DUNAÚJVÁROSI EGYETEM

INFORMATIKAI ÉS INFORMATIKAI BIZTONSÁGI SZABÁLYZAT

2019.
Dunaújváros

Dunaújvárosi Egyetem Szenátusa által 98-2018/2019. (2019.05.28.) sz. határozatával elfogadva

Hatályos: 2019. 05. 29. napjától

TARTALOMJEGYZÉK

I. Általános rendelkezések 6
1.§ Az informatikai és informatikai biztonsági szabályzat (IIBSZ) kiadásának célja, szerkezete, hatálya 6
2.§ A kötelező felülvizsgálat (revízió) időpontja 6
3.§ Kapcsolódó szabályozások (hivatkozások) 6
4.§ Értelmező rendelkezések 7
5.§ Az Intézmény átfogó informatikai menedzsmentje 7
6.§ Feladat-, felelősség- és hatáskörök 8
7.§ Jogszabályi, törvényességi megfelelőség 8
II. Információbiztonság 10
8.§ Információbiztonsági irányelvek 10
9.§ IT rendszerek biztonsági osztályai, besorolás 10
10.§ Informatikai biztonsági feladatkörök 11
11.§ ISZK központvezető 11
12.§ Szervezeti egységek vezetője 11
13.§ Rendszermérnök 12
14.§ Rendszergazda 13
15.§ Technikus 14
16.§ Felhasználó 15
17.§ Munkaállomások használata 16
18.§ Fokozott biztonságú munkaállomások 18
19.§ Mobil munkaállomások használata 18
20.§ Munkaállomások adatainak mentése 19
21.§ Elektronikus levelezés és Internet használat információbiztonsági követelményei 19
22.§ Informatikai biztonsági követelmények az IT rendszerek szállítási szerződéseiben 21
23.§ Informatikai eszközök beszerzése nyilvántartása és javítása 21
24.§ Internet domain név adminisztráció 22
25.§ Gazdálkodás az IP címekkel 23
26.§ Munkaállomások adatkezelése jogviszony megszűnése esetén 24
27.§ Személyes postafiók (email) adatkezelése jogviszony megszűnése esetén 24
III. Szolgáltatásszint menedzsment 26
28.§ A szolgáltatásszint menedzsment folyamata 26
29.§ A szolgáltatási megállapodások (SLA) tartalma 26

30.§ Megfigyelés, jelentés és áttekintés ... 28
IV. Ügyfélszolgálat, incidenskezelés ... 29
31.§ Központi ügyfélszolgálat (Help Desk) ... 29
32.§ Incidenskezelés ... 29
33.§ Incidensosztályozás és prioritás hozzárendelés ... 29
V. Problémakezelés ... 30
34.§ Probléma és az ismert hiba kezelése ... 30
35.§ Trend-azonosítás ... 30
36.§ Probléma megelőzés ... 30
VI. Konfigurációkezelés ... 32
37.§ Alapelvek és terminológia ... 32
38.§ A konfigurációkezelés adatbázisa ... 32
VII. Változáskezelés ... 33
39.§ Központosított változás-felügyelet ... 33
40.§ Változáskezelési folyamatok ... 33
41.§ Szerepkörök és felelősségek ... 33
VIII. Kiadáskezelés ... 34
42.§ Kiadáskezelés - új szolgáltatás indítása ... 34
43.§ A hiteles szoftver tár ... 34
44.§ Licencek kezelése ... 34
IX. IT szolgáltatásfolytonosság biztosítása ... 35
45.§ Kockázatkezelés ... 35
46.§ Vészhelyzetek kezelése és az IT szolgáltatásfolytonossági terv ... 35
X. Rendelkezésre-állás biztosítása ... 36
47.§ Rendelkezésre-állás, megbízhatóság, szervízelhetőség ... 36
48.§ Karbantarthatóság, biztonság szintjei ... 36
49.§ A magas szintű rendelkezésre-állás tervezése ... 36
XI. Kapacitások biztosítása ... 37
50.§ Kapacitáskezelés ... 37
51.§ Kapacitástervezés ... 37
52.§ A kapacitáskezelés eleme ... 37
XII. Záró rendelkezések ... 38
53.§ Az IIBSZ változásmenedzsmentje ... 38
54.§ Hatályba lépés ... 38
Az Informatikai és Információbiztonsági Szabályzat mellékletei ... 39
Fogalommagyarázat ... 46

I. ÁLTALÁNOS RENDELKEZÉSEK

1.§ Az informatikai és informatikai biztonsági szabályzat (IIBSZ) kiadásának célja, szerkezete, hatálya

(1) A szabályzat célja az intézményben folyó oktató-, kutató-fejlesztő munkát támogató, az információ szabad áramlását biztosító informatikai infrastruktúra elemeinek, az intézmény informatikai szolgáltatások kialakításának, üzemeltetésének, igénybevételének és ezek ellenőrzési lehetőségeinek szabályozása.

