

Iktatószám: TK/106/13-36/2018.

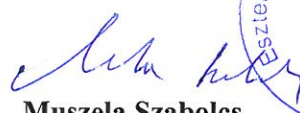
Az Esztergomi Tankerületi Központ

18/2018. (VII.30.) szabályzata

**Az Esztergomi Tankerületi Központ informatikai rendszereinek
felhasználásáról szóló szabályzata**

Készítette: Muszela Szabolcs mb. tankerületi igazgató

Esztergom, 2018. július 30.



Muszela Szabolcs
mb. tankerületi igazgató
Esztergomi Tankerületi Központ

Az Esztergomi Tankerületi Központ jelen Szabályzatát az állami köznevelési közfeladat ellátásában fenntartóként részt vevő szervekről, valamint a Klebelsberg Központról szóló 134/2016. (VI. 10.) Korm. rendelet 5. § (2) bekezdés 9. pontjában biztosított középírányítói hatáskörömben eljárva, a Klebelsberg Központ Szervezeti és Működési Szabályzatáról szóló 61/2016. (XII. 29.) EMMI utasítás 40. §-a alapján jóváhagyom:

Budapest,

utólagosan jóváhagyva

2020 JÚN 02.



Hajnal Gabriella
elnök
Klebelsberg Központ

Tartalomjegyzék

ELSŐ RÉSZ.....	4
I. Fejezet	4
Általános rendelkezések	4
1. A szabályzat hatálya.....	4
2. A szabályzat célja.....	4
II. Fejezet.....	4
3. Értelmező rendelkezések.....	4
4. A gazdálkodással kapcsolatos feladatellátás rendje	9
MÁSODIK RÉSZ	9
AZ Alapszolgáltatások szabályai.....	9
III. Fejezet	9
5. Általános szabályok	9
6. Az intranet, internet használat szabályai	9
7. Az internethasználat jogszerűsége, biztonsága	10
8. Az internet használatával kapcsolatos szabályok megsértőivel szembeni szankciók	11
9. Az elektronikus levelezés általános szabályai.....	11
10. A hivatali postafiókokkal kapcsolatos szabályok.....	11
11. Az elektronikus levelezés címzési előírásai	12
12. A levéltovábbítás.....	13
13. Az elektronikus levelezés etikettje.....	13
14. Az elektronikus levelezés magáncélú használata.....	13
15. Hálózati megosztások, szolgáltatások	14
IV. Fejezet	14
16. Általános szabályok	14
17. Informatikai jogosultság igénylés	14
18. Jelszavak képzése.....	15
19. Jelszavak kezelése.....	15
20. Felhasználói jogosultság kezelése.....	15
21. Informatikai jogosultság igénylés módja és annak beállítása	15
22. Felhasználói jogok módosítása a munkakör, a feladatkör változása vagy tartós távollét esetén	16
23. Felhasználói jogosultság megszüntetése	16
24. Speciális hozzáférések	16
25. Hozzáférési jogosultságok vizsgálata	17
26. Hozzáférési jogosultságok vizsgálata	17
27. Vírusvédelmi kötelezettség	17

28. Felhasználók jogai és kötelezettségei.....	18
V. Fejezet	19
29. Általános szabályok	19
30. Szoftverek telepítése és folyamatos üzemeltetése.....	20
31. A NISZ Zrt. feladata	20
32. Az INFO feladatai.....	21
33. Hardver berendezések telepítése és folyamatos üzemeltetése	21
34. Az informatikai hálózat fejlesztése és folyamatos üzemeltetése	21
35. Egyéb hálózati szolgáltatások	22
36. Informatikai Ügyfélszolgálat	22
37. Adatkezelés szabályozása az informatikai rendszerekben	24
38. Hivatali adatok kezelése.....	24
39. Adatbázis-módosítási jogok	24
40. Fejlesztésre és beszerzésre vonatkozó szabályok.....	25
41. Rendszerek bevezetése.....	25
42. A beszerzésre és szabványosítására vonatkozó szabályok.....	26
HARMADIK RÉSZ.....	26
Záró rendelkezések.....	26
MELLÉKLETEK	28
1. melléklet	28
Jogosultságigénylő lap	28
2. melléklet	29
Jogosultságigénylő nyilatkozat	29
3. melléklet	31
Jogosultság igénylő lap VPN rendszer hozzáférési jogosultság igényléséhez, módosításához és visszavonásához	31
4. melléklet	32
Adatkezelési hozzájárulás	32
5. melléklet	35
Servicedesk bejelentések csoportosítása	35
6. melléklet.....	36
NISZ minimumkövetelmények.....	36

Az Esztergomi Tankerületi Központ (a továbbiakban: Tankerületi Központ) Szervezeti és Működési Szabályzatának 5. § (2) bekezdés f) pontjában biztosított jogkörömben eljárva a Tankerületi Központ informatikai rendszereinek felhasználásának rendjét az alábbiak szerint szabályozom:

ELSŐ RÉSZ

I. FEJEZET

ÁLTALÁNOS RENDELKEZÉSEK

1. A szabályzat hatálya

1. § (1) A szabályzat szervezeti és személyi hatálya kiterjed:
- a) a Tankerületi Központ által, vagy hozzájárulásával beszerzett vagy üzemeltetésre a NISZ Zrt. részére átadott informatikai infrastruktúra elemekre és az azokon tárolt, illetve szolgáltatott adatokra, adatbázisokra (pl.: számítógépek, perifériák, az informatikai hálózat, hálózati erőforrások, hálózati szolgáltatások, rendszerszoftverek, alkalmazások),
 - b) a Tankerületi Központ valamennyi szervezeti egységére, a Tankerületi Központ valamennyi kormánytisztviselőjére, kormányzati ügykezelőjére, munkavállalójára, Tankerületi Központtal szerződéses vagy egyéb munkavégzésre irányuló jogviszonyban álló személyekre (a továbbiakban együttesen: foglalkoztatottak), valamint a központi szaksziszterek vonatkozásában köznevelési intézmény vezetőjére/közalkalmazottjára.
- (2) A szabályzat hatálya a Tankerületi Központ informatikai rendszerével, szolgáltatásaival egyéb szerződés alapján kapcsolatba kerülő természetes és jogi személyekre, jogi személyiséggel nem rendelkező szervezetekre (továbbiakban: külső személy) a velük kötött szerződésben rögzített mértékben, illetve a titoktartási nyilatkozat alapján terjed ki.
- (3) A Szabályzat megfelel a következő nemzetközi szabványoknak, illetve módszertanoknak:
- a) COBIT 4.0 szabvány,
 - b) ISO 27000-es szabványcsalád,
 - c) ITIL v3 módszertan.

2. A szabályzat célja

2. § (1) Az Informatikai Szabályzat a Tankerületi Központ szervezetében a Nemzeti Infokommunikációs Szolgáltató Zrt. (a továbbiakban: NISZ Zrt.) által üzemeltetett és a Tankerületi Központ által működtetett informatikai rendszer hardver, szoftver, e-mail, internet és intranet szolgáltatására vonatkozó intézkedéseket szabályozza.
- (2) A szabályzat célja:
- a) a szabálytalan felhasználás megakadályozása,
 - b) az eljárásrend-fegyelem erősítése.

II. FEJEZET

3. Értelmező rendelkezések

3. § E szabályzat alkalmazásában:

- 1. *A Tankerületi Központ informatikáért felelős szervezeti egysége:* a Gazdálkodási, Üzemeltetési és Pályázati Főosztály (a továbbiakban: INFO) jelen szabályzat szempontjából, az eszközök működésben tartásának biztosításával, illetve kiadott eszköz esetén ezen feladatok felügyeletével megbízott szereplő.

