SZOLNOKI
TANKERÜLETI
KÖZPONT

A Szolnoki Tankerületi Központ

KLIK/103/ 12 /2017. (...) szabályzata

A Szolnoki Tankerületi Központ informatikai rendszereinek felhasználásáról szóló szabályzata

Készítette:

Szolnok, 2017. ..... „.....”

Szolnoki Tankerületi Központ 01

.....

Szutorisz-Szügyi Csongor

tankerületi igazgató

Szolnoki Tankerületi Központ

A Szolnoki 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 középirányítói hatáskörömben eljárva, a Klebelsberg Központ Szervezeti és Működési Szabályzatáról szóló 61/2016. (XII. 29.) EMMI utasítás 40. §-a alapján jóváhagyom:

Budapest, 2017. ..november..... „2.....”

Klebelsberg K... Elnök

.....

dr. Solti Péter

elnök

Klebelsberg Központ

TARTALOM

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 8
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 9
8. Az internet használatával kapcsolatos szabályok megsértőivel szembeni szankciók 10
9. Az elektronikus levelezés általános szabályai 10
10. A hivatali postafiókokkal kapcsolatos szabályok 11
11. Az elektronikus levelezés címzési előírásai 12
12. A levéltovábbítás 12
13. Az elektronikus levelezés etikettje 13
14. Az elektronikus levelezés magáncélú használata 13
15. Hálózati megosztások, szolgáltatások 13
IV. Fejezet 13
16. Általános szabályok 13
17. Informatikai jogosultság igénylés 14
18. Jelszavak képzése 14
19. Jelszavak kezelése 14
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 15
23. Felhasználói jogosultság megszüntetése 16
24. Speciális hozzáférések 16

25. Hozzáférési jogosultságok vizsgálata 16
26. Hozzáférési jogosultságok vizsgálata 17
27. Vírusvédelmi kötelezettség 17
28. Felhasználók jogai és kötelezettségei 17
V. Fejezet 19
29. Általános szabályok 19
30. Szoftverek telepítése és folyamatos üzemeltetése 19
31. A NISZ Zrt. feladata 20
32. Az MBO feladatai 20
33. Hardver berendezések telepítése és folyamatos üzemeltetése 20
34. Az informatikai hálózat fejlesztése és folyamatos üzemeltetése 21
35. Egyéb hálózati szolgáltatások 21
36. Adatkezelés szabályozása az informatikai rendszerekben 22
37. Hivatali adatok kezelése 22
38. Adatbázis-módosítási jogok 22
39. Fejlesztésre és beszerzésre vonatkozó szabályok 22
40. Rendszerek bevezetése 23
41. A beszerzésre és szabványosítására vonatkozó szabályok 23
HARMADIK RÉSZ 24
Záró rendelkezések 24
MELLÉKLETEK 25
1. melléklet 25
Jogosultságigénylő lap 25
2. melléklet 26
Jogosultságigénylő nyilatkozat 26
3. melléklet 28
Jogosultság igénylő lap VPN rendszer hozzáférési jogosultság igényléséhez, módosításához és visszavonásához 28
4. melléklet 29
Adatkezelési hozzájárulás 29
5. melléklet 32
Servicedesk bejelentések csoportosítása 32
6. melléklet 33
NISZ minimumkövetelmények 33

A Szolnoki 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 szakrendszerek 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:* Műszaki és Beszerzési Osztály (a továbbiakban: MBO) 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 előbbiekben meghatározott cél elérését biztosítják.
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 tenyérnyomat, 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 végrehajtatja.

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 vezetőn pedig ezek vezetőit kell érteni.
22. *Bizalmasság:* 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. *Információ:* bizonyos tényekről, tárgyakról vagy jelenségekről hozzáférhető formában megadott megfigyelés, tapasztalat vagy ismeret, amely valakinek a tudását, ismeretkészletét, annak rendezettségét megváltoztatja, átalakítja, alapvetően befolyásolja, bizonytalanságát csökkenti vagy megszünteti.
33. *Információs rendszer:* azon eljárások, tevékenységek összessége, amelyek a szervezet működéséhez és irányításához szükséges információkat tárolják, előállítják, szétosztják.
34. *Informatika:* az információ rendszeres és automatikus – elsősorban számítógéppel történő – rögzítésével, tárolásával, feldolgozásával és továbbításával foglalkozó tudomány.

35. *Informatikai eszköz:* az informatikai és információszolgáltatás valamennyi tárgyi, illetve tárgyiasult szellemi komponense, így a számítógépek, számítógépes hálózatok és kapcsolódó eszközök, szoftverek, konfigurációk, rendszer-beállítási paraméterek, dokumentációk stb.

36. *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.

37. *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 adatosztályozás 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.

38. *Informatikai rendszer:* a hardverek és szoftverek olyan kombinációjából álló rendszer, amit az adat-, illetve információ-feldolgozás különböző feladatainak teljesítésére alkalmaznak.

39. *Írás, írási folyamat:* az adat rögzítésének fizikai folyamata valamilyen (papír alapú, mágneses, optikai, stb.) adathordozóra.

40. *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.

41. *ITIL:* informatikai rendszerek üzemeltetésére és fejlesztésére szolgáló módszertan, illetve szabvány- és ajánlás-gyűjtemény.

42. *LAN:* helyi adathálózat.

43. *Log, log-fájlok:* a rendszernapló bejegyzései.

44. *Letöltés:* adattartalom (szöveges, kép, hang, program, stb.) importálása saját gépre. *MBO: Műszaki és Beszerzési Osztály*, az informatikáért, informatikai szolgáltatásokért felelős szervezeti egység.

45. *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).

46. *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).

47. *Működőképesség:* A rendszernek és elemeinek az elvárt és igényelt üzemelési állapotban való fennmaradása. A működőképesség fogalom sok esetben azonos az üzembiztonság fogalommal.

48. *Olvasás, olvasási folyamat:* az előzőleg már rögzített adat dekódolása és megjelenítése.
49. *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).
50. *Output:* kijövő adat, információ. A rendszer által feldolgozott adatok fizikai megjelenítése.
51. *RBK:* Rendszer Beavatkozási Kérelem.
52. *Rendelkezésre állás*: annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek.
53. *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.
54. *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.
55. *SLA:* Service Level Agreement. Szolgáltatási szint szerződés.
56. *Szoftver:* az informatikai rendszer logikai része, amely a működés vezérléséhez szükséges.
57. *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.
58. *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 javaslattételi, az alaphozzáférést tekintve pedig engedélyezési joga van, azaz meghatározza, hogy az irányítása, vagy vezetése alatt álló munkatársnak 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.
59. *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 oldalakról történő letöltések által.