(2) A szabályzat informatikai szolgáltatásként határoz meg minden olyan, informatikai rendszerhez történő, hozzáférési, felhasználási lehetőséget, amelyet az üzemeltetők a felhasználók számára elérhetővé tesznek. A szabályzat meghatározza az eszközök kialakításának, használatának módját, feltételeit, kitér a jogi és etikai kérdésekre is.

(3) A szabályzat információbiztonsággal foglalkozó elemei összefoglalva tartalmazzák mindazon intézkedéseket és betartandó szabályokat, amelyek által a Dunaújvárosi Egyetem (továbbiakban DUE, vagy intézmény) információbiztonsága (rendszerek adatok és információ, rendelkezésre állása, sértetlensége és bizalmassága) fenntarthatóvá válik.

(4) Jelen szabályzat mindenkire nézve kötelező, aki használja a DUE informatikai szolgáltatásait, informatikai infrastruktúráját, annak berendezéseit (felhasználók). Az előbbieknek megfelelően a szabályzat személyi hatálya kiterjed a DUE összes hallgatójára és dolgozójára, aki oktatási, kutatási, tudományos vagy az intézmény adminisztrációs feladataihoz a DUE informatikai hálózatát és eszközeit használja. Ha az intézmény harmadik félnek is lehetőséget biztosít ezen infrastruktúrája használatára, akkor harmadik félre nézve is kötelező a szabályzatban foglaltakat betartani.

(5) A szabályzat alapszerkezete követi az ITIL (IT Infrastructure Library) de facto információ-technológiai és szolgáltatásirányítási szabvány szerkezetét. Ennek célja, hogy az intézmény információtechnológiai (IT) szolgáltatásaival kapcsolatos szemléletmódot mind felhasználói mind szolgáltatói oldalon erősítse.

(6) A mindenkori szabályzat felhasználók számára készült kivonata a DUE Informatikai Felhasználói Szabályzat (DUE-AUP), amely e szabályzat 1. sz. melléklete.

2.§ A kötelező felülvizsgálat (revízió) időpontja

(1) A szabályzat felülvizsgálatára az alábbiak szerint kerül sor:

a) Évente egy alkalommal (az esedékes következő felülvizsgálati időpontot a dokumentum lezárásakor kell kijelölni.)

b) Minden olyan esetben, amikor a szabályzatban leírtakban jelentős változás(ok) történnek.

c) Jelen szabályzat mellékletei az Informatikai Szolgáltató Központ központvezetői utasításai alapján módosíthatóak.

3.§ Kapcsolódó szabályozások (hivatkozások)

a) A Dunaújvárosi Egyetem Szervezeti és Működési Szabályzata (SZMSZ)

b) Hallgatók jogállását leíró dokumentumok

c) Adatkezelési és adatvédelmi szabályzat

d) Közalkalmazottak fegyelmi szabályzata

e) Beszerzési szabályzat

f) Közbeszerzési szabályzat

g) Informatikai Szolgáltató Központ Ügyrendje

h) Munkaköri leírások

4.§ Értelmező rendelkezések

(1) Informatikai rendszer: az intézmény informatikai hálózata, beleértve a hálózati eszközöket, szervereket, általános célú számítógépeket, felhasználói és rendszerszoftvereket, nyomtató, sokszorosító, digitalizáló berendezéseket és a telefonrendszert, továbbá ezek külső rendszerekkel való kapcsolatát biztosító eszközök egyetemi tulajdonban lévő elemeit.

(2) Információs rendszer: az informatikai rendszer egyes elemeiből felépülő önálló, vagy más informatikai rendszerekkel együttműködő rendszerkomponens, amely adatokat dolgoz fel és ezekből intézményi célokat szolgáló információt szolgáltat, vagy az intézmény számára más entitásokkal való kapcsolatot biztosítja. Az információs rendszer különböző hardver és szoftveralkalmazásokon és szolgáltatásokon keresztül valósul meg.