2. *Informatikai vezető:* a Tankerületi Központ SZMSZ-e szerint informatikai feladatokat ellátó szervezeti egység vezetője. Feladata az SZMSZ-ben, munkaköri leírásában meghatározottak végzése, különösen az informatikai rendszer kapacitáskezelése, a felhasználói jogok beállításainak ellenőriztetése, kapcsolattartás a NISZ-szel, az adatgazdákkal.
3. *Informatikai biztonsági felelős:* jelen szabályzatban az informatikai eszközök, rendszerek biztonságának felügyeletéért felelős személy.
4. *Felhasználó:* a Tankerületi Központ informatikai rendszerének használója az a személy, aki hozzáférési, használati jogosultságot, jogosultságokat kapott a Tankerületi Központ szolgálatában és érdekében végzendő munkája teljesítése céljából, a vonatkozó szabályok elfogadásával és aláírásával.
5. *Felelős:* a NISZ Zrt. dolgozója, vagy a Felhasználók csoportjából kijelölt személy, aki a meghatározott eszköz rendeltetésszerű működését biztosítja.
6. *Access Point (AP):* vezeték nélküli hálózati kapcsolatot megvalósító eszköz.
7. *Adat:* meghatározható, leírható elemi tulajdonság, adottság, személytelen tényt közlő ismeret, illetve tények, fogalmak, összefüggések formalizált reprezentációja, amely alkalmas személyek-, és az informatikai eszközök által történő kezelésre, feldolgozásra. Olyan jelsorozat (pld.: bit, byte, egyéb karakter stb.), amely lehetőséget teremt információ előállítására.
8. *Adatállomány:* egy nyilvántartó rendszerben kezelt adatok összessége. Adathordozón tárolt adatok halmaza, amelyet azonosító névvel látnak el.
9. *Adatátvitel:* adatok továbbítása összeköttetéseken, összekötő utakon (pl.: számítógépek között) információtechnológiai eszközök segítségével.
10. *Adatbázis:* adatok egymással kapcsolatban álló, rendezett állománya. Egy vagy több adatállomány összessége, amelyet erre alkalmas kezelőszoftverrel humán szereplő számára értelmezhető formában elérhetővé, megjeleníthetővé lehet tenni.
11. *Adatbiztonság:* az adatok rendelkezésre állásának kérdése. Célja, hogy a jogosult felhasználó – és csakis az – bármikor hozzáférhessen a számára szükséges adatállományhoz. Tágabb értelemben azon fizikai elemek, műszaki és szervezési megoldások, intézkedések összessége, mely az előbbieken meghatározott cél elérését biztosítja.
12. *Adatfeldolgozás:* az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől. Az adatok gyűjtése, rendszerezése, módosítása, tárolása, archiválása, törlése.
13. *Adatfeldolgozó:* Az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki, vagy amely az adatkezelő megbízásából – beleértve a jogszabály rendelkezése alapján történő megbízást is – a személyes adatok feldolgozását végzi.
14. *Adatgazda:* adott (ált. jogszabályban meghatározott) célra szolgáló és meghatározott összetételű adatok kezelését, felügyeletét végző személy (vagy szervezeti egység).
15. *Adatkezelés:* Az adatokon végzett bármely művelet vagy a műveletek összessége az alkalmazott eljárástól függetlenül, így az adatok gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása. Adatkezelésnek számít a fénykép, hang vagy képfelvétel készítése, valamint személy azonosítására alkalmas fizikai jellemzők (pld.: ujj vagy tenyérimpró, DNS minta, íriszkép) rögzítése is.

16. *Adatkezelő*: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki, vagy amely az adatok kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az általa megbízott adatfeldolgozóval végrehajtja.
17. *Adattovábbítás*: ha az adatot meghatározott harmadik személy számára hozzáférhetővé teszik.
18. *Adatvédelem*: a személyes adatok kezelésének korlátozását, az érintett személyek jogi védelmét, illetőleg információs önrendelkezésük gyakorlását biztosító szabályok, eljárások, eszközök és módszerek összessége.
19. *Alkalmazás, alkalmazói program*: valamely meghatározott cél érdekében működtetett (futtatott) algoritmus sorozat, amely a hardver és üzemi rendszer funkcióit használja, és amely a kimenetén a célinformációkat (outputot) szolgáltatja.
20. *Archiválás*: az adatok állományának kiírása egy elkülönített tárolóba. Ez utóbbi csak közvetetten hozzáférhető.
21. *Szervezeti egység*: a Tankerületi Központ SZMSZ-ében felsorolt főosztályokat, osztályokat, szervezeti egység vezetőin pedig ezek vezetőit kell érteni.
22. *Bizalom*: az elektronikus információs rendszer azon tulajdonsága, hogy a benne tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról.
23. *COBIT*: nemzetközileg elfogadott informatikai kontroll célok olyan gyűjteménye, amely általánosan alkalmazható és elfogadott az informatikai biztonsági ellenőrzés és szabályozás területén.
24. *Elektronikus adathordozó*: az adatok elektronikus, mágneses vagy optikai rögzítésére, tartós tárolására szolgáló eszköz.
25. *Futtatás, futtatási folyamat*: valamely program, algoritmus elindítása, működése, célfeladatának végzése a számítógépen. Általában operátorok végzik.
26. *Hardver*: az informatikai rendszer fizikai elemei, műszaki berendezések.
27. *Hálózat*: két vagy több számítógép, vagy általánosabban informatikai rendszerek összekapcsolása információtechnológiai eszközökkel, amely a komponensei közti adatcserét teszi lehetővé.
28. *Hírlevél*: levelező listán szereplő személyek, vagy szervezeti egységek felé, rendszeresen továbbított, elektronikus levél, mely esetleg tematikus tartalmú, pl.: jogszabályfigyelő, sajtószemle.
29. *Hozzáférés*: olyan eljárás, amely a felhasználó számára, jogosultsága függvényében elérhetővé teszi az informatikai rendszer erőforrásait.
30. *Hozzájárulás*: az érintett kívánságának önkéntes és határozott kinyilvánítása, amely megfelelő tájékoztatáson alapul, és amellyel félreérthetetlen beleegyezését adja a rá vonatkozó személyes adatok – teljes körű vagy egyes műveletekre kiterjedő – kezeléséhez.
31. *IBSZ*: Informatikai Biztonsági Szabályzat.
32. *INFO*: az informatikáért, informatikai szolgáltatásokért felelős szervezeti egység.
33. *Információ*: bizonyos tényekről, tárgyokról vagy jelenségekről hozzáférhető formában megadott megfigyelés, tapasztalat vagy ismeret, amely valakinek a tudását, ismeretkészletét, annak rendezettségét megváltoztatja, átalakítja, alapvetően befolyásolja, bizonytalanságát csökkenti vagy megszünteti.

