférési jogosultságait szűkíteni, korlátozni vagy esetlegesen kizárni a szolgáltatások igénybevételéből;

c) az Egyetem biztonságos működését veszélyeztető vagy zavaró munkaállomásokat, kommunikációs és más berendezéseket, eszközöket – informatikai adathálózatról történő – előzetes értesítés nélkül leválasztani, valamint intézkedni a zavar, illetve veszélyhelyzet megszüntetése érdekében.

9. § A FELHASZNÁLÓK JOGAI

(1) A hálózat használata során a felhasználó jogosult:

a) a munkavégzéshez szükséges programokkal ellátott, egy vagy több személy használatára beállított, felkészített számítógép, kommunikációs eszközök használatára;

b) a munkavégzéshez szükséges mértékben – a használatra vonatkozó, a felhasználó által elfogadott (és aláírással igazolt) feltételek mellett – a hálózati szolgáltatások igénybevételére;

c) működési zavar, meghibásodás, rendellenes működés esetén segítséget kérni;

d) a munkavégzéshez szükségesnek ítélt eszközök, szoftverek beszerzését, telepítését igényelni (az igény jogosságát a szervezeti egység vezetőjével együttműködve az Informatikai Iroda bírálja el);

e) levelező szolgáltatás és az Egyetem által biztosított elektronikus postafiók használatára (az Informatikai Iroda a felhasználói fiókot az Egyetem rendszerén belül előretelepített kliens programmal, illetve web felületen teszi elérhetővé);

f) az informatikai rendszerek és szolgáltatások tekintetében az Informatikai Iroda munkatársai részéről a személyhez fűződő jogainak tiszteletben tartására, amelytől eltérni kizárólag belső adatvédelmi szabályozás vagy jogszabály által meghatározott esetekben lehet;

g) tájékoztatásra az informatikai rendszereket és szolgáltatásokat érintő újdonságokról, frissítésekről, karbantartási vagy leállási eseményekről, továbbá az esetlegesen vele szemben az Egyetem által nyújtott szolgáltatások korlátozásáról vagy biztonsági incidensből fakadó eljárás lefolytatásáról;

h) a felhasználókra vonatkozó szabályokat megismerni.

10. § A FELHASZNÁLÓK KÖTELESSÉGEI

(1) Az informatikai rendszerek és szolgáltatások biztonságos használata érdekében a felhasználó köteles:

a) meghibásodás, üzemzavar észlelésekor, vírusfertőzés vagy annak gyanúja esetén haladéktalanul értesíteni az Informatikai Irodát a helpdesk@tf.hu e-mail címen, valamint a számítógép további használatát az Informatikai Iroda intézkedéséig felfüggeszteni. A hibaelhárítás folyamán az Informatikai Irodával együttműködni, számukra a szükséges információkat megadni;

b) adatvédelmi vagy információbiztonsági incidensek előfordulása esetén haladéktalanul értesíteni az Informatikai Irodát és az érintett szervezeti egység vezetőjét;

c) a jelen Szabályzatot megismerni, az abban foglaltakat betartani, valamint együttműködni az Informatikai Iroda munkatársaival a Szabályzat rendelkezéseinek betartatása érdekében;

d) az informatikai rendszereket és szolgáltatásokat annak céljaival megegyezően használni;

e) az informatikai hálózaton csak a számára engedélyezett erőforrásokat használni;

f) tevékenységével az egyetemi informatikai hálózaton feladataikat végzők tevékenységét nem zavarni, akadályozni, veszélyeztetni;

g) az informatikai szolgáltatások igénybevételéhez használatos jelszavait titkosan kezelni, azokat előírt gyakorisággal változtatni, a Szabályzat jelszóhasználattal kapcsolatos előírásait betartani (TILOS a hozzáférési jogosultságok, jelszavak átruházása, mások jelszavának használata, a hálózat, a levelezőrendszer – a tulajdonos felhatalmazása nélkül – más nevében történő igénybevétele);

h) gondoskodni adatainak tőle elvárható védelméről és az Egyetem által biztosított védelmi szolgáltatások aktívan tartásáról;

i) az informatikai szolgáltatások, a távfelügyeleti rendszerek működéséhez szükséges programok telepítését lehetővé tenni;

j) a számára biztosított informatikai és kommunikációs eszközöket működőképes állapotban megőrizni, ellenőrzéskor kérésre bemutatni, a jogviszony megszűnésekor visszaszolgáltatni és az eredeti/átvételkori állapotot visszaállítani. A felhasználó a részére biztosított eszközöket, berendezéseket nem bonthatja meg. A hardver és szoftverkörnyezetet – beleértve a számítógépes vírusellenőrzéssel és vírusirtással kapcsolatos szoftvereket is – nem vagy csak az Informatikai Iroda külön engedélyével módosíthatja, az eszközök hálózati és egyéb beállításaiban működést befolyásoló módosításokat nem végezhet.