(3) Informatikai eszközök: a szabályzat alkalmazása tekintetében esz-köznek tekintendők:

a) Számítógépek és azok perifériális berendezései (pl.: billentyűzet, egér, monitor) függetlenül a számítógép rendszerbeli funkciójától.

b) A számítógép hálózat passzív és aktív elemei (pl.: vezetékezés, kapcsoló-berendezések, forgalomirányítók, hálózatbiztonsági berendezések).

c) Az irodatechnikai berendezések (pl.: nyomtató, fénymásoló).

d) A fenti berendezésekhez tartozó dokumentációk, licencek.

(4) Szoftverek, licencek: a szabályzat alkalmazása tekintetében szoftver eszköznek minősül:

a) A számítógépek működtetését biztosító alapszoftver (pl.: operációs rendszer).

b) Az alkalmazások, informatikai rendszerek szoftverei (pl.: célprogramok, mérésadatgyűjtő programok).

c) Vásárolt célszoftverek (pl.: dobozos termékek, Office programok, grafikus szoftverek)

d) Használati licencek (pl.: vírusvédelmi rendszer, adatbázis kezelő használati licencei, Campus Licenc – Tisztaszoftver Program).

5.§ Az Intézmény átfogó informatikai menedzsmentje

(1) Az intézmény informatikai tevékenységének szabályozását és koordinálását az Informatikai Szolgáltató Központ (ISZK) látja el.

6.§ Feladat-, felelősség- és hatáskörök

(1) Minden üzemeltetett rendszer esetében az informatikai szabályzatnak való megfelelés az adott rendszert üzemeltető szervezeti egység vezetőjének felelőssége. Az adott szolgáltatás üzemeltetési feladatainak ellátásáért felelős személyt (rendszergazda, rendszermérnök), illetve az üzemeltetésért felelős szervezeti egységet (továbbiakban szolgáltató egység) az adott szolgáltatás, „szolgáltatást meghatározó megállapodásban" (Service Level Agreement - SLA) kell megnevezni.

(2) Az informatikai szolgáltatások szakmai felügyeletét az ISZK látja el. Az ISZK felelős a szolgáltató egység és a szolgáltatás igénybevevője között a szolgáltatás tartalmának és egyéb paramétereinek egyeztetéséért, a megállapodás betartásának ellenőrzéséért.

(3) Az ISZK központvezetője jogosult az egyes szolgáltatások IIBSZ megfelelőségének ellenőrzésére.

(4) Egyes intézményi stratégiába illő nagyobb fejlesztések, beruházások, vitatott informatikai szolgáltatás, vagy az informatikai és informatikai biztonsági szabályzat változtatására tett javaslatok körébe tartozó tevékenységek intézményi független kontrollja érdekében a kancellár szükség estén 5 fős ad-hoc bizottság létrehozását rendeli el. A bizottság tagjai: 1 fő az KIFÜ-NIIF infrastruktúráért felelős elnökhelyettese (vagy az általa kijelölt személy) - a bizottság elnöke; 2 fő külső szakértő; 1 fő a kancellár által megbízott belső szakértő, valamint az ISZK központvezetője.

7.§ Jogszabályi, törvényességi megfelelőség

(1) Az informatikai szolgáltatások igénybevétele során elkövetett bűncselekményekért, illetve egyéb jogsértésekért a szolgáltatást igénybevevő büntetőjogi felelősséggel tartozik.

(2) A szolgáltatás üzemeltetője a jogszabályokban meghatározott nyilvántartásokat köteles vezetni. Törvényes megkeresés alapján, a vonatkozó jogszabályi kereteknek megfelelve az intézmény minden, a bűncselekmény elkövetésének gyanúja alá eső felhasználó adatait, valamint a rendelkezésre állási időn belül előállítható naplózott adatokat a nyomozóhatóságnak kiszolgáltatja. Ezen adatok kiszolgáltatása kizárólag az intézmény Adatkezelési és adatvédelmi szabályzatban leírtak szerint történhet.

(3) A szolgáltatások igénybevevőit a szabályzatban foglaltak megsértése esetén – az esemény súlyától függően – az alábbi szankciók sújthatják:

a) A szolgáltatás korlátozása.

b) Szolgáltatás megtagadás (kizárás a szolgáltatásból).

c) Az okozott anyagi kár megtérítése.

d) Eljárás kezdeményezése az intézményi fegyelmi szabályzat szerint.

e) Polgári jogi eljárás kezdeményezése, vagy büntető feljelentés megtétele.