34. *Információs rendszer:* azon eljárások, tevékenységek összessége, amelyek a szervezet működéséhez és irányításához szükséges információkat tárolják, előállítják, szétosztják.
35. *Informatika:* az információ rendszeres és automatikus – elsősorban számítógéppel történő – rögzítésével, tárolásával, feldolgozásával és továbbításával foglalkozó tudomány.
36. *Informatikai eszköz:* az informatikai és információszolgáltatás valamennyi tárgyi, illetve tárgyasult szellemi komponense, így a számítógépek, számítógépes hálózatok és kapcsolódó eszközök, szoftverek, konfigurációk, rendszer-beállítási paraméterek, dokumentációk stb.
37. *Informatikai biztonság:* az informatikai rendszer olyan állapota, amelyben az adatokhoz minden felhasználó kizárólag jogosultsága mértékében tud hozzáférni. Az adatok egyéb módon nem változnak, hitelességük megállapítható.
38. *Informatikai biztonsági felelős:* az informatikai biztonságért felelős személy (a továbbiakban: informatikai biztonsági felelős) ellátja a törvényben és annak végrehajtási rendeleteiben meghatározott feladatokat, amelynek során feladatkörébe tartozik különösen
 - a) a hivatali informatikai biztonsági tevékenység szakmai támogatása, ellenőrzése, a Tankerületi Központ biztonságpolitikai érdekeinek és törekvéseinek érvényesítése;
 - b) a Tankerületi Központ működését közvetlenül vagy közvetve érintő adatok és információk rendelkezésre állásának, integritásának, bizalmasságának és sértetlenségének megőrzése, az adatkezelések jogszerűsége, minősége, az adatszűrés szabályozása, ellenőrzése, szervezése;
 - c) a Tankerületi Központ informatikai biztonságának, mint állapotnak a fenntartását szolgáló és garantáló műszaki-technikai, fizikai, jogi és adminisztratív, tervezési, szervezési, vezetési, oktatási, végrehajtási feladatok és intézkedések irányítása, összehangolása, kidolgozása, ezek folyamatos korszerűsítése, valamint az e területet érintő jogszabályok, belső utasítások betartásának, illetve betartatásának ellenőrzése.
39. *Informatikai rendszer:* a hardverek és szoftverek olyan kombinációjából álló rendszer, amit az adat-, illetve információ-feldolgozás különböző feladatainak teljesítésére alkalmaznak.
40. *Írás, írási folyamat:* az adat rögzítésének fizikai folyamata valamilyen (papír alapú, mágneses, optikai, stb.) adathordozóra.
41. *ISO 27000 szabványcsalád:* az információbiztonsági irányítási rendszer tanúsítására szolgáló szabványok gyűjteménye, amelyek alapján azt alkalmazó intézményben – a működési kockázatokat figyelembe vevő megközelítésen alapulva – kialakítható, bevezethető, működtethető, figyelhető, átvizsgálható, fenntartható és fejleszthető az információvédelem.
42. *ITIL:* informatikai rendszerek üzemeltetésére és fejlesztésére szolgáló módszertan, illetve szabvány- és ajánlás-gyűjtemény.
43. *LAN:* helyi adathálózat.
44. *Log, log-fájlok:* a rendszernapló bejegyzései.
45. *Letöltés:* adattartalom (szöveges, kép, hang, program, stb.) importálása saját gépre.
46. *Meghajtó:* fájlrendszerrel formázott, meghajtó-betűjellel jelölt adattároló terület. A tár lehet hajlékonylemez, CD, merevlemez vagy más típusú lemez. A meghajtó tartalmának megtekintéséhez a meghajtó ikonjára kell kattintani (pld.: a Windows Intézőben vagy a Sajátgép ablakban).
47. *Mentés:* az adatok reprodukálása (átmásolása, duplikálása) egy elkülönített tárolóhelyre,

(meghajtóra). A művelet után az adat továbbra is közvetlenül elérhető marad (az adat a helyén marad, ld: archiválás).

48. *Működőképesség*: A rendszernek és elemeinek az elvárt és igényelt üzemelési állapotban való fennmaradása. A működőképesség fogalom sok esetben az üzembiztonság fogalommal.
49. *Olvasás, olvasási folyamat*: az előzőleg már rögzített adat dekódolása és megjelenítése.
50. *Operációs rendszer*: az az algoritmusokkal meghatározható speciális program, amely lehetővé teszi, hogy a felhasználó kapcsolatba lépjen a gép fizikai egységeivel. Lehetővé teszi a meghatározott célok érdekében telepített programok futtatását, értelmezését a gépi logika, a processzor számára. Tágabb értelemben: kapcsolat az ember és a gép között. A gépek alapvető, kötelezően létező programja. Sokféle van (pld.: DOS, Windows, Linux, Unix).
51. *Output*: kijövő adat, információ. A rendszer által feldolgozott adatok fizikai megjelenítése.
52. *RBK*: Rendszer Beavatkozási Kérelem.
53. *Rendelkezésre állás*: annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek.
54. *Rendszerprogram*: olyan alapszoftver, amelyre szükség van, hogy valamely informatikai rendszer hardvereit használhassuk és az alkalmazói programokat működtessük. A rendszerprogramok nagy részét az operációs rendszerek alkotják.
55. *Sértetlenség*: az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az az elvárt forrásból származik (hitelesség) és a származás ellenőrizhetőségét, bizonyosságát (letagadhatatlanságát) is, illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható.
56. *SLA*: Service Level Agreement. Szolgáltatási szint szerződés.
57. *Szoftver*: az informatikai rendszer logikai része, amely a működés vezérléséhez szükséges.
58. *Tartomány*: Számítógépek olyan csoportja, amely egy hálózatrészt alkot, és közös címtáradatbázist használ. A tartomány felügyelet szempontjából egy egységet képez, amelyre közös szabályok és eljárások vonatkoznak. Minden tartománynak egyedi neve van.
59. *Vezető*: A munkáltatói jogkör gyakorlója (a továbbiakban: vezető) felel a vezetése vagy irányítása alatt álló szervezet, vagy szervezeti egység területén és/vagy kezelésében lévő informatikai eszközök szabályszerű használatáért, működtetéséért, az Informatikai Szabályzatban és más utasításokban foglaltak betartásáért és betartatásáért.

Az adatokhoz (alkalmazásokhoz) történő hozzáférés megadását biztosító folyamatban a vezetőnek javaslattevői, az alaphozzáférést tekintve pedig engedélyezési joga van, azaz meghatározza, hogy az irányítása, vagy vezetése alatt álló munkatárnak a hivatali vagy projekt oldali feladatainak elvégzéséhez milyen adatokhoz szükséges hozzáférnie.

A vezető javaslatát az adatgazda hagyja jóvá. Az adatgazdát ebben a döntési körben utasítani nem lehet.

60. *Vírus*: A számítógépes vírus olyan program, amely saját másolatait helyezi el más, végrehajtható programokban vagy dokumentumokban. Többnyire rosszindulatú, más állományokat használhatatlanná, sőt teljesen tönkre is tehet. A vírusok manapság jellemzően pendrive vagy e-mail segítségével terjednek, az internetes böngészés mellett, valamint a megbízhatatlan oldalokról történő letöltések által.

61. *Ügyfélszolgálat:* A Tankerületi Központ Informatikai szervezeti egysége által üzemeltetett szolgáltatás, amelyen keresztül hivatalosan lehet ügyeket, tipikusan informatikai hibákat, vagy új igényeket bejelenteni. Az informatika email-en a miklos.nagy@kk.gov.hu címen érhető el. Telefonszáma: +36-33-795-203

4. A gazdálkodással kapcsolatos feladatellátás rendje

4. § A központosított informatikai és elektronikus hírközlési szolgáltatásokat egyedi szolgáltatási megállapodás útján igénybe vevő szervezetekről, valamint a központi szolgáltató által üzemeltetett vagy fejlesztett informatikai rendszerekről szóló 7/2013. (II. 26.) NFM rendelet (a továbbiakban: Rendelet). alapján a Rendelet hatálya alá tartozó eszközök biztosítása és üzemeltetése a NISZ Zrt. feladata.

MÁSODIK RÉSZ

AZ ALAPSZOLGÁLTATÁSOK SZABÁLYAI

III. FEJEZET

5. Általános szabályok

- 5. §** (1) Az INFO a munkaállomásokon végzett munkát alapszolgáltatás biztosításával támogatja. Az alapszolgáltatás biztosítása a szabványos informatikai munkakörnyezet létrehozását, folyamatos működésének biztosítását és a kapcsolódó szolgáltatások ellátását jelenti.
- (2) Az alapszolgáltatást csak a felhasználói jogosultsággal rendelkező személyek vehetik igénybe, amelyet az INFO biztosít számukra az érintett szervezeti egység vezetőjének döntése alapján.
- (3) Az alapszolgáltatástól eltérő, szakmailag indokolható igényeket az érintett szervezeti egység vezetője az INFO felé írásban jelzi. Az adott igényt kiszolgáló informatikai eszközök specifikálása és kiválasztása az INFO hatáskörébe tartozik.
- (4) A Tankerületi Központ az informatikai infrastruktúrát kizárólag a munkaköri feladatok ellátása érdekében történő munkavégzés céljából bocsátja a felhasználók rendelkezésére.
- (5) A felhasználó az informatikai infrastruktúrát köteles rendeltetésének megfelelően használni. A Tankerületi Központ szervezeti egységének vezetője személyében felelős a szervezeti egység területén lévő informatikai infrastruktúra rendeltetésszerű használatáért.
- (6) Amennyiben a felhasználói jogosultság alapját képező jogviszony megszűnik, a felhasználó hozzáférési jogosultságának és postafiókjának megszüntetése nem az INFO feladata, mivel erre a személyi ügyekért felelős szervezeti egység által elvégzett kiléptetési munkafolyamat keretei között kerül sor. Hasonlóképpen a beléptetés során létrehozott postafiókok, felhasználói témaszámok, valamint jelszavak létrehozása is a foglalkoztatott beléptetési folyamatának része, így ezekért is az illetékes szervezeti egység felel.