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 MBO 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 MBO biztosít számukra az érintett szervezeti egység vezetőjének döntése alapján.

(3) Az alapszolgáltatástól eltérő, szakmailag indokolható igényeket az érintett szervezeti egység vezetője az MBO felé írásban jelzi. Az adott igényt kiszolgáló informatikai eszközök specifikálása és kiválasztása az MBO 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 MBO 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 MBO vezetője tájékoztatja a tankerületi igazgatót. A naplófájl készítésének és ellenőrzésének célja, hogy a felhasználók internethasználata 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 közerkölcsöt 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 mindenkire 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 korlátot 2048 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 MBO legfeljebb 3 hónap időtartamra, az adott címre automatikus válaszadási szabályt állít be, amely a feladót értesíti a változásról. A fiókot 6 hónap után a fiók archiválását követően 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 fájlt 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 címzetteknél 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 belülre és kívülre nem szabad tömeges mennyiségben (200 címzettet meghaladóan) küldeni vagy továbbítani, kivéve, ha a Tankerületi Központ működése szempontjából indokolt az e-mail tartalom minden címzetthez 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 üzenet küldése a Tankerületi Központon kívülre 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 vezetéknevéből és keresztnevének (keresztneveinek) első betűjéből képződik.

(6) Kettős családnév esetén az elöl álló családnevet 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 keresztnevek esetén a kettős betű első betűjét kell használni (pl. Kovács Csilla esetén „kovacsc"). Abban az esetben, ha az így képzett szó a NISZ Informatikai Rendszerében már foglalt, akkor a keresztnév (keresztnevek) következő betűjének felhasználásával az azonosítót képezni (pl. Kovács Béla és Kovács Bernadett esetén az egyik "kovacsb" 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, beszkennelt 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 Ügyfélszolgálathoz 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 beszkennelt jogosultságigénylő lapot, az 4. melléklet szerinti, beszkennelt 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, beszkennelt 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 szervezeten 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 MBO 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 MBO ennek birtokában teszi meg a következő intézkedéseket.

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

(5) Az MBO a zárolás után 30 nappal a felhasználó postafiókjának, valamint a személyes könyvtárában tárolt adatainak – a szükséges dokumentumok archiválását követően - törléséről intézkedik. A zárolás és a törlés közötti időtartam meghosszabbítására a tankerületi igazgató jogosult.

(6) A felhasználó jogosultságainak megszüntetésével egyidejűleg köteles az MBO 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 MBO a határidő lejárta 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 kötelmek,

d) a nyilatkozat megszegése esetén a hozzáférési jogosultság azonnal törlendő.

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 felkérik 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, megrongálására, 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 érzékenységüket 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 megóvja. 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 felelősségeket 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 MBO 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 jogtiszta szoftver telepítésére kerülhet sor.

(2) Szoftvertelepítési feladatot az MBO telepítési jogkörrel rendelkező munkatársai, valamint a NISZ Zrt. rendszergazdái láthatnak el.

(3) Az alapszolgáltatástól eltérő szoftverigényeket az érintett szervezeti egység vezetője az MBO felé, írásban jelezheti. Az MBO 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 MBO, a NISZ Zrt. esetleges bevonásával elvégzi a telepítést, és a szoftver nyilvántartásba vételét.

(5) Külső szállító cég szoftvertelepítést csak az MBO felügyelete mellett végezhet.

(6) Az MBO 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 vesztett, tovább nem alkalmazható szoftverek selejtezésének kezdeményezése.

32. Az MBO feladatai

36. § (1) Az MBO feladatai:

a) saját készítésű szoftverek esetén a szükséges dokumentációk elkészítése, illetve a telepített szoftverek dokumentációjának átvétele a szállítótól,

b) a szoftverek telepítése, illetve a szoftverek telepítésének megszervezése, amennyiben a telepítés külső erőforrás igénybevételével történik,

c) a szoftverkövetés biztosítása, az új verziók megismerése, beszerzésük szakmai előkészítése, a korábbi verziók aktualizálása,

d) az aktualitásukat vesztett, tovább nem alkalmazható szoftverek selejtezésének kezdeményezése,

e) a felhasználók szoftver üzemeltetési problémáinak megoldása folyamatos szakmai tanácsadással, helyszíni hibaelhárítással vagy ügyfélszolgálati eszközök felhasználásával.

(2) Megfelelő képzettséggel és szakmai tudással rendelkező informatikus egyszerre egy időben több rendszergazdai feladatkört is elláthat, ha a feladatkörök nem zárják ki egymást.

33. Hardver berendezések telepítése és folyamatos üzemeltetése

37. § (1) A beszerzett hardver berendezések telepítésre történő előkészítése és a rendeltetési helyére való telepítése, a szükséges hardverbővítés, illetve csere a NISZ Zrt. feladata. A feladatot indokolt esetben átadhatja a szállító részére, amelynek során a telepítéskor a NISZ Zrt., illetve az MBO kijelölt dolgozójának felügyelete kötelező.

(2) Informatikai eszközök használatba vételére, függetlenül a beszerzésének forrásától, vagy módjától (pl. projekt keretei között beszerzett eszközök), ugyanazok a szabályok vonatkoznak:

a) a szállító az eszközökből egy példányt a NISZ Zrt. telephelyére előzetesen eljuttatja,

b) a NISZ Zrt. az eszközök üzemeltetését bevizsgálja,

c) sikeres bevizsgálást követően az összes eszköz a NISZ Zrt. raktárába kerül, és innen az informatikai vezető utasítása alapján kerül kihelyezésre,

d) sikertelen bevizsgálás esetén az eszközök vagy nem, vagy az informatikai vezető írásos hozzájárulása, és külön utasítása alapján helyezhetőek használatba.

(3) A beszerzések során törekedni kell a NISZ Zrt. által meghatározott minimum követelmények betartására (lásd 6. számú. melléklet).

(4) A központi rendszer hardverein végrehajtandó módosítások elvégzése, az informatikai vezető felé történő benyújtásával kezdeményezhető.

(5) A nyomtatók beszerzésekor, telepítésekor az egyedi nyomtatók helyett törekedni kell a multi-funkciós eszközökkel történő nyomtató központok kialakítására.

34. Az informatikai hálózat fejlesztése és folyamatos üzemeltetése

38. § (1) Hálózatfejlesztés tekintetében az MBO felelőssége, hogy a Tankerületi Központ Informatikai Stratégiájának hatályba lépését követően, a megfelelő hálózatfejlesztés szakmai terve rendelkezésre álljon és a beszerzés az abban lefektetett szakmai követelményeknek, valamint a fejlesztési irányelveknek megfelelően valósuljon meg.