k) felelősséget vállalni az Egyetem tulajdonát képező informatikai, kommunikációs eszközökben vagy eszközökkel okozott szabályellenes cselekedetekért, károkért;

l) USB memóriakulcsok vagy más külső adathordozók csatlakoztatása után az Informatikai Iroda által biztosított számítógépes vírusellenőrző eszközökkel a vírusellenőrzést, vírusirtást végrehajtani;

m) az Egyetem által biztosított informatikai szolgáltatások esetében, különösen az egyetemi levelező rendszerben és a telefonkönyvben tárolt adataiban (különösen: név, szervezeti egység, beosztás, munkahelyi telefonszám, iroda) történt

változásokat (különösen: névváltozás, más szervezeti egységhez történt áthelyezés, telefonszám változás) az Informatikai Irodánál bejelenteni.

11. § A MEG NEM ENGEDETT TEVÉKENYSÉGEK

(1) A szabályzat súlyos megsértésének gyanúja vagy információbiztonsági incidens esetén a cselekményt ki kell vizsgálni és javaslatot kell tenni a szükséges intézkedésekre az alábbiak szerint:

a) A szabályzat gondatlan megszegése esetén az érintett felhasználót figyelmeztetni kell.

b) Gondatlanságból adódó információbiztonsági incidens esetén fegyelmi eljárást kell indítani.

c) A szabályzat szándékos megsértése vagy fegyelmi eljárás esetén az érintett felhasználó az informatikai szolgáltatások használatából ideiglenesen vagy véglegesen kizárható, és az eset súlyosságától függően eljárás lefolytatása kezdeményezhető ellene. Az informatikai szolgáltatásokat csak az eljárás lefolytatása után és annak eredményétől függően veheti újra igénybe.

(2) Amennyiben a jelen § szerinti meg nem engedett tevékenységekből következően anyagi kár keletkezett, az érintett felhasználót annak megtérítésére kell kötelezni a vonatkozó jogszabályok vagy egyetemi szabályzatok alapján.

12. § AZ EGYETEMI INFORMATIKAI ADATHÁLÓZAT ÜZEMELTETÉSE, ÉPÍTÉSE ÉS BŐVÍTÉSE

(1) Kizárólag az Informatikai Iroda jogosult az informatikai (vezetékes vagy vezeték nélküli) adathálózat bővítésére, átalakítására. Az informatikai adathálózatot a lehetőségeket figyelembe véve az Informatikai Iroda az igényeknek megfelelően folyamatosan bővíti és karbantartja. Hálózat vagy hálózatrész építése, módosítása, valamint az Egyetem rendszerén kívüli szolgáltatásokhoz, hálózatokhoz állandó kapcsolat (különösen: site-to-site VPN) létesítése külső erőforrások bevonása esetében is csak az Informatikai Iroda engedélyével és közreműködésével történhet. Arra jogosultsággal nem rendelkező személy a kialakított rendszeren nem változtathat, végpontot nem helyezhet át, aktív vagy szerver-feladatokat ellátó eszközt a hálózatra nem kapcsolhat rá és arról nem kapcsolhat le.

13. § AZ EGYETEMI INFORMATIKAI ADATHÁLÓZAT HASZNÁLATÁNAK SZABÁLYAI

Az informatikai adathálózat használata során az alábbi rendelkezéseket szükséges betartani:

a) Új hálózatrészek építésének tervezését, kivitelezését, a már megépült hálózatrészek módosítását csak az Informatikai Iroda vagy annak felügyeletével az Egyetem által megbízott kivitelező végezheti.

b) Hálózati aktív eszközöket (switch, router, tűzfal) csak az Informatikai Iroda csatlakoztathat a hálózatra vagy köthet le arról. Az aktív eszközök kapcsolatainak megbontására és az eszközök bármilyen konfigurálására csak az Informatikai Iroda jogosult.

c) Az informatikai adathálózatra idegen, nem az Egyetem által biztosított informatikai berendezést fizikailag csak az Informatikai Iroda engedélyével lehet csatlakoztatni. Ha az eszköz adattárolásra is alkalmas, akkor annak előzetes vírusmentestését kötelező elvégezni. Az adatok tárolására vonatkozó jelen és más vonatkozó egyetemi szabályzatok és előírások betartására különös figyelmet kell fordítani.

d) Az Informatikai Iroda az engedély kiadását megtagadhatja, ha a csatlakoztatni kívánt berendezés az informatikai adathálózat működését, rendeltetésszerű használatát, működési vagy adatvédelmi biztonságát (a továbbiakban: hálózati biztonság) veszélyeztetné.

e) Saját személyi számítógép egyetemi munkavégzés céljából az Egyetem által nyújtott belső szolgáltatások elérésére csak az Informatikai Irodának történő előzetes bejelentés, a gépek alapvető paramétereinek és felhasználójának nyilvántartásba vétele után, az Informatikai Iroda által megszabott feltételekkel használható, kivéve az „f” pontban meghatározott eseteket.

f) Időszakos rendezvények (különösen: konferenciák, gyakorlatok vagy más események) idején az Egyetem területén működő vezeték nélküli internet szolgáltatást az Informatikai Iroda által meghatározott feltételekkel (ideiglenes wifi szegmensek kialakításával), be nem jelentett számítógépekkel is igénybe lehet venni, de csak vendéghálózaton az Egyetem informatikai eszközeinek és szolgáltatásainak kizárása mellett. A használathoz szükséges hitelesítés

módszertanát az Informatikai Iroda határozza meg és teszi közzé az esemény idejére.

g) A belső 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.