6. Az intranet, internet használat szabályai

- 6. §** (1) A Tankerületi Központ szélessávú internet elérése valamennyi felhasználó részére biztosított, de a hozzáférési jogosultsági szint különböző lehet.
- (2) A tankerületi igazgató jogosult az internet használatának – jelen szabályzat keretei közötti – korlátozására, valamint az internethasználat jogosultságának a visszavonására.
- (3) A Tankerületi Központ erre kijelölt informatikai munkatársai a felhasználók által böngészett oldalak listáját naplózzák, amelyről kérés esetén az INFO vezetője tájékoztatja a tankerületi igazgatót. A naplófájl készítésének és ellenőrzésének célja, hogy a felhasználók internethasználatuk megfeleljen a

Tankerületi Központ jogos érdekeinek.

7. Az internethasználat jogszerűsége, biztonsága

7. § (1) Az informatikai vezető a tankerületi igazgató internethasználatról szóló döntése alapján az internethasználatot korlátozhatja, a jogosultságot visszavonhatja.

(2) Minden felhasználó saját felelősségére használja az internetet, mint szolgáltatást, ezért annak használata kizárólag a törvények és egyéb jogszabályok keretei között megengedett.

(3) Az internet szolgáltatás eléréséhez, kizárólag a Tankerületi Központban rendszeresített internetes alkalmazások használhatók. Tilos olyan internetes alkalmazások használata, amelyek

- a) sérthetik a Tankerületi Központ informatikai rendszereinek, alkalmazásainak biztonságát,
- b) lehetővé teszik a hivatali adatbázisok bizalmasságának, sértetlenségének, rendelkezésre állásának megsértését,
- c) a Tankerületi Központ erőforrásainak illegális megosztására irányulnak (pl. FTP szerver, torrent), vagy
- d) licenc szerződésével a Tankerületi Központ nem rendelkezik.

(4) Tilos

- a) a hálózat erőforrásainak, a hálózaton elérhető adatoknak illetéktelen módosítására, megsemmisítésére irányuló tevékenység, az azokhoz történő illetéktelen hozzáférés, a hálózat biztonságát veszélyeztető információk, programok terjesztése,
- b) a másokra nézve sértő, mások vallási, etnikai, politikai vagy más jellegű érzékenységét sértő, másokat zaklató tevékenység (pl. pornográf, vagy közérkölcstől sértő anyagok közzététele, letöltése),
- c) a tiltott haszonszerzésre irányuló tevékenység (pl. piramis- vagy pilótajáték), szoftver szándékos és tudatos illegális terjesztése,
- d) a profitszerzést célzó direkt üzleti célú tevékenység, reklámok terjesztése,
- e) a hálózat, illetve erőforrásai normális működését megzavaró, veszélyeztető tevékenység,
- f) a szoftverek letöltése során a szoftver tulajdonosa által szabott jogi feltételeket megszegni, a szerzői jogvédelemmel kapcsolatos jogszabályok betartása mindenre nézve kötelező,
- g) a file-cserélők használata és nagyméretű file-ok magáncélú letöltése, vagy
- h) a felhasználóknak a Web-böngészők biztonsági beállításait (pl. cookie-k, JavaScriptek, ActiveX környezetek, plug-in-ek, jelszó megjegyzés tiltás használatát) megváltoztatni,
- i) a böngészőben felbukkanó párbeszéd ablakok megnyitása, amelyek segédprogramok telepítésére, vagy egyes funkciók kikapcsolására ösztönöznek,
- j) az Internetes webhelyek eléréséhez szükséges jelszavakat úgy megválasztani, hogy azokból a Tankerületi Központ informatikai rendszerében használt jelszóra következtetni lehessen.

(5) A Tankerületi Központ az IBSZ-ben leírtak szerint fenntartja a jogot állománytípustól (pl.: MPG, JPG, BMP, WMV stb.), valamint mérettől függő letöltés korlátozására.

(6) A korlátozás alá eső formátumú, vagy az engedélyezett méretet meghaladó állományok letöltését, felkérésre és az informatikai vezető engedélyével az informatikai rendszerek üzemeltetéséért felelős rendszergazda végzi el.

8. Az internet használatával kapcsolatos szabályok megsértőivel szembeni szankciók

- 8. §** (1) Az internethasználatot a tankerületi igazgató által kijelölt személy ellenőrizheti.
- (2) Az internethasználati szabályokat szándékosan és súlyosan megsértő felhasználó az internet hálózati szolgáltatásokból ideiglenesen, vagy véglegesen kizárható.
- (3) Ha az internethasználati szabályok megsértése kismértékű, vagy nem tekinthető szándékosnak, akkor a felhasználót figyelmeztetni és a szabályozásról tájékoztatni kell. A figyelmeztetés utáni ismételt elkövetést szándékosnak kell tekinteni. Az internethasználati szabályok megsértése fegyelmi felelősségre vonást, illetve kártérítési eljárást vonhat maga után.

9. Az elektronikus levelezés általános szabályai

- 9. §** (1) A Tankerületi Központon belüli és a külső partnerekkel fenntartott kapcsolatokból adódó információáramlás folyamatosan áttevődik az elektronikus levelezési rendszerre, ezzel lecsökkentve a papíron történő információtovábbítás mennyiségét. A Tankerületi Központon belül kizárólag az informatikai vezető által jóváhagyott csoportmunka támogató és levelező rendszer használata engedélyezett.
- (2) Az elektronikus levelezési rendszert csak az ügyviteli folyamatokkal, illetve azok támogatására lehet használni.
- (3) A levelezéssel kapcsolatos gyanús eseményről értesíteni kell az informatikáért felelős szervezeti egység vezetőjét, valamint az informatikai biztonsági felelőst.
- (4) Az elektronikus levelezés zavartalan működést, a mindenkori igényeknek és forgalomnak megfelelő hardver és szoftver erőforrások meglétét, a szakszerű szolgáltatását a NISZ Zrt. szerződés szerint biztosítja.

10. A hivatali postafiókokkal kapcsolatos szabályok

- 10. §** (1) A Tankerületi Központ a felhasználó részére névre szóló postafiókot biztosít. A postafiókok távolról, a NISZ Zrt. WebAccess szolgáltatásán keresztül is elérhetők a <https://msg.gov.hu/owa> címen; tartomány: central; felhasználónév megegyezik a Tankerületi Központon belül használt bejelentkezési névvel. Az e-mail címek képzési szabálya: "utónév.vezetéknév@kk.gov.hu". Amennyiben az e-mail cím már foglalt, úgy a vezetéknévhez illesztve a következő szabad sorszámot kell felhasználni, pl.: "utónév.vezetéknév2@kk.gov.hu".
- (2) A felhasználói postafiók mérete 1 GB, amelyet az informatikai vezető az erőforrások függvényében módosíthat. Amennyiben a postafiók a megadott méretet eléri, vagy meghaladja, a felhasználók e-mailt küldeni nem tudnak. A postafiókok méretének rendszeres időközönként történő ellenőrzése a felhasználó feladata, ezzel párhuzamosan a felhasználó a rendszer által automatikus küldött levélben értesül, hogy a postafiókja megtelt.
- (3) Az elektronikus levél mérete korlátozott. Ez jelenleg, figyelembe véve a rendelkezésre álló adatátviteli korlát 20 MByte. Ettől eltérni csak az informatikai vezető engedélyével lehet.
- (4) A Tankerületi Központ levelezési szolgáltatását igénybe vevő felhasználók munkaállomásainak alkalmasnak kell lennie a ZIP formátumú, tömörített állományok kezelésére. A mérethatárt túllépő állományokat több részletben kell feladni, és azt a tárgy mezőben jelezni kell.
- (5) A postafiókot hivatali munkaidőben lehetőség szerint 2 óránként ellenőrizni kell a rövid határidejű feladatok kezelése érdekében.
- (6) A levélnek kötelező tárgyat adni, mert ellenkező esetben a levelező rendszerek vírusnak vélhetik és törölhetik. A levél tárgyának röviden, de értelmezhető módon utalnia kell a levél tartalmára, amelyet

kötelező feltüntetni.