(2) A NISZ Zrt. biztosítja a Tankerületi Központ informatikai hálózata egészének, mint rendszernek a megbízható működését amely különösen

a) a hálózati eszközök rendszeres ellenőrzésének és felügyeletének,

b) a hálózati topológia folyamatos megjelenítésének és a fizikai vagy virtuális LAN-ok működése áttekintésének, tervezésének,

c) hálózati eszközleltár elkészítésének és naprakészen tartásának,

d) a hatáskörébe tartozó berendezésekkel kapcsolatos hibabejelentések fogadásának és azok elhárításának megszervezésének,

e) a munkaállomások, nyomtatók, szkennerek nyilvántartása elkészítésének és naprakészen tartásának, hálózatba kapcsolásának, megbízható üzemeltetésének és a feladatainak

f) a hálózati berendezések megelőző karbantartásának, tisztításának, valamint a szükséges konfiguráció módosításoknak

elvégzését jelenti.

(3) Azokat a helyiségeket, amelyekben az informatikai infrastruktúra elemei üzemelnek, zárral kell ellátni és a jogosult használóik távollétében zárva kell tartani.

35. Egyéb hálózati szolgáltatások

39. § (5) A WLAN eszközök helytelen konfigurációja a Tankerületi Központ zárt – és az esetleges behatolási pontokon többszörösen védett – hálózatán biztonsági réseket jelentenek.

(2) Amennyiben a meghatározott hardver és szoftver feltételeknek a WLAN hálózati elemek nem felelnek meg, azok telepítése, üzemeltetése és használata nem engedélyezett. A megfelelő minősítéssel rendelkező eszközök esetén jogosultsági rendszerrel védeni kell a hálózatot, titkosítással pedig az adatkommunikációt.

(3) A Tankerületi Központ jelen informatikai és hálózati struktúrájából adódóan az IEEE802.11i szabvány szerinti WPA2 kialakítás kivitelezhető, a későbbiekben azonban mindenképpen a WPA Enterprise megoldást, vagy magasabb biztonsági szintet nyújtó megoldást szükséges alkalmazni.

(4) Az Access Point (továbbiakban AP) telepítése, üzembe helyezése minden esetben a Tankerületi Központ MBO munkatársa által dokumentált formában történik. Az AP-k kezelése, felügyelete vezeték

nélküli hálózaton keresztül nem engedélyezett.

(5) Az AP-kat hálózatra csatlakoztatni kizárólag olyan megoldással lehet, hogy szükség esetén haladéktalanul leválaszthatóak legyenek róla.

(6) Az egyes elhelyezési lehetőségek vizsgálatával (klienssel történő mérésével), az üzemelési hely (az esztétikai szempontokat is figyelembe véve) az épületen kívül legkisebb mérhető sugárzást biztosító ponton jelölhető ki.

(7) Az MBO az AP-kon keresztül folytatott hálózati tevékenységet naplózza. A megszokottól eltérő tevékenység esetén a körülményt haladéktalanul jelezni kell az Informatikai Biztonsági Felelős felé.

36. Adatkezelés szabályozása az informatikai rendszerekben

40. § Az adatkezelés részletes szabályait külön szabályzat tartalmazza.

37. Hivatali adatok kezelése

41. § (1) Az egyes eljárások tartama alatt a Tankerületi Központ gondoskodik róla, hogy a személyes adatok védelme biztosított legyen.

(2) A Tankerületi Központ közérdekű adataihoz, információihoz, valamint a közérdekből nyilvános adataihoz a felhasználók korlátozás nélkül hozzáférhetnek.

(3) A fenti pontba nem tartozó hivatali adatokhoz (személyes adat, különleges adat) kizárólag az arra feljogosított személyek férhetnek hozzá.

(4) A Tankerületi Központ informatikai rendszereiben tárolt adatok tartalmáért az adatgazda felelős.

(5) A Tankerületi Központ informatikai rendszereinek adatbázisaiból kizárólag azok a személyek kérdezhetnek le adatokat, akiknek a kérdezendő adatokra vonatkozó intézkedési vagy felhasználási joguk van.

(6) A Tankerületi Központ minden dolgozója felelősséggel tartozik a munkájával kapcsolatban a birtokában lévő, illetve tudomására jutott információ rendeltetésszerű kezeléséért és felhasználásáért.

(7) Az adatkezeléssel megbízott munkatársaknak az informatikai rendszerek használatára történő kiképzése, és továbbképzése, naprakész nyilvántartása az alkalmazásgazda, illetve az MBO feladata.

(8) Az MBO rendszerfejlesztői, alkalmazás üzemeltetői az informatikai vezető engedélyével technikai hozzáférési joggal rendelkeznek a kezelésükben lévő minden üzemeltetésre átvett vagy központi fejlesztésű adatbázisra. A Tankerületi Központ informatikai rendszerének zavarmentes üzemeltetéséhez szükséges technikai hozzáférési jog nem jelent felhasználói jogot.

38. Adatbázis-módosítási jogok

42. § (1) Az adatbázisok adattartalmáért, az adatok rögzítéséért, módosításáért és törléséért az adatgazda felel, aki meghatározza a jogosultsággal rendelkezők személyét és az adott rendszerhez történő hozzáférési jogosultság mértékét. Az MBO erre kijelölt adatbázis rendszergazdája az üzemeltetés biztosítása érdekében technikai műveleteket hajthat végre az adatbázisokon, azonban az adattartalmon semmiféle változtatást nem végezhet. Az adatbázis és adatállománya szerzői jogi védettséget élvez.

(2) Adatbázis biztonsági mentését (dump), az informatikai vezető rendelhet el.

39. Fejlesztésre és beszerzésre vonatkozó szabályok

43. § (1) Legfontosabb célkitűzés a Tankerületi Központ munkájának hatékony támogatására az egységes, integrált informatikai rendszer létrehozása.

(2) Az egységes, integrált informatikai rendszer kialakítása az MBO feladata és felelőssége.

(3) Az informatikai fejlesztéseket a Tankerületi Központ középtávú Informatikai Stratégiája, valamint a közbeszerzésekről szóló törvény rendelkezései alapján kell végrehajtani. Az informatikai fejlesztéseket időtartam, értékhatár, vagy a beruházás tárgya alapján projekt keretében, a Tankerületi Központ által jóváhagyott célokmány, engedélyokirat alapján, tervezetten, jól ellenőrizhetően, határidőre és költségkereten belül kell megvalósítani. Kiemelt cél továbbá, hogy a projekt eredményeként a felhasználók munkáját hatékonyan támogató, azok igényeinek megfelelő termék jöjjön létre.