(4) A szolgáltatásokat igénybe vevők b), c), d), e) szerinti szankcionálása csak akkor történhet meg, ha az üzemeltető az intézmény kancellárjának dokumentáltan bejelentette a szankció elrendelését kiváltó eseményt (incidens). A bejelentés felelőse a szolgáltatást nyújtó szervezeti egység vezetője. A HR és Jogi Iroda vezetőjének hatáskörébe tartozik

az incidens kivizsgálása és a szankcionálás szintjének megállapítása érdekében teendő intézkedés.

(5) Nem büntetőjogi kategóriába tartozó incidensek bejelentése az ISZK-hoz is történhet, akinek kötelessége az incidens kivizsgálása. Az ISZK központvezetőjének mérlegelési joga van arra, hogy a bejelentett incidenst jelentse a magyarországi Hun-CERT (Hungarian National Computer Emergency Response Team) szervezetnek.

II. INFORMÁCIÓBIZTONSÁG

8.§ Információbiztonsági irányelvek

(1) Az információbiztonsági irányelvek célja, hogy a DUE szervezeti egységei részére egységes és általános értelmezést adjon az informatikai rendszerekben kezelt adatok bizalmassága, hitelessége, sértetlensége, rendelkezésre állása és funkcionalitása biztosítása érdekében követendő tevékenységekre. Az irányelveket figyelembe véve meghatározható az informatikai biztonsági szabályozás alapján az egyes adatokat kezelő informatikai rendszerek biztonsági osztályba sorolása. Kidolgozhatóak a konkrét, rendszerbiztonsági szabályozások, amelyek az informatikai rendszer teljes életciklusában meghatározzák a szabványos biztonsági funkciók tervezéséhez, megvalósításához, üzemeltetéséhez és megszüntetéséhez szükséges alapelveket és követelményeket.

9.§ IT rendszerek biztonsági osztályai, besorolás

(1) A DUE informatikai rendszerei négy üzemviteli kockázati kategóriába kerültek besorolásra. A biztonsági kategóriák jele: A, B, C és D. A legmagasabb biztonsági szint jele „A”. Ezen kategóriába sorolás független az adatok biztonsági besorolásától.

(2) Kritikus rendszerek („A” biztonsági kategória)

Az intézmény működése szempontjából kritikus, az intézmény egészére kiterjedő rendszerek, amelyek egyben szenzitív, illetve személyes adatokat is tartalmaznak. Ezek a rendszerek információbiztonság szempontból kiemelt védelmet igényelnek. Az érintett rendszerek az alábbiak:

a) Tanulmányi rendszer.

b) Online oktatási rendszer (pl.: Moodle)

c) Bér- és Munkaügyi rendszer.

d) Gazdasági, ügyviteli, számviteli rendszerek.

e) Iratkezelési (iktatási) rendszer.

f) Központi levelező kiszolgáló.

g) Központi tárhely-kiszolgáló.

h) Központi dokumentumkezelő rendszer.

i) Intézményi személyi azonosító rendszerek címtára (pl.: Active Directory).

(3) Kiemelt rendszerek („B” biztonsági kategória)

Az intézmény működése szempontjából rendkívül fontos rendszerek, amelyek elsősorban technikai jellegűek, a rajtuk tárolt adatok nem személyes jellegűek, viszont közvetett hatással vannak az intézmény működésére, megítélésére. Ezek:

a) Az informatikai hálózat elemei, beleértve a vezetékes és vezeték nélküli adathálózatot.

b) Az intézményi szerver-, háttértár- és adatmentési infrastruktúra elemei.

c) Hálózatmenedzsment eszközök és kiszolgálók.

d) Információtechnológiai (environmental, middleware) rendszerek, melyek központi szolgáltatásokat nyújtanak. (pl.: metadirectory, belső fejlesztésű rendszerek)

e) Kommunikációs rendszerek (központi web-szolgáltatás, intranet)

(4) Normál rendszerek („C" biztonsági kategória)

„A" vagy „B" kategóriába nem sorolt, a teljes intézmény napi működése szempontjából nem kritikus, illetőleg az intézménynek csak egyes részeire kiterjedő rendszerek.

a) Műszaki berendezésekhez tartozó rendszerek. (pl.: épületfelügyeleti rendszer)

b) Oktatástechnológiai (oktatást támogató) rendszerek.

c) Lokális (csak az adott gépen futó) alkalmazások és szolgáltatások.