(7) A levelek automatikus aláírását a levelező rendszerben be kell állítani. Az aláírásnak a hivatali adatok közül tartalmaznia kell az aláíró

- a) nevét,
- b) munkakörének megnevezését,
- c) szervezeti egységének megnevezését,
- d) szervezeti egységének címét, levélcímét,
- e) telefonszámát,
- f) mobiltelefonszámát – amennyiben ilyennel rendelkezik,
- g) e-mail címét.

(8) Az elküldött levelek tartalmáért a küldő felel.

(9) Hírszolgálatokra, hírlevelekre történő feliratkozás csak az informatikai vezetővel történt előzetes egyeztetés után szabad.

(10) Egy munkanapot meghaladó távollét esetén a felhasználónak a programban automatikus válaszadási szabályt kell beállítania, amely tudatja a beérkezett levelek feladójával, hogy a címzett mettől-meddig van távol, és ki helyettesíti. A válaszlevélben helyettesítőjének elérhetőségét is meg kell adnia.

(11) Személyes fiók archiválását a felhasználónak kell elvégeznie. Törölnie csak a nem iktatott leveleket szabad, az iktatott e-mail-eket szükség esetén archiválni kell. Ezért teljes mértékben a felhasználó felel.

(12) A foglalkoztatott kilépése esetén az INFO legfeljebb 3 hónap időtartamra, az adott címre automatikus válaszadási szabályt állít be, amely a feladót értesíti a változásról. A fiókot 6 hónap után a kilépett dolgozó vezetőjének beleegyezésével törölni lehet.

11. Az elektronikus levelezés címzési előírásai

11. § (1) A levél címzése az alábbi adatokból áll:

- a) Címzett (To): akinek a levél szól;
- b) Másolat (CC): aki másolatban kapja meg a levelet;
- c) Titkos másolat (BCC): a levél címzettje nem látja, kinek címezték még meg a levelet.

(2) Levelezési listákra való levél küldésekor figyelembe kell venni, hogy a lista minden tagja megkapja a levelet, ezért ezeknél a leveleknél fokozottan kell ügyelni a levél tartalmára.

(3) Az e-mail mellékleteként lehetőség van fájl vagy fájlokat csatolni, amelynek során

- a) ügyelni kell a méretkorlátozásokra,
- b) a csatolás előtt ellenőrizni kell a csatolandó fájl méretét,
- c) Elektronikus levelezésben nem fogadhatók és küldhetők csatolmányként az alábbi kiterjesztésű állományok:
 - ca) Futtatható állományok: bat; com; exe; pif;
 - cb) Adatbázis állományok: dbf; dat;
 - cc) Média állományok: wmv; avi; mpeg; mp3; wav; mid;

- cd) Egyéb állományok: dll; sys; inf; hlp; bin;
- d) ügyelni kell arra, hogy a mellékelt fájl neve legyen rövid és tömör (30 karakternél nem hosszabb), ékezetes betűket ne tartalmazzon (külföldi címzetteknel problémát okozhat az ékezetes betűkből álló fájl név).

12. A levéltovábbítás

12. § A Tankerületi Központ elektronikus levelező rendszerén belül biztonsági szempontból érzékeny adatok kerülhetnek továbbításra. A biztonság fokozása érdekében a Tankerületi Központon belül csoportmunka-támogató rendszerek (fájl szerver, Sharepoint alrendszerek) üzemelnek, amelyek az adatokat biztonságos, mások által nem értelmezhető formában tárolják, és továbbítják. Ezt a biztonságot azonban csak a Tankerületi Központ informatikai rendszerén belül lehet biztosítani, az Internet irányába küldött levelek mások által könnyen értelmezhetőek, manipulálhatóak, ezért

- a) a Tankerületi Központ bármely postafiókján külső e-mail címre történő továbbítási szabályt beállítani tilos,
- b) a központi címjegyzékbe csak átfogó jelentőségű, állandóan szükséges listák kerülhetnek, melyek létrehozását az Informatikai vezető engedélyezi.

13. Az elektronikus levelezés etikettje

13. § (1) Egy e-mail-t a Tankerületi Központon belülrre és kívülrre nem szabad tömeges mennyiségben (200 címzettet meghaladóan) küldeni vagy továbbítani, kivéve, ha a Tankerületi Központ működése szempontjából indokolt az e-mail tartalom minden címzethez való eljuttatása. A hivatalos e-mail nyelvezetének meg kell felelnie az általános és a kormánytisztviselői hivatás etikai szabályainak.

(2) Szigorúan tilos a közízlést, a Tankerületi Központ jó hírnevét veszélyeztető, erkölcstelen, vagy politikai tartalmú e-mail elküldése.

(3) Tilos olyan levelek továbbítása a Tankerületi Központ levelező rendszerében, amelyek bármilyen nyelven arra szólítanak fel, hogy a levelet minél több címre kell továbbítani.

(4) Tilos válaszolni olyan levelekre, amelyek arra szólítanak fel, hogy a Tankerületi Központ biztonsági rendszeréről, vagy a felhasználó saját hozzáférési adatairól (tartománynév, felhasználónév, jelszó) adjon tájékoztatást.

(5) Tilos az elektronikus levelező rendszeren „Titkos”, vagy „Szigorúan titkos” információt titkosítás nélkül továbbítani.

(6) A levélszűrésen fennakadt levelekről automatikus üzenet csak a Tankerületi Központ alkalmazottjának küldhető.

(7) Automata üzenettovábbítás a Tankerületi Központon kívülrre tilos.

(8) Ismeretlen vagy ismert feladótól érkező, de értelmetlen tárgyat tartalmazó levelet (amely általában értelmetlennek tűnő csatolmányt is tartalmaz, vagy idegen nyelven íródott) megnyitni tilos. A Tankerületi Központ Ügyfélszolgálatát erről értesíteni kell, aki intézkedik a levél ellenőrzésével kapcsolatban. Az Ügyfélszolgálat aktuális elérése megtalálható az intraneten.

14. Az elektronikus levelezés magáncélú használata

14. § A hivatali e-mail címekkel történő esetleges (hivatali) visszaélés esetén a felhasználóval szemben eljárás indítható. A személyes postafiókra a munka folyamatossága érdekében helyettesítés állítható be.

15. Hálózati megosztások, szolgáltatások

15. § A Tankerületi Központ hálózatán belül biztonsági okokból csak szerver biztosíthat megosztott szolgáltatásokat. Egyéb, munkaállomáson megosztott erőforrás-, fájlmegosztás biztonsági okokból nem engedélyezett. Kivételt képeznek ez alól az informatikai vezető engedélyével egyes speciális tevékenységet, célfeladatot ellátó számítógépes rendszerek, a szükséges mértékben.

IV. FEJEZET

A FELHASZNÁLÓKRA VONATKOZÓ SZABÁLYOK

16. Általános szabályok

16. § (1) Felhasználó az a természetes személy, aki az informatikai rendszer erőforrásait és szolgáltatásait a napi munkájának elvégzéséhez igénybe veszi. Nem tekintendő felhasználónak az, aki az Interneten keresztül veszi igénybe a Tankerületi Központ által nyilvánossá tett informatikai szolgáltatásokat, és így kerül kapcsolatba az informatikai infrastruktúrával.

(2) A felhasználó részére felhasználói jogot kérő szervezeti egység vezetője felelősséggel tartozik a felhasználó részére biztosítandó jogosultság meghatározásáért.