(4) A projekt megvalósításáért az MBO támogatásával a Tankerületi Központ projektszervezete felelős.

(5) Informatikai szolgáltatások üzemeltetésre történő átvételére szigorú belső (pl. projekt szervezettől MBO felé), vagy külső (fejlesztőtől az MBO felé) történő átadás-átvételi procedúra keretei között van kizárólag lehetőség.

40. Rendszerek bevezetése

44. § (1) Rendszerfejlesztési projektek esetén kiemelten fontos fázis a rendszerek éles indulásának előkészítése.

(2) A projektirányító feladata, hogy részletes ütemtervet készítsen, és szigorúan ellenőrizze a feladatok végrehajtását.

(3) A rendszer bevezetésének legfontosabb előfeltételei

a) a sikeres felhasználói és üzemeltetői oktatás,

b) az aktualizált felhasználói és üzemeltetési dokumentáció,

c) a sikeres felhasználói elfogadási teszt és

d) a rendszer bevezetését elrendelő intézkedés.

(4) A megfelelő minőségű és mennyiségű oktatás elvégzése a fejlesztők feladata. A felhasználók és üzemeltetők oktatáson való részvételét az illetékes szervezeti egységek vezetőinek kell biztosítani.

(5) A kialakított rendszert és a kapcsolódó dokumentumokat csak akkor lehet elfogadni és külső fejlesztés esetén a teljesítést igazolni, ha a projekt végrehajtásáért felelős vezetők, szerepkörüknek megfelelően teljes körűen nyilatkoznak arról, hogy a rendszer megfelel a követelményeknek, és azok üzembe helyezhetők. Felhasználók esetén ez a funkcionális, informatikai vonatkozásban pedig a nem funkcionális követelményeknek való megfelelést jelenti.

(6) Az informatikai rendszerek adatokkal történő feltöltése, annak tervezése a szolgáltatást elsődlegesen használó szervezeti egység(ek), a projektekért felelős szervezeti egység, az érintett projekt szervezet, valamint az MBO közös és egyetemleges felelőssége.

41. A beszerzésre és szabványosítására vonatkozó szabályok

45. § (1) Az informatikai beszerzések tekintetében a Tankerületi Központ beszerzésekre vonatkozó szabályzatai és eljárásrendjei az irányadók. A beszerzések műszaki tartalmának meghatározásában pedig az MBO ad módszertani támogatást.

(2) Informatikai fejlesztési- és eszközbeszerzési igényeit az igénylő szervezeti egység az MBO felé írásban jelezheti. Az igényhez szakmai indoklást kell adni.

(3) Az igények elbírálása, illetve az adott szervezeti egység részére kivitelezhető megoldási javaslat tétele az MBO feladata.

(4) Az informatikai fejlesztések megkezdésére csak akkor kerülhet sor, ha annak fedezete a költségvetésben biztosított és az ahhoz szükséges célokmány, engedélyokirat jóváhagyásra került.

(5) A beszerzések során alkalmazott műszaki specifikáció, azzal egyenértékű termékek meghatározása, garanciális és jótállási feltételek meghatározása az MBO feladata.

(6) A beszerzés módjának, engedélyeztetésének, illetve a beszerzések lebonyolítása a Gazdálkodási , Műszaki és Pályázati Főosztály feladata.

(7) Más szervezeti egységek által indított informatikai tárgyú beszerzéseket informatikai szakmai szempontból az MBO ellenőrzi, szakmailag indokolt esetben, a beszerzés indítása előtt, vagy annak folyamatában pontosítja.

(8) Informatikai tárgyú beszerzések esetén, annak forrásától függetlenül, a beszerzés lebonyolításához szükséges „beszerzés tárgya szerinti" szakértőt, bíráló bizottsági tisztségviselőt az informatikai vezető jelöli ki.

(9) A Tankerületi Központ szervezeti egységei által igényelt informatikai rendszerek koncepciójának, előzetes költségbecslésének elkészítése, a fejlesztés előkészítése, megvalósítása, a rendszer bevezetése és technikai üzemeltetése a NISZ Zrt. támogatásával az MBO feladata a szakmailag érintett szervezeti egység közreműködése mellett. Ettől eltérni csak indokolt esetben, az igénylő szervezeti egység és az informatikai vezető írásos megállapodása esetén lehet.

(10) Az informatikai rendszerben alkalmazni kívánt informatikai elemek (szoftverek, hardver valamint hálózati berendezések, továbbá szolgáltatások) beszerzése során az adott informatikai eszközt igénylő felhasználó vagy szervezet legfontosabb igényeit a rendelkezésre álló anyagi erőforrások függvényében kell kielégíteni a beszerzés anyagi fedezete és felhasználhatósága biztosításának függvényében.

(11) A beszerezni kívánt termék kizárólag jogtiszta forrásból származhat, a termékre vonatkozó licenc egyértelmű ellenőrizhetősége mellett.

(12) A termék beszerzése csak a szoftver gyártójától, vagy annak hivatalos viszonteladójától történhet.

(13) A terméknek meg kell felelnie a Tankerületi Központ információs infrastruktúra egységesítési törekvéseinek és utasításaiban foglaltaknak.

HARMADIK RÉSZ

ZÁRÓ RENDELKEZÉSEK

46. § (1) Jelen szabályzat a Klebelsberg Központ elnökének jóváhagyását követő 5. napon lép hatályba.

(2) Jelen szabályzat előkészítéséért és aktualizálásáért az MBO felelős.

(3) Jelen szabályzat hatályba lépésével egyidejűleg hatályát veszíti az e tárgykörben kiadott korábbi szabályozás.

MELLÉKLETEK

1. melléklet

Jogosultságigénylő lap

Felhasználó neve:	
Szervezeti egység neve:	
Iroda/Főosztály:	
Osztály:	
Telefon:	
Hálózati azonosító *:	

Az alábbi jogosultságok a fent feltüntetett felhasználóra vonatkoznak.