(5) Egyéb rendszerek („D" biztonsági kategória)

Az előző három kategóriába nem sorolható informatikai rendszerek.

10.§ Informatikai biztonsági feladatkörök

(1) Az informatikai rendszerek biztonságának védelme, a szabályozások betartása érdekében egyes személyek beosztásukból következően feladatokat végeznek, felelősséggel tartoznak és hatáskörökkel rendelkeznek.

11.§ ISZK központvezető

(1) Feladata:

Az egyetem informatikai-szolgáltatási koncepciójának képviselete, az intézmény informatikai rendszerei üzemeltetésének, működésének irányítása és ellenőrzése, továbbá az ISZK ügyrendben rögzített feladatokkal rendelkező Informatikai Szolgáltató Központ vezetése.

(2) Felelőssége:

a) A biztonsági irányelvekbe illeszkedő fejlesztési és üzemeltetési stratégia kialakítása, előterjesztése a döntéshozó fórumok elé.

b) Az egyetem informatikai biztonsági követelményeinek betartatása.

(3) Hatásköre:

Az egyetem informatikai rendszereinek tekintetében utasítási joggal rendelkezik:

a) Fejlesztések megvalósításában.

b) Üzemviteli, biztonsági és egyéb informatikai üzemeltetési kérdésekben.

12.§ Szervezeti egységek vezetője

(1) Feladata a vezetése alatt álló szervezeti egységre kiterjedően:

a) A hivatalos munkaidőn túli géphasználat ellenőrzése.

b) A hozzáférési jogosultságok megadásának és visszavonásának kezdeményezése.

c) A szervezeti egység által gyűjtött és kezelt adatok biztonsági osztályba sorolása.

d) Részvétel a rendellenes használattal kapcsolatos ügyek kivizsgálásában.

(2) Felelőssége:

A vezetése alatt álló szervezeti egységre kiterjedően az informatikai és informatikai biztonsági követelmények (jelen szabályzat) betartatása.

(3) Hatásköre:

A vezetése alatt álló szervezeti egységre kiterjedően jogosultság-jóváhagyási-, ellenőrzési jog illeti meg.

13.§ Rendszermérnök

(1) Rendszermérnök az intézmény kiemelt fontosságú informatikai rendszereinek (pl.: Windows infrastruktúra, Office rendszerek, LAN és WIFI hálózat, stb.) mérnöki (tervezési, kivitelezési, fejlesztési, üzemeltetési és felügyeleti) feladatait ellátó személy, akit a kancellár írásban bíz meg. Az intézményi rendszerek egyes elemeire a megfelelő mérnöki feladatok biztosítása érdekében az ISZK vezetője is kezdeményezheti a rendszermérnöki megbízás kiadását, amelyet írásban, a kancellárnak címezve kell megtennie.

(2) Feladata az ISZK központvezető támogatása a szolgáltatási, üzemeltetetési és üzemviteli rendszerek koncepciójának kialakításában és a koncepciónak megfelelő technikai / technológiai munkák kivitelezésében. A munkakör magas szakmai tudást és tapasztalatot igényel, és / vagy rendkívül bizalmas természetű. Ide tartozik a központi szerverüzemeltetés, virtuálszerver környezet kialakítása és működtetése, adathálózati struktúra kialakítása, hálózati aktív eszközök, tűzfalak konfigurálása, hálózat- és szerverfelügyeleti folyamatos munkák ellátása.

(3) Főbb rendszermérnöki feladatok:

a) Szolgáltatási rendszerek alapkonfigurációjának kialakítása.

b) Szolgáltató rendszerek felügyelete, kapcsolattartás a support cégekkel (pl.: hiba bejelentése és az elhárítás nyomon követése).

c) Kiadott programjavítások végrehajtása.

d) Adatmentések kezelése (tervezés, kivitelezés, üzemeltetés).

e) DHCP szolgáltatás meghatározása (vlan, címkiosztási rend, alhálózatok).

f) Email szolgáltatás meghatározása, ellenőrzés.

g) Dokumentum menedzsment rendszerek fejlesztése, működtetése, üzemviteli feladatai.