(3) Külső felhasználóknak tekintendők mindazok, akik valamely szervezeti egység vezetőjének indokolt kérésére, a velük kötött szerződésben rögzített mértékben és titoktartási nyilatkozat alapján meghatározott időre, adott feladat elvégzésére felhasználói jogosultságot kapnak.

(4) A külső felhasználók részére felhasználói jogot szervezeti egység vezetőjének felelőssége a jelen Szabályzatban megfogalmazott előírások megismertetése és elfogadtatása.

17. Informatikai jogosultság igénylés

17. § (1) A hozzáférés szabályozásának alapelve a következő: minden hozzáférés tiltott, kivéve, ha az nincs kifejezetten megengedve.

(2) A felhasználók azonosítója – a felhasználó név, vagy user ID – a felhasználó identitásának egyedi, jellemző, ellenőrizhető és hitelesítésre alkalmas megjelenítése az informatikai rendszerben.

(3) A felhasználó-azonosító segítségével az egyes erőforrásokhoz, folyamatokhoz és adatokhoz történő hozzáférés megfelelően korlátozható és követhető, ugyanakkor a rendszer számára a biztonsági funkciók során ellenőrizhető.

(4) A felhasználói azonosítónak minden esetben egyedinek kell lennie, azaz semmilyen körülmények között sem adható ki különböző személyek részére megegyező azonosító.

(5) A felhasználói azonosító képzése a hálózati operációs rendszerben elfogadott és alkalmazott azonosítás alapján történik, az azonosító a felhasználó személynevéből képzett szó, amely a személy vezetéknévéből és keresztnévének (keresztneveinek) első betűjéből képződik.

(6) Kettős családnév esetén az elől álló családnévet teljes egészében, a második helyen álló családnév esetén pedig annak első betűjét kell felhasználni (pl.: Feketéné Szili Judit esetén „feketenesj”, vagy Nemes Nagy Ágnes esetén „nemesna”). Kettős keresztnév esetén a második keresztnév első betűjét is fel kell használni. Kettős betűvel kezdődő keresztnévek esetén a kettős betű első betűjét kell használni (pl. Kovács Csilla esetén „kovacs”). Abban az esetben, ha az így képzett szó a NISZ Informatikai Rendszerében már foglalt, akkor a keresztnév (keresztnévek) következő betűjének felhasználásával az azonosítót képezni (pl. Kovács Béla és Kovács Bernadett esetén az egyik "kovacs" a másik "kovacsbe").

(7) A felhasználónevek (korábbi felhasználó távozása után) újbóli felhasználása tilos.

18. Jelszavak képzése

18. § (1) A felhasználók azonosítása felhasználói név és jelszó segítségével történik. A felhasználók – az informatikai szabályzatokban és utasításokban foglalt és annak megfelelően dokumentált kivételektől eltekintve – nem ismerhetik meg egymás jelszavát, nem használhatják más felhasználók bejelentkezéseit. Minden rendszert úgy kell beállítani, hogy hozzáférés csak érvényes felhasználónévvel és jelszóval legyen lehetséges.

(2) A rendszereknek ki kell kényszeríteniük az alábbi feltételeknek megfelelő jelszavak használatát, azaz minden jelszónak meg kell felelnie az Informatikai Biztonsági Szabályzatban előírtaknak.

(3) Tilos jelszavakat más felhasználókkal megosztani, szigorúan tilos jelszavakat nyilvánosan megosztani.

19. Jelszavak kezelése

19. § (1) A rendszerek, illetve szoftverek telepítése után az alapértelmezett jelszavakat meg kell változtatni.

(2) A felhasználói jelszavakat bizalmasan kell kezelni.

(3) A felhasználó a rendszerbe való első belépéshez ideiglenes jelszót kap, amelyet az első lehetséges alkalommal köteles megváltoztatni. Amennyiben egy alkalmazásnál a jelszó ilyen megváltoztatása nem lehetséges, a jelszó politika elveit fokozott szigorúsággal kell alkalmazni.

(4) Egy számítógéprendszeren a jelszavakat sohasem szabad nem védett módon tárolni.

(5) Jelszavak elfelejtése, illetve más által történő megismerése esetén új jelszót kell igényelni.

20. Felhasználói jogosultság kezelése

20. § Hivatalos, dokumentált eljárás során kell kiadni és megszüntetni a felhasználói jogosultságokat.

21. Informatikai jogosultság igénylés módja és annak beállítása

21. § (1) A Tankerületi Központ szervezeti egységének vezetője kérelmezi a felhasználó jogosultságigényét. A felhasználó foglalkoztatotti jogviszonyát érintő változásról (kinevezés, áthelyezés, felfüggesztés, munkaviszony megszűnése stb.) a szervezeti egység vezetője köteles, illetve egyéb jogosultságigény esetén jogosult az 1. melléklet, illetve távoli hozzáférési igény esetén a 3. melléklet szerinti, a jogosultságot igénylő személy által aláírt és az adott szervezeti egység vezetője által kérelmezett, beszkenelt jogosultságigénylő lapot benyújtani az Ügyfélszolgálatra.

(2) Külső felhasználó jogosultságáért a Tankerületi Központ szervezeti egységének vezetője, a kérelmet benyújtó vezetője felel. Ennek megfelelően minden változásról (alapul szolgáló szerződés és titoktartási nyilatkozat megszűnése stb.) az Ügyfélszolgálatához köteles az 1. melléklet, távoli hozzáférési igény esetén a 3. melléklet szerinti, a jogosultságot igénylő személy által aláírt és az adott szervezeti egység vezetője által kérelmezett beszkenelt jogosultságigénylő lapot, az 4. melléklet szerinti, beszkenelt adatkezelési hozzájárulást, valamint a felhasználói jogosultság alapjául szolgáló szerződést benyújtani az Ügyfélszolgálatra.

(3) Névre szóló postafiókra és naptárra vonatkozó hozzáférési, illetve egyéb jogosultság kiterjesztésére, további felhasználó számára a 2. melléklet szerinti aláírt, beszkenelt jogosultságigénylő nyilatkozat benyújtásával, Ügyfélszolgálatra. Ennek egy példányát az érintett szervezeti egység vezetőjénél kell megőrizni.

(4) A szervezeti egység vezetője által jóváhagyott jogosultságigény kizárólag az informatikai hálózat, illetve erőforrásai üzemeltetésének veszélyeztetése esetén, megfelelő informatikai szakmai

indokolással utasítható el.

22. Felhasználói jogok módosítása a munkakör, a feladatkör változása vagy tartós távollét esetén

22. § (1) A felhasználó feladatkörének vagy munkakörének teljes vagy részleges megváltozása, a dolgozó szervezetén belüli ideiglenes átirányítása, illetve más szervezeti egységhez kerülése, vagy munkaszerződésétől eltérő foglalkoztatása esetén az új munkaköre szerinti közvetlen vezetője az adatgazdának tesz javaslatot új hozzáférés engedélyezésére, illetve módosítására az informatikai jogosultsági űrlapon keresztül. A régi, nem használt jogosultságok megszüntetése a jogosultságot eredetileg igénylő adatgazda vezető felelőssége, amely bejelentésének a munkakör váltásakor vagy megszűnésekor haladéktalanul meg kell történnie.

(2) Ha a felhasználó munkaköre úgy változik, hogy hozzáférési jogai egyes adatokhoz megszűnnek vagy módosulnak, de közvetlen munkakör váltás nem történik a kiadott jogosultságok módosítását az adatgazda kezdeményezi az informatikai vezetőnél az informatikai jogosultsági űrlap kitöltésével.

(3) 30 napot meghaladó tartós távollét esetén a munkakör szerinti közvetlen vezetőnek az adatgazdával egyeztetve, haladéktalanul (legkésőbb a távollét megkezdésének időpontjában) jeleznie kell a jogosultságok felfüggesztésének igényét az informatikai vezető felé. A felfüggesztés kérése és a tartós távollét utáni feloldása az informatikai jogosultsági űrlap adatgazda általi kitöltésével történik. A felfüggesztés tényének haladéktalan jelzése a közvetlen vezető és az adatgazda együttes felelőssége.