Dátum	**Szolgáltatás megnevezése**	**Jogosultsági szint vagy egyéb bejegyzések**	**Rendszergazda vagy adatgazda aláírása**
	Hálózati azonosító kiosztása		

Kelt: ..... PH

Igénylő aláírása	Kérelmező szervezeti egység vezetője

* Rendszergazda tölti ki

2. melléklet

Jogosultságigénylő nyilatkozat

a Tankerületi Központ által biztosított elektronikus levelező rendszer részét képező névre szóló postafiók és naptár hozzáférési jogairól

Alulírott _____(név), a Tankerületi Központ

_____ _____ (szervezeti egység neve), **informatikai felhasználója** aláírásommal igazolom, hogy a Tankerületi Központ által biztosított MS Outlook for Windows elektronikus levelező rendszer-szoftver részét képező, nevemre szóló postafiók és naptár hozzáférését az alábbiakban felsorolt személyek részére, és a megjelölt jogokkal biztosítom:

Elektronikus levelező postafiókhoz hozzáférési jog/meghatalmazás biztosítása

1./ Név: ....., beosztás: .....részére

- ☐ e-mail küldése a nevemben
- ☐ egyéb .....

2./ Név: ....., beosztás: .....részére

- ☐ e-mail küldése a nevemben
- ☐ egyéb .....

☐ Nem biztosítok hozzáférési jogot/meghatalmazást a nevemre szóló postafiókomhoz.

☐ A postafiók(ok) tulajdonosa(i) által biztosított hozzáférési jogokon kívül nem rendelkezem közvetlen hozzáférési joggal más, a Tankerületi Központ által kezelt postafiókokhoz.

Naptár megosztása/hozzáférési jog biztosítása

1./ Név: ....., beosztás: .....részére

- ☐ olvasás
- ☐ írás
- ☐ elemek törlése
- ☐ egyéb

2./ Név: ....., beosztás: .....részére

- ☐ olvasás
- ☐ írás
- ☐ elemek törlése
- ☐ egyéb

3./ Név: ....., beosztás: .....részére

- ☐ olvasás
- ☐ írás
- ☐ elemek törlése
- ☐ egyéb

4./ Név: ....., beosztás: .....részére

- ☐ olvasás
- ☐ írás
- ☐ elemek törlése
- ☐ egyéb

5./ Név: ....., beosztás: .....részére

- ☐ olvasás
- ☐ írás
- ☐ elemek törlése
- ☐ egyéb

☐ Nem biztosítok hozzáférést/nem osztom meg a naptáramat.

☐ A naptár(ak) tulajdonosa(i) által biztosított hozzáférési jogokon kívül nem rendelkezem közvetlen hozzáférési joggal más, a Tankerületi Központ által kezelt postafiókhoz tartozó naptárhoz.

Tudomásul veszem, hogy az Informatikai Szabályzatról szóló szabályzatban foglaltak betartását a tankerületi igazgató által kiadott megbízólevéllel rendelkező személy jogosult ellenőrizni.

Kelt: _____, 20 _____ hó _____ nap.

_____

nyilatkozattevő aláírása

A nyilatkozat egy példányát az érintett szervezeti egység vezetőjénél kell megőrizni.

3. melléklet

Jogosultság igénylő lap VPN rendszer hozzáférési jogosultság igényléséhez, módosításához és visszavonásához

Iktatószám:.....

Igénylő adatai (igénylő tölti ki, Tankerületi Központ dolgozó esetén csak a *-gal jelölt mezőket)

*Igénylő családi neve:	
*Igénylő utóneve(i):	
Igénylő születési családi neve:	
Igénylő születési utóneve(i):	
Igénylő születési helye, ideje:	
Igénylő anyja születési családi és utóneve(i):	
*Igénylő szervezeti egység vagy külső cég neve:	
Igénylő külső cég székhelye:	
Igénylő telefonszáma:	
Igénylő e-mail címe:	
Igényelt jogosultság érvényességének kezdete:	
Igényelt jogosultság érvényességének vége:	

Igényelt jogosultság adatai

Kategória (**igény** ☐, **visszavonás** ☐):	**Belső** ☐ **Külső** ☐
Külsős felhasználó esetén az elérni kívánt	
Jóváhagyó személy neve:	
Jóváhagyó személy beosztása:	
Jóváhagyás dátuma:	
Jóváhagyó (szervezeti egység vezető) aláírása:	

Jogosultság beállítás adatai (végrehajtó személy tölti ki):

Felhasználó login neve az Active Directory-ban:	
Felhasználó csoporttagsága az Active	**Belső** ☐ **Külső** ☐
Jogosultság beállítását végző személy neve:	
Jogosultság beállítás dátuma:	
Engedélyező aláírása:	

Megjegyzés:

Kérem, hogy a megnevezett a megjelölt időponttól kezdődően a táblázatban megadott jogosultságokkal rendelkezzen.

Kelt: .....

PH.

....

Igénylő aláírása Kérelmező szervezeti egység vezetője

4. melléklet

Adatkezelési hozzájárulás

A Tankerületi Központ Műszaki és Beszerzési Osztálya a felhasználók (érintettek) személyes adatait bizalmasan, a hatályos jogszabályi előírásokkal összhangban kezeli, gondoskodik azok biztonságáról, megteszi azokat az intézkedéseket, amelyek a vonatkozó jogszabályi rendelkezések érvényre juttatásához szükségesek. Felhasználóink kérése esetén a kérelemben foglaltaknak megfelelően minden esetben részletes tájékoztatást nyújtunk a kezelt személyes adatokról, az adatkezelés céljáról, jogalapjáról, időtartamáról és az adatkezeléssel összefüggő tevékenységről.

Alulírott

családi és utóneve : .....

születési családi és utóneve: .....

születési helye és ideje: .....

anyja születési családi és utóneve: .....

személyi igazolvány száma: .....

ezennel hozzájárulok ahhoz, hogy a Tankerületi Központ ... Informatikai (Fő)osztálya a - jelen nyilatkozat elválaszthatatlan részét képező - alábbi tájékoztatóban foglalt keretek között a meghatározott személyes adataimat az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvényben foglaltaknak megfelelően nyilvántartsa és kezelje.

Dátum: ....., ...

.....

aláírás

Adatkezelési tájékoztató

1. Az adatkezelő neve:

Tankerületi Központ ... Informatikai (Fő)osztálya (a továbbiakban: MBO)

2. Az adatkezelő címe:

Székhely: 1054 Budapest, Bajcsy-Zsilinszky út 42-46.

3. Az adatkezelő elérhetősége:

Email: .....@kk.gov.hu

4. Az adatkezelés célja:

A Tankerületi Központ informatikai biztonságának megteremtése és biztosítása céljából egyértelműen azonosítani szükséges a VPN rendszerhez hozzáférési jogosultsággal rendelkező felhasználók személyét.