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 Informatikai Iroda vagy az Egyetem által szerződött kivitelezők/karbantartók végezhetik az Informatikai Iroda szakmai felügyelete mellett. Minden más esetben a feszültségmentesítést a hatóság (tűzoltóság, katasztrófavédelem) végzi el.

14. § AZ EGYETEMI INFORMATIKAI ADATHÁLÓZAT HIBAELHÁRÍTÁSÁNAK SZABÁLYAI

Az informatikai adathálózat bármilyen jellegű meghibásodása esetén a hiba elhárítását az Informatikai Iroda a lehető leghamarabb, de legkésőbb a bejelentést követő első munkanapon megkezdi. Abban az esetben, ha a hiba elhárításához külső segítség szükséges vagy a hiba oka a hálózaton kívül keletkezett, akkor a hibát bejelenteni, elhárítására intézkedni, a javítást megrendelni az Informatikai Iroda jogosult.

II. FEJEZET AZ INFORMATIKAI SZOFTVEREK ÜZEMELTETÉSE

15. § TÁMOGATOTT PROTOKOLLOK

Az Informatikai Iroda az egyes protokollok, portok, illetve az ezeket használó alkalmazások használatát a működési stabilitás, valamint az adat- és információbiztonság érdekében időlegesen vagy véglegesen, VLAN-onként, helyszínenként vagy az Egyetem teljes hálózatára kiterjedő hatállyal korlátozhatja vagy megtilthatja, amennyiben az informatikai eszközök és szolgáltatások használata és működtetése esetén incidenst tapasztal.

16. § KRITIKUS ADATOKAT TARTALMAZÓ SZÁMÍTÓGÉPEK HASZNÁLATA

Az adatvédelmi szempontból kritikus adatokat (különösen: tanulmányi, személyügyi, pénzügyi, ügyviteli információkat) tároló számítógépek fizikai és logikai védelmére fokozott figyelmet kell fordítani és a belépéshez lehetőség szerint többfaktoros azonosítást kell alkalmazni. Ezen gépek körét az érintett szervezeti egységek vezetői határozzák meg.

17. § SZEMÉLYI SZÁMÍTÓGÉPEK FELKÉSZÍTÉSE A HASZNÁLATRA

(1) Az egyes hálózati szolgáltatások igénybevételére használható, illetve a technikai segítségnyújtással támogatott programok körét az Informatikai Iroda a telepítési protokollban határozza meg.

(2) A munkavégzésre kijelölt számítógépeken – az első hálózatra kapcsolás előtt – az előzetes ellenőrzést, a használathoz előírt programok telepítését, a feladatra történő felkészítést, valamint a személyre szabást az Informatikai Iroda hajtja végre.

(3) Az Informatikai Iroda a számítógépeket a telepítési protokoll szerint leltárba véve és a felhasználó nevére kiadva, előre telepített operációs rendszerrel, irodai programcsomaggal, vírusvédelmi szoftverrel és a hálózati szolgáltatások igénybevételére alkalmas programokkal, személyre szólóan felkészítve adja át.

(4) A számítógép hálózati beállításainak, rendszerelemeinek módosítására, az operációs rendszer és a gépre feltelepített alapszoftverek konfigurációjának megváltoztatására, szükség szerinti újratelepítésére vagy új programok telepítésére kizárólag az Informatikai Iroda jogosult.

(5) A felhasználó részére átadott munkaállomás a névre szóló felkészítés után más felhasználónak nem adható át. A jogviszony vagy az eszköz szükségességének megszűnése esetén az eszközt minden esetben le kell adni az Informatikai Iroda részére a felhasználói jogosultságok megszüntetésével együtt, amit a felhasználó közvetlen munkahelyi vezetője kezdeményez. Az Informatikai Iroda a munkaállomást más felhasználó részére csak teljes újratelepítést és személyre szabást követően adhatja ki.

18. § SZERVEREK ÜZEMELTETÉSE

(1) Az Egyetem által üzemeltetett számítógépeken kívül szerverek, informatikai szolgáltatások elindítása, ilyen szolgáltatást nyújtó számítógépek adathálózatra kapcsolása szigorúan tilos.

(2) Az Egyetem szervereinek felügyelete – beleértve az operációs rendszerek karbantartását, frissítését is – az Informatikai Iroda és az Egyetem ezen feladatok ellátásra szerződött partnereinek feladata.