(4) A felhasználót megillető jogosítványok megszüntetésére vonatkozó vezetői kezdeményezést az informatikai vezető tudomásul veszi, és végrehajtását kezdeményezi.

23. Felhasználói jogosultság megszüntetése

23. § (1) A Tankerületi Központtal foglalkoztatotti jogviszonyban álló személy jogviszonyának megszűnése esetén a közvetlen felettes kezdeményezi a dolgozó jogosultságainak megszüntetését, amelyet a kitöltött és aláírt informatikai jogosultsági űrlap segítségével tesz meg.

(2) A kilépő Elszámoló lapot az INFO vezetője (illetve az általa meghatározott személy) is aláírja, igazolva az informatikai eszközök leadását. A Kilépő elszámolási lap – informatikai vezető által történő – aláírására akkor van mód, ha azzal egyidejűleg a dolgozó közvetlen vezetője az adatgazdával egyeztetve az informatikai jogosultsági űrlap kitöltésével kéri a felhasználó jogosultságainak törlését.

(3) Az INFO ennek birtokában teszi meg a következő intézkedéseket.

(4) A felhasználót megillető jogosítványok megszüntetését a hivatalosan aláírt informatikai jogosultsági űrlap megérkezésével az üzemeltetés haladéktalanul elvégzetteti. A törléssel egyidejűleg a volt munkatárs minden hozzá tartozó felhasználói könyvtárhoz a vezetője olvasási jogot kap.

(5) Az INFO a zárolás után 30 nappal a felhasználó postafiókjának, valamint a személyes könyvtárában tárolt adatainak törléséről intézkedik. A zárolás és a törlés közötti időtartam meghosszabbítására a tankerületi igazgató jogosult.

(6) A felhasználó jogosultságainak megszüntetésével egyidejűleg köteles az INFO számára visszaszolgáltatni a jogviszonyának fennállása alatt a Tankerületi Központtól átvett infokommunikációs eszközöket. Az átadás tényét az átvevő a Kilépési papír aláírásával igazolja.

24. Speciális hozzáférések

24. § (1) Távoli hozzáférés: a felhasználók a hivatali rendszerhez távolról kizárólag titkosított kapcsolaton keresztül férhetnek hozzá. A munkatársak távolról való bejelentkezése munkavégzés céljából szükséges lehet, de kizárólag indokolt esetben szabad a jogosultságot megadni a fokozott informatikai biztonsági kockázat miatt.

(2) Távolról való bejelentkezésre – az adatgazda jóváhagyásával – kizárólag az informatikai vezető adhat engedélyt.

25. § Ideiglenes felhasználói azonosítók: bizonyos feladatok elvégzéséhez, többek között az ellenőrzött helyettesítéshez, szükség lehet a Tankerületi Központ munkatársai vagy külsős felhasználók részére ideiglenes felhasználói azonosítókat létrehozni. Ideiglenes felhasználói azonosítók csak határozott időre adhatók. Ilyen esetben a következőképpen kell eljárni:

- a) az ideiglenes felhasználói kérelmet az adatgazda engedélyezi, amelyet az informatikai vezetőnek kell jóváhagynia,
- b) az ideiglenes hozzáférési jogosultságokat az INFO a határidő lejártá után automatikusan megszünteti,
- c) külsős felhasználók, szervezetek részére kizárólag adatbiztonsági és titoktartási nyilatkozat bekérésével engedélyezhető a hozzáférés. A nyilatkozatban rögzítendő a hozzáférő személye (személyes adatok), illetve szervezet esetén az a vezető képviselő, aki a hozzáférési felelősséget vállalja. Rögzítendő továbbá a hozzáférés célja, időtartama, az elérhető adatok köre és az adatok felhasználására vonatkozó kötelemények,
- d) a nyilatkozat megszegése esetén a hozzáférési jogosultság azonnal törölendő.

25. Hozzáférési jogosultságok vizsgálata

26. § (1) Az informatikai biztonsági felelős az adatgazdák számára megfelelő jogosultság mellett az Intraneten elérhetővé teszi a szakrendszerekhez hozzáférő felhasználók listáját, amelyet legalább 3 havonta frissít. Az adatgazdák ellenőrzik a jogosultságok kiosztását, valamint a biztosított szerepköröket. Ha eltérést tapasztalnak az általuk engedélyezett adatok, valamint a lista között, akkor a felhasználó közvetlen vezetőjét erről tájékoztatják, és felkérlik az informatikai vezetőt a jogosultság megszüntetésére.

(2) Az informatikai biztonsági felelősnek a felhasználók hozzáférési jogosultságának kezelését minden szervezeti változást követően, de legalább évente át kell vizsgálnia. Meg kell győződnie az adatgazdák számára küldött kivonatok aktualitásáról.

(3) Az új berendezések és alkalmazások általában rendelkeznek alapértelmezett felhasználó/jelszó beállítással. Ezt a telepítés (üzembe helyezés) során minden esetben meg kell változtatni. Egyetlen rendszerben sem maradhat alapértelmezett felhasználói név, illetve alapértelmezett jelszó. Erről minden rendszer telepítése után, és az éves ellenőrzések alkalmával is meg kell győződni.

26. Hozzáférési jogosultságok vizsgálata

27. § Számítógép zárolása: az őrizetlenül hagyott számítógépeket olyan képernyővédővel kell védeni, amely legkésőbb 10 perccel a felhasználó utolsó tevékenysége után automatikusan aktiválódik, zárolja a számítógépet és feloldása csak jelszó alkalmazásával lehetséges.

27. Vírusvédelmi kötelezettség

28. § (1) Alapesetben a védelmet támogató eszközök, hardver és szoftver elemek beszerzése a Tankerületi Központ, üzembe helyezése és üzemeltetés NISZ Zrt. feladata és felelőssége, ettől konkrét esetekben, szerződés alapján el lehet térni, összhangban a vonatkozó jogszabályi előírásokkal és a belső szabályokkal.

(2) Amennyiben a felhasználó a szokásostól eltérő működést, rendellenességet észlel, azt haladéktalanul köteles jelenteni az Ügyfélszolgálat munkatársainak.

28. Felhasználók jogai és kötelezettségei

29. § A felhasználó jogosult:

- a) igénybe venni az Ügyfélszolgálat szolgáltatást,
- b) a Tankerületi Központ informatikai infrastruktúráját a hálózati azonosító nevéhez (user account) hozzárendelt jogosultságok alapján munkaköri feladatai ellátásához használni,
- c) az alapszolgáltatásokon túli, a munkavégzéséhez szükséges informatikai erőforrásokra irányuló igényét a szervezeti egysége vezetőjétől kérni,
- d) indokolt esetben észrevételt tenni az üzemeltető személyzet intézkedéseivel kapcsolatban a saját szervezeti egységének vezetőjénél.

30. § A felhasználó köteles:

- a) a felhasználókra vonatkozó szabályokat betartani,
- b) az informatikai hálózatot rendeltetésszerűen és megfelelően használni,
- c) az üzemeltető személyzet szóbeli, írásbeli szakmai utasításait betartani,
- d) a felfedezett biztonsági problémákat bejelenteni az Ügyfélszolgálat munkatársainak,
- e) a meghibásodásokat bejelenteni az Ügyfélszolgálat munkatársainak,
- f) az Ügyfélszolgálat kérésére a hiba bejelentésének rögzítéséhez szükséges minden adatot, információt – a tőle elvárható pontossággal – megadni,
- g) a saját hálózati azonosító nevét használni és az ehhez tartozó jelszót bizalmasan kezelni,
- h) Tankerületi Központon kívüli forrásból származó adatokon, vagy alkalmazásokon (CD, USB meghajtó, stb.) a munkaállomásra, vagy a hálózatra való feltöltés előtt vírusellenőrzést végezni,
- i) a vírusfertőzésre utaló jelek észlelését azonnal jelenteni kell az Ügyfélszolgálat felé és egyidejűleg a számítógépes munkavégzést fel kell függeszteni.