5. Az adatkezelés jogalapja:

Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Info tv.) 5. §-a szerint az érintett *jelen hozzájárulása.*

6. A kezelt adatok köre:

Az érintett neve, születési helye és ideje, anyja neve, személyi igazolvány száma, telefonszáma, érintett email címe, login neve.

7. Adattovábbítás:

Az MBO az általa vezetett nyilvántartásban szereplő adatokat - a Tankerületi Központon belül – zártan kezeli, harmadik fél részére a jogszabályi kötelezettségeken kívül, ideiglenesen sem teszi hozzáférhetővé. A kezelt adatok reklámozási és egyéb üzleti célból történő felhasználása kizárt.

8. Ki ismerheti meg az adatokat:

Az MBO által vezetett nyilvántartásba - eljárásában indokolt mértékig – ellenőrzés céljából jogosult betekinteni, illetve az MBO hozzájárulásával abból adatokat átvenni:

a) tankerületi igazgató,

b) az MBO vezetője,

c) meghatározott körben az MBO vezetője által feljogosított - az MBO alkalmazásban álló - személy, célhoz kötötten munkavégzése céljából, a munkaköri leírásban rögzítettek szerint,

d) saját adatai tekintetében az adatbázisban szereplő személy,

e) feladatkörükben eljárva a nemzetbiztonsági szolgálatok, valamint a közszolgálati jogviszonnyal összefüggésben indult büntetőeljárásban a nyomozó hatóság, az ügyész és a bíróság,

f) az ügyészi törvényességi feladatkörében eljárva az ügyész.

9. Az adatkezelés időtartama:

A VPN rendszerhez történő érvényes hozzáférés időtartama alatt - az ahhoz szükséges feltételek fennállása esetén, – ezt követően a hozzáférési jogosultság megszűnésétől számított 5 évig.

Az MBO törli a nyilvántartásból az érintett adatait az érintett ilyen irányú kérelme alapján. Ebben az esetben az érintett hozzáférési jogosultsága megszűnik.

A személy adatainak törlését személyesen vagy meghatalmazott képviselője útján, továbbá elektronikus formában a MBO-nél írásban kérheti.

10. Az érintett tájékoztatása, adatainak helyesbítése, kijavítása:

Az érintett kérelmére az MBO tájékoztatást ad az általa kezelt adatokról, az adatkezelés céljáról, jogalapjáról, időtartamáról és az adatkezeléssel összefüggő tevékenységéről, továbbá arról, hogy kik és milyen célból kapják vagy kapták meg az adatokat.

Az érintett kérelmére saját adatairól a nyilvántartásból kivonatot, másolatot, illetve szóbeli tájékoztatást kell adni. A tájékoztatás ingyenes, ha a tájékoztatást kérő a folyó évben azonos adatkörre vonatkozóan tájékoztatási kérelmet az adatkezelőhöz még nem nyújtott be. Egyéb esetekben költségtérítés állapítható meg. A már megfizetett költségtérítést vissza kell téríteni, ha a tájékoztatás kérése helyesbítéshez vezetett. A tájékoztatást az MBO a kérelem beérkezésétől számítva legkésőbb 30 napon belül megadja.

Az érintett adatairól tájékoztatást, adatainak helyesbítését, kijavítását, törlését vagy zárolását személyesen vagy meghatalmazott képviselője útján, továbbá elektronikus formában az MBO-nál írásban kérheti.

Az érintett, jelen „Adatkezelési tájékoztató" elválaszthatatlan részét képező „Adatkezelési hozzájárulás" aláírásával kijelenti, hogy a Tankerületi Központ Informatikai Szabályzatról szóló szabályzatban foglalt - a VPN rendszerhez történő hozzáféréssel kapcsolatos - szabályokat megismerte és azokat kötelező jellegűnek tekinti magára nézve. Az érintett jogérvényesítési lehetőségeit az Info tv., valamint a Polgári Törvénykönyvről szóló 2013. évi V. törvény alapján bíróság előtt gyakorolhatja, továbbá a személyes adatai védelmének érvényesülése ellenőrzése és elősegítése érdekében a Nemzeti Adatvédelmi és Információszabadság Hatósághoz fordulhat. (címe: 1125 Budapest, Szilágyi Erzsébet fasor 22/c, email: ugyfelszolgalat@naih.hu)

11. Adatkezelés nyilvántartási száma:

NAIH-

Budapest, ... „....."

5. melléklet

Servicedesk bejelentések csoportosítása

1. A bejelentést rögzítő Servicedesk munkatárs minden helyben nem megoldott bejelentést az alábbi - **hivatali munkaidő alatti** - sürgősségi kategóriák szerint csoportosít:

A) sürgősségi kategóriák	B) hiba elhárításának	
	megkezdése	befejezése
1. azonnali	0,5 órán belül	8 órán belül
2. sürgős	4 órán belül	16 órán belül
3. gyors	8 órán belül	24 órán belül
4. normál	8 órán belül	168 órán belül

Az azonnali sürgősségi kategóriába sorolt feladatok elvégzését munkaidőn kívül is a fenti táblázatban meghatározott időponton belül meg kell kezdeni és elvégezni.

6. melléklet

NISZ minimumkövetelmények

KORMÁNYZATI BESZERZÉSI MŰSZAKI SZINT 2016

MUNKAÁLLOMÁS

Általános elvárások

Az ajánlott termékek csak új, a szállítást megelőzően sehol nem használt eszközök lehetnek, amelyet a szállítás során, amennyiben Vevő külön kéri, az Eladónak igazolnia kell.

Az Ajánlattevő ajánlatában a hatályos magyarországi szabványok és előírások figyelembevételével, a jelen műszaki leírásban meghatározott feltételeknek megfelelő eszközöknek és megoldásoknak kell szerepelniük.

Az Ajánlatkérő az eszközök valamennyi paraméterének meghatározásánál azt vette figyelembe, hogy azok üzleti célú felhasználásra kerülnek.

- A szállításra kerülő PC-knek azonos BIOS-sal/firmware-el és BIOS/firmware verzióval kell rendelkezniük.
- A szállításra kerülő PC-knek azonos fizikai kiépítéssel kell rendelkezniük (pl.: a beszerelésre kerülő egyéb alkatrészek (hálókártya, VGA kártya) ugyan arra a portra és csatlakozóra (SATA1) kerüljenek.
- A szállításra kerülő PC-knek azonos alkatrészekből kell összeszerelni (pl.: alaplap, CPU, hálókártya, VGA kártya).
- A szállításra kerülő PC-kbe szerelt alkatrészeknek azonos BIOS-sal/firmware-el és BIOS/firmware verzióval kell rendelkezniük.
- A szállításra kerülő PC-knek és a vele szállított alkatrészeknek a garancia érvényesítése egységesen és egyben kezelhető legyen.