(3) Az Egyetem szerverein futó alkalmazásokat, adatbázis rendszereket megfelelő módon, rendszeresen frissíteni szükséges, valamint gondoskodni kell az operációs rendszerek, alkalmazások verziófrissítéséről. Abban az esetben, ha az alkalmazásgazda nem gondoskodik az alkalmazáskörnyezet megfelelő frissítéséről és emiatt annak egyetemi rendszereken történő futtatása biztonsági kockázatot jelent, az Informatikai Iroda az alkalmazásgazda tájékoztatását követően az adott szolgáltatást ideiglenesen vagy véglegesen lekapcsolhatja.

19. § TÁVOLI MUNKAVÉGZÉS

(1) Az Informatikai Iroda a szervezeti egységek vezetőinek javaslata alapján lehetővé teszi a kijelölt felhasználók részére az informatikai szolgáltatások távoli elérését. A távoli munkavégzés során is be kell tartani a jelen Szabályzat előírásait, különös tekintettel az illetéktelen hozzáférés megakadályozására. A távoli hozzáférés esetében kötelező biztonsági követelmény, hogy a hitelesítés során használt jelszót és az adatforgalmat titkosítani szükséges.

(2) A távoli munkavégzés során VPN szolgáltatás segítségével csatlakoztatott eszközök fokozott védelme és az illetéktelen hozzáférés megakadályozása érdekében a felhasználó köteles az Informatikai Iroda iránymutatásait betartani.

(3) A VPN kapcsolat felépítését követően szigorúan tilos szoftvert letölteni és installálni, torrent vagy engedély nélküli ftp letöltést/megosztást indítani, kártékony kódot tartalmazó weboldalt megnyitni, internetes játékokat használni és az Egyetem által biztosított vagy külső informatikai szolgáltatások ellen bármilyen manipulációt végezni.

(4) Amennyiben a felhasználónak kiadott munkaállomással kapcsolatban a felhasználó bármilyen gyanús vagy szokatlan működést tapasztal, a VPN segítségével felépített adatkapcsolatot meg kell szüntetni és kérni kell az Informatikai Iroda segítségét.

20. § ADATOK ELHELYEZÉSÉNEK SZABÁLYAI A HÁLÓZATON

(1) Az Informatikai Iroda a több felhasználó által közösen használt adatok biztonságos, illetéktelen hozzáféréstől védett elhelyezésére a szervereken szükség szerint tárhelyet biztosít. A tárterülethez történő hozzáférés beállítása az adatokért felelős szervezeti egység vezetőjének írásos igénye alapján, az Informatikai Iroda részére küldött elektronikus üzenet formájában történik.

(2) A felhasználók a munkavégzésükkel kapcsolatban keletkezett adatokat a hálózati szervereken a számukra kijelölt mappákban helyezhetik el, amelyekről központi mentés készül. Ez a tárterület kizárólag a munkavégzéssel kapcsolatos adatok tárolására használható. Magán, nem a munkavégzéshez vagy az egyetemi foglalkoztatáshoz kapcsolódó személyes tartalmakat (fénykép, zene, video, szoftver, telepítő média, stb.) a központi tárhelyen szigorúan tilos tárolni. A tárterületek adattartalmáért a jogosult felhasználó felel.

(3) A felhasználók az Egyetem informatikai infrastruktúráját nem használhatják illegális vagy nem az Egyetem tulajdonában lévő szoftverek és egyéb tartalmak tárolására. Az Informatikai Iroda gyanú vagy figyelmeztetés esetén jogosult a foglalkoztatottak számítógépén vagy felhős tárhelyén tárolt adatokat jogtisztaság szempontjából ellenőrizni és az érintett foglalkoztatottat figyelmeztetni, vagy a tartalom törlésére felszólítani. Illegális tartalom használata esetén a teljes jogi felelősség a felhasználót terheli.

(4) Saját meghajtón tárolt adattartalmak az Informatikai Iroda által nem kerülnek mentésre, azok tárolásáért, mentéséért és hordozásáért a felhasználó felel.

(5) A tárterülettel történő gazdálkodás az Informatikai Iroda feladata.

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

(1) Az Egyetem internetes megjelenítését biztosító web szervereit az Informatikai Iroda üzemelteti és felel azok működőképességéért. Az egyetemi honlap tartalomkezelő rendszerének üzemeltetését az Egyetemmel erre a feladatra szerződött partner végzi.

(2) Az egyetemi honlap egységes megjelenéséért, tartalmáért a Kommunikációs és Rendezvényszervezési Igazgatóság felelős.

(3) A honlapon csak publikus, közérdekű és közérdekből nyilvános adatok jeleníthetők meg.

(4) Az egyes szervezeti egységekre vonatkozó információk tartalmáért, pontosságáért, naprakészségéért az adott szervezeti egység vezetője a felelős.