31. § A felhasználókra vonatkozó tilalmak

- a) az informatikai szolgáltatások igénybevétele során jogszabályokba ütköző cselekmények megvalósítása különösen mások személyiségi jogainak megsértése, szerzői jogok megsértése,
- b) a Tankerületi Központ hálózatához kapcsolódó más – hazai vagy nemzetközi – hálózatok deklarált szabályaiba ütköző cselekmények elkövetése,
- c) a hálózat, illetve erőforrásai működését megzavaró, veszélyeztető események szándékos előidézése,
- d) a hálózatot, illetve erőforrásait indokolatlanul, vagy pazarló módon igénybe vevő funkciók elindítása,
- e) a hálózat erőforrásaihoz, a hálózaton elérhető adatokhoz történő illetéktelen hozzáférés, azok illetéktelen használata, illetve az erre irányuló kísérlet,
- f) a hálózat erőforrásainak, a hálózaton elérhető adatoknak illetéktelen módosítására, megromlására, vagy megsemmisítésére irányuló tevékenység végzése,
- g) a hálózat biztonságát veszélyeztető információk kiszolgáltatása, illetve programok terjesztése,
- h) jogszabályokba ütközően másokra nézve sértő, vallási, etnikai, politikai vagy más jellegű

érzékenységet sértő, zaklató tevékenység végzése,

- i) mások munkájának indokolatlan és túlzott mértékű zavarása vagy akadályozása, különösen kéretlen levelek küldése,
- j) más felhasználók magánjellegű adatainak vagy dokumentumainak illetéktelen megtekintése, másolása,
- k) a hálózat bármely végpontjába informatikus tudta és engedélye nélkül bármilyen eszköz csatlakoztatása (a munkaállomásba csatlakoztatott bármilyen eszközt, USB meghajtót le kell választani és fizikailag el kell távolítani a szükséges felhasználás után),
- l) bármilyen jelszót (password) másokkal megosztani; helyettesítés esetén a felhasználó csak a saját azonosító nevével és jelszavával léphet be,
- m) az informatikai eszközök meghibásodása esetén a hiba kijavítását megkísérelni, azonban meg kell tennie mindazokat az intézkedéseket, amelyekkel az infrastruktúrát további károsodásoktól megóvjá. Ilyen esetben haladéktalanul értesíteni kell az Ügyfélszolgálat munkatársait, és a számítógépes munkavégzést fel kell függeszteni.

32. § (1) A felhasználónak – egyéb jogszabályi feltételek fennállása esetén – kártérítési kötelezettség terhe mellett tilos

- a) a gépek megbontása, a hardver konfigurációk megváltoztatása,
- b) a hálózat megbontása, átstrukturálása, gépek, eszközök engedély nélküli csatlakoztatása,
- c) a munkaállomás kábelezésének megbontása,
- d) a hálózati csatlakozás megszüntetése (kivéve katasztrófahelyzet esetén),
- e) a monitort vagy a számítógép házat bekapcsolt állapotban letakarni, vagy azokon bármit tárolni,
- f) az informatikai berendezések közelébe nagyfeszültségű vagy erősen mágneses eszközt még időlegesen is elhelyezni,
- g) a berendezéseket hőforrás mellé helyezni vagy bármilyen más módon sugárzó hőhatásnak kitenni,
- h) a munkaállomásokon futó víruskeresőt leállítani vagy kiiktatni.
- i) a munkaállomások külső adattároló eszközről történő rendszerindítása, kivéve, ha az informatikai vezető által kiadott – rendszergazdákra, informatikusokra vonatkozó – IT Üzemeltetési Utasítás (a továbbiakban: Üzemeltetési Utasítás) másképpen rendelkezik.

(2) Az informatikai vezető a munkáltatói jogkör gyakorlójánál fegyelmi eljárás megindítását kezdeményezheti, ha a felhasználó jelen Szabályzatot megszegi. Külső felhasználó esetén a kárigény érvényesítésére a polgári jog általános szabályai az irányadók.

V. FEJEZET

ÜZEMELTETÉSRE VONATKOZÓ SZABÁLYOK

29. Általános szabályok

33. § (1) A Tankerületi Központ központi üzemeltetésű informatikai rendszereinek megbízható üzemeltetéséért a NISZ Zrt. a Tankerületi Központtal kötött megállapodás szerint felelős, amely kiterjed az informatikai rendszer erőforrásainak és szolgáltatásainak folyamatos biztosítására, új elemek üzembe helyezésére, az esetlegesen jelentkező hibák kijavítására, a mentések, illetve helyreállítások végzésére és a rendszer használatával kapcsolatos gyorssegély ellátására.

- (2) A központi szakrendszerek üzemeltetésének szabályait az informatikai vezető adott rendszerre vonatkozó – informatikusokra vonatkozó – Üzemeltetési Utasítása tartalmazza, amely leírja az elvégzendő feladatokat az üzemeltetői munkakörben foglalkoztatott szakemberek számára, ilyen minőségükben meghatározza a szerepköröket és felelőségeket a rendszerek használatának jogosultság kiosztása kivételével.
- (3) Amennyiben egy informatikai üzemeltetői munkakörben foglalkoztatott szakember jelen Szabályzat szerinti felhasználóként kerül kapcsolatba az informatikai rendszerrel (pl. felhasználói módon elindít egy alkalmazást), akkor rá is érvényesek a felhasználókra vonatkozó szabályok.
- (4) A központilag üzemeltetett rendszerek napi mentése és a biztonsági archiválásához tartozó feladatok ellátása, a rendszer és az adatállományok visszaállíthatóságának biztosítása a NISZ Zrt. feladata és felelőssége, összhangban a vonatkozó jogszabályi előírásokkal és belső szabályokkal.
- (5) A személyi használatba kiadott informatikai eszközök informatikai támogatását az INFO csak a Tankerületi Központ területén, munkaidőben biztosítja.
- (6) Az üzemeltetéssel kapcsolatos tevékenységek részletes szabályozását az informatikai vezető Üzemeltetési Utasítása tartalmazza. Ennek naprakészen tartásáról az informatikai vezető gondoskodik.

30. Szoftverek telepítése és folyamatos üzemeltetése

- 34. §** (1) A Tankerületi Központ számítógépes hálózatának szerverein, munkaállomásain csak jogtisztta szoftver telepítésére kerülhet sor.
- (2) Szoftvertelepítési feladatot az INFO telepítési jogkörrel rendelkező munkatársai, valamint a NISZ Zrt. rendszergazdái láthatnak el.
- (3) Az alapszolgáltatástól eltérő szoftverigényeket az érintett szervezeti egység vezetője az INFO felé, írásban jelezheti. Az INFO szakmai szempontból megvizsgálja a Tankerületi Központ informatikai architektúráján való üzemeltethetőség lehetőségét, majd indokolt esetben azok beszerzése érdekében a Tankerületi Központ beszerzési szabályainak megfelelően jár el.
- (4) Szabad felhasználású szoftver esetén az INFO, a NISZ Zrt. esetleges bevonásával elvégzi a telepítést, és a szoftver nyilvántartásba vételét.
- (5) Külső szállító cég szoftvertelepítést csak az INFO felügyelete mellett végezhet.
- (6) Az INFO feladata a NISZ Zrt. által megadott, valamint az általa telepített (telepítendő) szoftverek jogtisztaságának ellenőrzése, és a tételes szoftver nyilvántartás vezetése.

31. A NISZ Zrt. feladata

35. § Összhangban a vonatkozó jogszabályi előírásokkal és a belső szabályokkal

- a) az informatikai infrastruktúra működőképességének biztosítása,
- b) a felhasználói igényeket kielégítő, szabványos telepítési eljárások kidolgozása, a hardverek, szoftverek átvétele a szállítótól,
- c) szerver operációs rendszerek telepítése és beállítása,
- d) a szoftverek biztonsági másolatainak elkészítése és a másolatok – védelmi előírásoknak – megfelelő tárolása,
- e) szerverprogramok szoftverkövetésének biztosítása, az új verziók megismerése, beszerzésük szakmai előkészítése, a korábbi verziók aktualizálása,
- f) az aktualitásukat veszített, tovább nem alkalmazható szoftverek selejtezésének kezdeményezése.