- A szállításra kerülő PC-knek egyedi azonosítóval kell rendelkezniük.

Ajánlattevő feladatai

A jelen műszaki leírásban rögzített követelményeknek megfelelő, ajánlattevő ajánlatában megajánlott hardver eszközök szállítása a közbeszerzési eljárás eredményeként megkötendő szerződés keretében. A kiszállítás Ajánlatkérő központi raktárába (Budapest X., Maglódi u. 6. szám) vagy Budapest közigazgatási területén megadott egyéb címre történik. A végfelhasználókhoz történő kiszállítás és üzembe helyezés nem az Ajánlattevő feladata. Ajánlatkérő a szállítás során előteljesítést elfogad a teljes mennyiség tekintetében.

Munkaállomás jótállás

Nyertes Ajánlattevőnek vállalnia kell a szállított eszközökre vonatkozóan azok teljes körű, helyszíni jótállását a kiszállítástól a gyártó által biztosított, de minimum 3 évig azaz **36 hónapig** alábbi feltételeknek megfelelően:

- A meghibásodott eszközöket Ajánlatkérő szakértői cserélik a felhasználóknál és a meghibásodott eszközöket tárolják, és a hibát bejelentik Ajánlattevőnek.
- Ajánlatkérő magyarországi munkarendjének, nyitvatartási időablakának megfelelően, munkanapokon, munkaidőben (**H-CS: 8:00-16:50; P: 8:00-14:20**) telefonos és email alapú csatornákat biztosít a szállított eszközökkel kapcsolatos hibabejelentések fogadására. Telefonon történő hibabejelentés esetén Megrendelőnek hibabejelentését **4 órán** belül írásban (e-mailen) meg kell erősítenie.
- A hibabejelentéseket **1 munkanapon** belül kell visszaigazolni Ajánlatkérő felé
- A meghibásodott eszközöket Ajánlattevőnek el kell szállítania és a javítást saját telephelyén kell elvégeznie. A javítás után a hibátlanul működő eszközöket vissza kell szállítania arra a telephelyre, ahonnan eredetileg elszállította.

3

- A bejelentéstől számított **5 munkanapon** belül meg kell történnie a meghibásodott eszközök elszállításának.
- A bejelentéstől számított **15 munkanapon** belül visszaszállítja a megjavított és hibátlanul működő eszközt.
- A normál használat során bekövetkezett minden hibára érvényesnek kell lennie a szervizszolgáltatásnak úgy, hogy a későbbiekben semmilyen díj nem számítható fel.
- A nem javítható eszközöket nyertes Ajánlattevőnek cserélnie kell **15 munkanapon** belül az előzőekben rögzített paraméterekkel rendelkező, azonos gyártótól származó eszközre.

Az Ajánlatkérő adatbiztonsági előírásai következtében **HDD, SDD, adathordozó** hiba esetén, a hibás **HDD, SDD, adathordozó** nem kerül visszaadásra Ajánlattevő részére.

Standard (Dolgozói, Vezetői) munkaállomás műszaki leírás
- Forma: SFF vagy MT ház, alkalmas legyen legalább félmagas bővítő kártya fogadására
- Akár 85% hatásfokú tápegység
- Alaplap: Alaplapon feltüntetett gyártó a gép gyártójával azonos legyen
- Processzor: minimálisan 4 thread egyidejű kezelésére képes legyen, legalább valós 4 core-ral rendelkezzen Legalább 6950 Passmark érték (például: INTEL i5-6500)
- Memória: minimum DDR3 vagy DDR4, min **4 GB**, minimum 1600 MHz további bővítési lehetőség 8GB-ra modul csere nélkül, 4 GB RAM-nak 1 modullal kel megvalósulnia.
- Lemez csatoló: Minimum 6Gbit/s sebesség
- Belső adathordozó1: min. 256 GB méretű **SSD**, legalább 75 IOPS sebességű, 6Gbit/s sebességű csatolófelülettel, az adathordozónak a Serial ATA 0 portra kell csatlakoznia
- Alaplapi bővítő helyek: Legalább 1db PCIe x16
- Biztonsági funkciók: minimum **TPM** 1.2 chip
- Hálózati csatoló: legkevesebb 1 darab, minimum 1Gbit/s sebességű Ethernet (RJ45) hálózati csatoló felület
- Hang: fülhallgató kimenettel és és beépített hangszóróval rendelkezzen
- USB: Munkaállomáson kivezetésre került USB portok száma **összesen minimum 8db.** Kivezette USB portoknál minimum 4db USB 3.0 portnak kell lennie. Minimum 2 db USB 3.0 csatlakozónak alapkiépítésben a ház elején kell kialakításra kerülnie és minimum 2 db USB 3.0 és 4 db USB 2.0 csatlakozónak a ház hátulján kell kialakításra kerülnie.
- Monitor csatlakozás: 2 kijelző egyidejű csatlakozását lehetővé tevő konfiguráció, extended desktop üzemmód támogatása szükséges. Minimum 1 db digitális port szükséges és minimum 1 db analóg port szükséges, amelynél a digitális portnak Displayport-nak kell lennie és az analóg portnak D-SUB portnak kell lennie. Displayport, esetén ha az eszközön MiniDP port van, akkor a megajánlott eszközzel együtt szállítani kell egy olyan átalakítót, amely lehetőséget ad az eszközt normál Displayport-ra történő csatlakoztatását.
- Megjelenítés: minimálisan 1920x1080 felbontás és 24 bites színmélység lehetőségének támogatása
- WOL támogatás: Wake-On-LAN támogatás szükséges
- Energia hatékonyság: ENERGY STAR 6.0 minősítés
- BIOS/UEFI: UEFI és Legacy boot funkció támogatása;
- Támogatott operációs rendszer alól, a bios/uefi frissíthető, illetve bios/uefi konfigurációmódosítás végrehajtható legyen futtatással (segédprogrammal vagy standalone);
- Egységes típus (model) azonosítással és darabonként egyedi azonosítóval (pld: UUID vagy GUID) kell rendelkeznie
- Menedzselhetőség: biztosítani kell a System Center Configuration Manager 2007, 2012 alatti menedzselhetőséget (tömeges központi OS telepítés, szoftverfrissítések kezelése, konfiguráció felügyelete, konfigurációkezelés, leltárinformációk (HW, SW), alkalmazásfelügyelet)
- Operációs rendszer támogatás: 32 és 64 bites Windows 7, Windows 8.1 és Windows 10 Enterprise futtatása biztosított kell, hogy legyen
- Driverek: Minden a gépben található eszköz kell, hogy rendelkezzen Windows 7, Windows 8.1 és Windows 10 Enterprise (32 és 64 bit) kompatibilis Microsoft vagy a gyártó által biztosított és támogatott