(5) Az egyetemi honlapon történő adat/információ megjelenítésnél szigorúan be kell tartani a személyes és közérdekű adatok védelmére és biztonságára vonatkozó jogszabályokban meghatározott előírásokat.

22. § DOMAIN NEVEK HASZNÁLATÁNAK, TANÚSÍTVÁNYOK IGÉNYLÉSÉNEK SZABÁLYAI

(1) Az Egyetem által használt internetes megjelenést szolgáló domain nevek igénylésére, kezelésére kizárólag az Informatikai Iroda jogosult. Új domain név, SSL kapcsolatot igénylő szerver és felhasználói tanúsítvány, lejárt helyett új tanúsítvány igénylése esetén az Informatikai Irodához kell fordulni.

(2) Az Egyetemmel kapcsolatos események hivatalos internetes megjelentetésére elsődleges forrásként az ezeken a domain neveken belül működtetett web felületek szolgálnak.

III. FEJEZET INFORMATIKAI BIZTONSÁG

23. § INTERNET ÉS ELEKTRONIKUS LEVELEZÉS HASZNÁLATA

(1) A hálózaton biztosított internetelérés és levelezés a munkavégzésre és az azzal összefüggő egyetemi feladatok ellátására szolgál.

(2) Az Egyetem a felhasználók számára biztosítja az interneten keresztüli elektronikus levelezés lehetőségét. Az elektronikus levelezési címeket az erre a célra

rendszeresített igénylőlap kitöltésével lehet igényelni, melynek aláírásával a felhasználó kötelezettséget vállal a jelen Szabályzatban foglaltak betartására.

(4) Az informatikai szolgáltatások használatának jogosultsága a munkaviszony megszűnéséig tart. Az Informatikai Iroda az egyetemi kilépő lap benyújtásakor, az azon megjelölt határidővel (ami főszabályként a munkaviszony megszűnésének napja, indokolt esetben az azt követő 30. nap) gondoskodik a kilépő munkavállaló hálózati jogosultságainak megszüntetéséről, törléséről. Egyedi méltánylást igénylő esetben a campus főigazgató a hozzáférés további meghosszabbításáról rendelkezhet.

(5) Az Egyetem működésével, az egyetemi feladatok ellátásával kapcsolatos levelezéshez, kiadványokban történő megjelentetéshez csak a hivatalos egyetemi e-mail cím használható és jeleníthető meg.

(6) Az Informatikai Iroda a tf.hu tartományban az egyes szervezeti egységek számára, illetve az Egyetem működésével kapcsolatos speciális feladatokra tematikus e-mail címet biztosíthat. Ezeknek az e-mail címeknek utalniuk kell a szervezeti egységre vagy az adott feladatra. Ilyen célra a saját személyes e-mail címeket használni tilos.

(7) A felhasználók a hálózat és a levelezőrendszer használata során az alábbi szabályokat kötelesek betartani:

a) Az egyetemi e-mail címek – a személyhez kötéstől függetlenül – a munkavégzést, az egyetemi feladatok ellátását szolgálják, magáncélra azok nem használhatók. Továbbá magán e-mail címek munkavégzésre történő használata vagy az egyetemi levelezés magán postafiókra történő átirányítása szigorúan tilos.

b) Az Egyetemmel kapcsolatos széles körű tájékoztatás a belső kommunikációs felületen keresztül történhet. Az Informatikai Iroda feladata, hogy a Kommunikációs és Rendezvényszervezési Igazgatóság jelzésére az Egyetem érdekeit sértő tartalmak eltávolításában segítséget nyújtson.

c) Az Egyetem levelezőrendszere a nyílt interneten, web felületen is elérhető (webmail). A levelező rendszer web felületen történő használata csak megbízható környezetben (vírusvédelemmel és biztonsági frissítésekkel naprakészen tartott munkaállomásról vagy mobil eszközről) történhet.

d) Tilos minden olyan üzenetküldés, amelyet a nemzetközi hálózatok írott és íratlan szabályai (netikett) tiltanak.

e) Tilos olyan adatok, levelek továbbítása, amelyekben bármelyik, a feladó azonosítására szolgáló információ hamis, ideértve az elektronikus levél szándékosan hamis feladóval történő küldését is, továbbá a feladó vagy a küldő eltitkolását, hamisított fejlécű IP csomagok vagy üzenetek küldését.

f) Tilos a levelezőrendszeren biztonsági szempontból érzékeny adatot titkosítás nélkül továbbítani, illetéktelen személy részére hozzáférhetővé tenni.

g) Tilos másokra nézve sértő, vallási, etnikai, politikai vagy más jellegű érzékenységet bántó, zaklató tartalom közzététele.

h) Tilos lánclevelet, kéretlen reklámokat (spam) küldeni.

i) Tilos az illegális tartalmak terjesztése és olyan tartalmú üzenetek küldése, amely a másik felhasználó rendszerének megsemmisítését célozza, vagy működését hátrányosan befolyásolja.

(8) Az Egyetem fenntartja a jogot arra, hogy a vonatkozó jogszabályok betartásával a felhasználók internet forgalmát, annak tartalmát figyelemmel kísérje és naplózza, továbbá a veszélyt rejtő internetes honlapok elérését letiltsa. A naplózásra az informatikai adathálózat biztonságos és rendeltetés szerinti használatának, optimális leterheltségének, sebességének kialakítása és fenntartása érdekében kerülhet sor.

24. § MEGTÉVESZTÉS (SOCIAL ENGINEERING)

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

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

b) Ismeretlen címről érkező, egyetemi viszonylatban nem megszokott tárgyú gyanús e-mailt, és csatolmányait tilos megnyitni, mert vírusokkal fertőzhetik meg a számítógépet és a hálózatot. Gyanús vagy kártékony tartalmú levelek esetén a

beérkezés tényét kötelező jelenteni a helpdesk@tf.hu e-mail címen, hogy szükség esetén a további eszkaláció megtörténhessen.

c) Az e-mailekben szereplő linkekre csak nagy körültekintéssel szabad kattintani, mivel rosszindulatú kódokat tartalmazó honlapokra irányíthatja át a felhasználó számítógépét. Léteznek olyan manipulált weboldalak, amelyek internetes címe csak egy-két karakterben tér el a megnyitni szándékozott honlap címétől és megjelenésükben szinte teljes mértékben megegyezők, de azokat károkozási szándékkal feltehetőleg csalók készítették.

d) Az időszakosan nem használt számítógépet minden esetben ki kell kapcsolni vagy jelszó védetten zárolni kell.

e) A nyomtatókból a nyomtatott tartalmat minden esetben el kell távolítani és a nyomtatót a nyomtatás közben felügyelni kell. A nyomtatás során az ezzel a funkcióval rendelkező nyomtatókon lehetőség szerint alkalmazni kell a biztonságos nyomtatás funkciót, amely kártyás vagy kódos authentikációt (hitelesítést) használ.

25. § KÖZÖSSÉGI HÁLÓZATOK HASZNÁLATA

(1) Az Egyetem használja az internetes közösségi oldalakat is tevékenységének széleskörű megismertetésére, társadalmi elfogadottságának növelésére, oktatási és kutatási portfóliójának népszerűsítésére.

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

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

26. § SZOFTVERJOGTISZTASÁG, SZOFTVEREK TELEPÍTÉSE, FRISSÍTÉSE

(1) Az egyetemi számítógépekre csak az Egyetem által megvásárolt, jogtiszta szoftverek telepíthetők csak az Informatikai Iroda által.

(2) Az egyetemi munkaállomásokon telepített operációs rendszerek, irodai szoftverek frissítése az interneten keresztül automatikusan, illetve speciális esetekben az Informatikai Iroda közreműködésével történik. A frissítési folyamat felhasználói beavatkozást nem igényel.

27. § A SZÁMÍTÓGÉPES VÍRUSVÉDELEM

(1) A számítógép vírussal vagy más rosszindulatú programmal, történő fertőződése súlyos biztonsági kockázat. Az Egyetem hálózatában az Informatikai Iroda által biztosított és felügyelt több szintű vírusvédelmi rendszer működik. Abban az esetben, ha ennek ellenére valamelyik számítógép, felhasználói munkaállomás vírussal fertőződik, az Informatikai Iroda – a vírusmentesítés és az ellenőrzések idejére, a fertőzés terjedésének megakadályozása érdekében – kizárhatja azt a hálózati forgalomból. A felhasználó ilyen esetben köteles a mielőbbi vírusmentesítés érdekében együttműködni az Informatikai Irodával.

(2) Több munkaállomás számítógépes vírusfertőzése esetén a vírusmentesítés és az ellenőrzések idejére, a fertőzés terjedésének megakadályozása érdekében az Informatikai Iroda jogosult az adott hálózati szegmens izolálására vagy kizárására.

(3) A felhasználóknak be kell tartaniuk a vírusvédelemre vonatkozó alapvető szabályokat és az ide vonatkozó egyéb rendelkezéseket.

(4) A vírusvédelmi rendszer frissítése központilag, felhasználói beavatkozás nélkül történik. A központi vírusfrissítés elérhetetlensége esetén a munkaállomások vírusvédelmi rendszerének frissítése az interneten keresztül történik.

IV. FEJEZET A GYAKORLÓ ISKOLÁRA VONATKOZÓ KÜLÖNÖS SZABÁLYOK

28. § FELADATMEGOSZTÁS AZ INFORMATIKAI IRODA ÉS GYAKORLÓ ISKOLA KÖZÖTT

(1) A Gyakorló Iskola hálózata által nyújtott, a Gyakorló Iskola felhasználói által igénybe vehető informatikai és kommunikációs szolgáltatások körét – az Informatikai Irodát is érintő szolgáltatások esetében – az Informatikai Irodával történő előzetes egyeztetés alapján a Gyakorló Iskola igazgatója határozza meg.