driverrel. Az operációs rendszerbe beépített driveren kívül, az összes meghajtó programnak elérhetőnek kell lennie az interneten a gyártói oldalon.
- Szállítandó Licence: Microsoft Windows 10 Pro 64 bit HUN OEM vagy ezzel egyenértékű
- Burkolat alapszíne: fekete vagy szürke (sötét)
5
Az egyes Standard (Dolgozói, Vezetői) munkaállomás notebookkal együtt szállítandó periféria eszközök:
Billentyűzet
Elvárt jótállási idő: legalább 12 hónap
- Magyar billentyűzet kiosztású, 101 gombos
- Vezetékes kivitel, amely legalább 1.8m hosszúságú USB A csatlakozóval ellátott
- Kivitele a gombok elhelyezkedése tekintetében párhuzamos egyenes irányú
- Burkolat alapszíne: fekete vagy szürke (sötét)
- Kompatibilitással bírjon, illetve működéséhez külön külső szoftvert ne igényeljen Windows 7, 8.1, 10 esetén

Az Ajánlattevő ajánlatában csak azonos gyártótól származó, azonos típusú, a Standard (Dolgozói, Vezetői) munkaállomással együtt szállítandó Billentyűzeteket ajánlhat meg.
Egér
Elvárt jótállási idő: legalább 12 hónap
- Optikai, legalább 1,8m hosszúságú vezetékes USB A csatlakozású
- 2 alap gombbal és scroll görgővel szerelt gombbal rendelkezzen
- Felbontás legalább 1000 dpi
- Burkolat alapszíne: fekete vagy szürke (sötét)
- Kompatibilitással bírjon, illetve működéséhez külön külső szoftvert ne igényeljen Windows 7, 8.1, 10 esetén

Az Ajánlattevő ajánlatában csak azonos gyártótól származó, azonos típusú, a Standard (Dolgozói, Vezetői) munkaállomással együtt szállítandó Billentyűzeteket ajánlhat meg.
Az egyenértékűség minimális feltételei Microsoft Windows 10 Pro esetén:
- Meglévő Windows alapú alkalmazások futtatási lehetősége
- 32-64 bites programok futtatási lehetősége
- 32 és 48 bites színmélységek támogatása
- 256 logikai processzor támogatása
- SSD támogatás, gyorsítás, particionálás támogatás
- Virtual Hard Disk (VHD) formátumok natív kezelése (Ajánlatkérő meglévő upgrade joga alapján Enterprise vagy Ultimate verzióval)
- Felhasználói fiókok felügyelete
- Hordozható meghajtók tartalmának titkosítása BitLockerrel (Ajánlatkérő meglévő upgrade joga alapján Enterprise vagy Ultimate verzióval)

Az Ajánlattevő ajánlatában csak azonos gyártótól származó, azonos típusú Standard (Dolgozói, Vezetői) munkaállomásokat ajánlhat meg, amelyek teljesen megegyező kiépítésűek és azonos BIOS/UEFI/Firmware verzióval rendelkeznek. 6

Standard (Dolgozói, Vezetői) munkaállomás megfelelőségi táblázat Műszaki leírás szerinti elvárt műszaki követelmények	**Nyilatkozat a megfelelésről (igen/nem/pontos paraméter)**
Forma: SFF vagy MT ház, alkalmas legyen legalább félmagas bővítő kártya fogadására	kérjük a pontos paraméter megadását
Akár 85% hatásfokú tápegység	kérjük a pontos paraméter megadását
Alaplap: Alaplapon feltüntetett gyártó a gép gyártójával azonos legyen	igen/nem

Processzor: minimálisan 4 thread egyidejű kezelésére képes legyen, legalább valós 4 core-ral rendelkezzen Legalább 6950 Passmark érték (például: INTEL i5-6500)	kérjük a pontos paraméter megadását
Memória: minimum DDR3 vagy DDR4, min **4 GB**, minimum 1600 MHz további bővítési lehetőség 8GB-ra modul csere nélkül	kérjük a pontos paraméter megadását
Lemez csatoló: Minimum 6Gbit/s sebesség	igen/nem
Belső adathordozó1: min. 256 GB méretű **SSD**, legalább 75 IOPS sebességű, 6Gbit/s sebességű csatolófelülettel, az adathordozónak a Serial ATA 0 portra kell csatlakoznia	kérjük a pontos paraméter megadását
Alaplapi bővítő helyek: Legalább 1db PCIe x16	igen/nem
Biztonsági funkciók: minimum **TPM** 1.2 chip	igen/nem
Hálózati csatoló: minimum 1 db 1Gbit/s sebességű Ethernet (RJ45) hálózati csatoló	kérjük a pontos paraméter megadását
Hang: Fülhallgató kimenettel rendelkezzen a konfiguráció, és beépített hangszóróval	igen/nem
USB: Munkaállomáson kivezetésre került USB portok száma **összesen minimum 8db.** Kivezette USB portoknál **minimum 4db USB 3.0** portnak kell lennie. Minimum 2 db USB 3.0 csatlakozónak alapkiépítésben a ház elején kell kialakításra kerülnie és minimum 2 db USB 3.0 és 4 db USB 2.0 csatlakozónak a házhátulján kell kialakításra kerülnie.	kérjük a pontos paraméter megadását
Monitor csatlakozás: 2 kijelző egyidejű csatlakozását lehetővé tevő konfiguráció, extended desktop üzemmód támogatása szükséges. Minimum **1 db digitális port** szükséges és minimum **1 db analóg port** szükséges, amelynél a digitális portnak Displayport-nak kell lennie és az analóg portnak **D-SUB** portnak kell lennie. **Displayport,** esetén ha az eszközön MiniDP port van, akkor a megajánlott eszközzel együtt szállítani kell egy olyan átalakítót, amely lehetőséget ad az eszközt normál Displayport-ra történő csatlakoztatását.	kérjük a pontos paraméter megadását
Megjelenítés: min **1920x1080** felbontással és 24 bites színmélységgel	igen/nem
WOL támogatás: Wake-On-LAN támogatás szükséges	igen/nem
BIOS/UEFI: UEFI és Legacy boot funkció támogatása;	igen/nem