(2) A Gyakorló Iskola által használt informatikai alapinfrastruktúra:

a) A Gyakorló Iskola működését biztosító informatikai rendszerek informatikai kiszolgálása és a Gyakorló Iskola tevékenységi körébe tartozó informatikai rendszerek üzemeltetése a Gyakorló Iskola feladata.

b) A Gyakorló Iskola használatában lévő és igényei szerint kialakított virtuális hálózati szegmens üzemeltetése, üzembiztosságának fenntartása az Informatikai Iroda feladata.

c) A Gyakorló Iskola használatában lévő virtuális hálózati szegmens folyamatos karbantartása, fejlesztése, valamint a lehetőségek figyelembevételével a felmerülő igényekhez történő igazítása, továbbá az új technikai lehetőségek alkalmazhatóságának megteremtése – a Gyakorló Iskolával történő egyeztetést követően – az Informatikai Iroda feladata.

d) A Gyakorló Iskola hálózati szegmens üzemzavarának esetében az Informatikai Iroda köteles a hibaelhárítást a bejelentést követően haladéktalanul megkezdeni. Munkaszüneti nap esetén az Informatikai Iroda az azt követő első munkanapon köteles a hibaelhárítást megkezdeni.

(3) Általános szabályok a Gyakorló Iskola informatikai eszközeinek használatára vonatkozóan:

a) A Gyakorló Iskola által használt informatikai eszközök működéséhez szükséges szoftverek telepítése és jogtisztasága a Gyakorló Iskola felelősségi körébe tartozik.

b) A Gyakorló Iskola által használt informatikai eszközök és adatok vírusvédelme a Gyakorló Iskola felelősségi körébe tartozik.

c) A Gyakorló Iskola által használt informatikai eszközök és szoftverek nyilvántartása a Gyakorló Iskola felelősségi körébe tartozik.

(4) A Gyakorló Iskola által üzemeltetett informatikai rendszerek:

a) A Gyakorló Iskola rendszerbe állításra tervezett, az egyetemi rendszereket globálisan érintő informatikai és kommunikációs eszközeinek, rendszerek szolgáltatásainak, rendszerbe illeszthetőségének vizsgálata, döntés meghozatala az alkalmazhatóságukról, vagy alkalmazásuk kizárásáról – az Informatikai Irodával történt előzetes egyeztetés után – a Gyakorló Iskola felelősségi körébe tartozik.

b) A Gyakorló Iskola által nyújtott hálózati szolgáltatások körének, az egyes szolgáltatások igénybevételi feltételeinek meghatározása, a hálózati biztonság érdekében az egyes szolgáltatások használatának felhasználói azonosításhoz kötése, a felhasználók körének szűkítése, korlátozása a Gyakorló Iskola felelősségi körébe tartozik.

c) Speciális szaktudást igénylő feladatoknál külső informatikai szolgáltató igénybevétele a Gyakorló Iskola felelősségi körébe tartozik. Azokban az esetekben, amelyek érintik az Informatikai Iroda feladat- és hatáskörét, illetve felelősségi területeit, a Gyakorló Iskola köteles egyeztetni az Informatikai Irodával.

(5) A Gyakorló Iskola felhasználói által használt, munkavégzéshez szükséges informatikai környezet:

a) A Gyakorló Iskola felhasználóinak az elektronikus – a tfgyakorlo.hu domain alatt üzemeltetett – levelezéssel kapcsolatos postafiókok, címek, hozzáférések biztosítása az Informatikai Iroda feladat- és hatáskörébe tartozik. A Gyakorló Iskola felhasználóira is vonatkoznak a jelen Szabályzatban az internet használatával és elektronikus levelezéssel kapcsolatos általános szabályok.

b) A Gyakorló Iskola saját Microsoft infrastruktúrájának üzemeltetése a Gyakorló Iskola feladat- és felelősségi körébe tartozik.

c) A Gyakorló Iskola saját Microsoft infrastruktúráját használó (szerver és kliens) számítógépek támogatása a Gyakorló Iskola feladat- és felelősségi körébe tartozik.

d) A Gyakorló Iskola felhasználói, illetve honlapja számára központi tárhely biztosítása, struktúrájának, hozzáféréseinek és jogosultsági szintjeinek beállítása a Gyakorló Iskola feladat- és felelősségi körébe tartozik.

e) A Gyakorló Iskola informatikai és hálózati erőforrásai jogosultságainak szabályozása a Gyakorló Iskola felelősségi körébe tartozik. Az Egyetem informatikai hálózatán való jogosultságok tekintetében – a Gyakorló Iskola felhasználói esetében is – a jelen szabályzatban rögzített általános rendelkezések az irányadók.

f) A Gyakorló Iskola felhasználói személyi számítógépeinek (asztali és hordozható gépek) felkészítése, a napi munkához szükséges programok, programrendszerek telepítése és konfigurálása a Gyakorló Iskola feladat- és felelősségi körébe tartozik. Az Informatikai Iroda feladat- és hatáskörét érintő esetekben a Gyakorló Iskola köteles előzetesen egyeztetni az Informatikai Irodával.

g) A Gyakorló Iskola felhasználói számítógépein a helyi rendszergazdai jogosultságokról való döntés a Gyakorló Iskola felelősségi körébe tartozik.

h) A Gyakorló Iskola felhasználóinak saját tulajdonú informatikai eszközei hálózatra kapcsolásának engedélyezése – az Informatikai Irodával történő előzetes egyeztetést követően, az Informatikai Iroda egyetértésével – a Gyakorló Iskola felelősségi körébe tartozik.

i) A Gyakorló Iskola felhasználói számára a távoli munkavégzéshez (VPN kapcsolat) használt központi szolgáltatások biztosítása az Informatikai Iroda feladata.

(6) A Gyakorló Iskola által használt informatikai eszközök:

a) A Gyakorló Iskola használatában, kezelésében lévő informatikai eszközök beszerzése a Műszaki és Ellátási Igazgatóság feladata.

b) A Gyakorló Iskola a belső igényeinek, tevékenységi körébe tartozó feladatainak kiszolgáló szervereit, valamint lokális informatikai hálózatát kiszolgáló eszközöket az Egyetem a Gyakorló Iskola szervertermében helyezi el, annak őrzését a Gyakorló Iskola végzi, továbbá az informatikai eszközök biztonságos üzemeltetéséhez szükséges feltételeket a Gyakorló Iskola biztosítja. Az informatikai eszközök üzemeltetése a Gyakorló Iskola feladat- és felelősségi körébe tartozik, de az információbiztonsági szempontokat az Informatikai Irodával egyeztetve szükséges alkalmaznia.

(7) Szankciók alkalmazása a biztonsági előírásokat megsértő Gyakorló Iskola felhasználókkal szemben, továbbá a szankciókkal sújtott felhasználók haladéktalan

tájékoztatása a Gyakorló Iskola felelősségi körébe tartozik. A foganatosított szankciókról és a szankciókkal sújtott személyekről a Gyakorló Iskola haladéktalanul köteles írásban vagy e-mailben tájékoztatni az Informatikai Irodát.

29. § GYAKORLÓ ISKOLA FELHASZNÁLÓINAK KÖTELESSÉGEI

(1) A Gyakorló Iskola felhasználóinak kötelességei vonatkozásában a jelen szabályzatban rögzítettek az irányadók, azzal a kivétellel, hogy a Gyakorló Iskola felhasználói az informatikai eszközök és hálózat használata folyamán tapasztalt bármiféle meghibásodás, rendellenesség, a vonatkozó biztonsági szabályzatokban foglaltak megsértése esetén elsőként a Gyakorló Iskola informatikusát értesítik. Informatikai biztonsági incidens észlelése esetén a Gyakorló Iskola informatikusának haladéktalanul tájékoztatnia kell az Informatikai Irodát. A Gyakorló Iskolának a hálózattal kapcsolatos hibaelhárítás során az Informatikai Irodával együtt kell működnie.

V. FEJEZET KOCKÁZATKEZELÉS

30. § KOCKÁZATMENEDZSMENT

(1) Annak érdekében, hogy az Egyetemnél az informatikai biztonság érvényesítése során a kockázatarányos védelem elve érvényesüljön az informatikai biztonsági kérdésekkel kapcsolatosan folyamatosan alkalmazni kell a kockázatkezelési szabályokat.

(2) A kockázatmenedzsment célja, hogy az információk bizalmasságát, sértetlenségét, valamint rendelkezésre állását veszélyeztető kockázati tényezők azonosításával, a kockázatok csökkentésével biztosítsa az informatikai biztonság növelését, szinten tartását.

(3) A teljes körű kockázatfelmérést jelentős változás esetén (pl.: technológia, illetve szolgáltatás be-, illetve kivezetése), de legalább évente kell végrehajtani az informatikai rendszer minden elemére vonatkozóan. A kockázatfelmérés és annak eredményének ismertetése az Egyetem vezetői részére az Informatikai Iroda vezetőjének feladata.

(4) A felmerült kockázatok kezelésére (csökkentésére) az Informatikai Iroda vezetője akciótervet készít, amelynek a feltárt kockázatok függvényében az alábbiakat kell tartalmaznia:

a) javaslatokat a technikai eszközök megváltoztatására, vagy fejlesztésére (pl.: új védelmi eszközök alkalmazása, vagy a jelenlegi átkonfigurálása);
b) javaslatokat a vonatkozó hatályos szabályozás megváltoztatására;
c) javaslatokat a személyi állományra vonatkozóan;
d) a kockázatok tudatos felvállalását, ha a védelmi intézkedés közvetlen és közvetett anyagi vonzata nagyobb vagy közel azonos, mint a fenyegetettség által elszenvedhető közvetlen és közvetett anyagi kár.