h) Active Directory és más címtár rendszerek fejlesztése, működtetése, üzemviteli feladatai - címtár-szinkronizáló rendszer felügyelete.

i) Üzemviteli körülmények meghatározásában való részvétel.

j) Virtualszerver-környezet létrehozása, rendszeradminisztrálása.

k) Szerver operációs rendszerek telepítése, alkalmazói rendszer paraméterek és biztonsági konfigurációk elvégzése.

l) Hálózati konfigurációk kialakítása, tűzfalszabályok kialakítása és felügyelete.

m) Rendszertechnikai változtatások előkészítése, tesztrendszer kialakítása, bevezetés.

n) Logok elemzése, következtetések levonása, javaslattétel.

o) Jelszó és egyéb biztonsági házirendek konfigurálása.

p) További feladatköreit a munkaköri leírása tartalmazza.

(4) Felelőssége:

a) A meghatározott feladatok elvégzése (a munkaköri leírással összhangban).

b) A hozzárendelt alkalmazói rendszerek esetében a licenc-gazdálkodás figyelemmel kísérése.

c) Titok- és bizalmas adatkezelés szabályainak betartása.

(5) Hatásköre:

a) Eljárni a feladatait érintő ügyekben.

14.§ Rendszergazda

(1) A rendszergazda az intézmény informatikai rendszereinek (pl.: tanulmányi, gazdasági rendszerek, stb.) vagy meghatározott hálózatának üzemeltetési- és felügyeleti feladatait ellátó személy, mely feladatot munkaköri leírása alapján látja el. Az intézményi rendszerek egyes elemeire a megfelelő üzemeltetés és felügyelet biztosítása érdekében az ISZK vezetője is kezdeményezheti a rendszergazdai megbízás kiadását, amelyet írásban, a kancellárnak címezve kell megtennie.

(2) Feladata egy, vagy több meghatározott, központi üzemeltetésű és/vagy alkalmazói rendszer üzemvitelének figyelemmel kísérése (pl.: tanulmányi rendszer, gazdasági rendszer, nyilvános web szolgáltatás, hálózati és szerverrendszerek, mentési rendszer, tároló adminisztráció, könyvtári rendszer felügyelete), kapcsolattartás az alkalmazói rendszert szállító / működtető (gyakran külső vállalkozás) és a felhasználók között. A rendszerleírásban foglalt feladatok maradéktalan elvégzése, az alkalmazói rendszer belső dokumentálása, felhasználók oktatása.

(3) Főbb feladata (a hozzá rendelt rendszerek vonatkozásában):

a) A kliens operációs rendszer (nem szerver) paraméterek meghatározása, a kliens operációs rendszerek konfigurálása.

b) Alkalmazói rendszerek telepítése, testreszabása - felhasználói igények vs. intézményi szabályozás összhangját biztosítva.

c) Szakmai önképzés, szakirodalom, web (Wikipedia, KnowledgeBase) tanulmányozása, igénybejelentés szakmai továbbképzésre.

d) Alkalmazói rendszerek futtatási környezetének biztonsági beállításai, a központvezető és a rendszermérnökök útmutatásai alapján.

e) Vírusvédelmi rendszer menedzsment rendszerének működtetése.

f) Windows operációs rendszer frissítés-kezelő rendszerének működtetése.

g) Ha a rendszergazda nem az ISZK állományába tartozik, akkor feladata a szakmai együttműködés az ISZK-val.

h) További feladatköreit a munkaköri leírása tartalmazza.

(4) Felelőssége:

a) A meghatározott feladatok elvégzése (a munkaköri leírással összhangban).

b) A hozzárendelt alkalmazói rendszerek esetében a licenc-gazdálkodás figyelemmel kísérése.

c) Titok- és bizalmas adatkezelés szabályainak betartása.

(5) Hatásköre:

a) Eljárni a feladatait érintő ügyekben.

15.§ Technikus

(1) Feladata a HelpDesk feladatok ellátása napi rendszerességgel, beleértve az informatikai eszközök hardver és szoftver javítását telefonos segítséggel, vagy a felhasználó munkahelyén, komolyabb probléma esetén az ISZK-hoz beszállítással. Szükség esetén külső szervizszolgáltatás megrendelésének kezdeményezése. Informatikai eszközök időszakos karbantartása, vásárolt számítógépek, nyomtatók, szkennerek, stb. üzembe helyezése a felhasználói munkahelyeken, vagy oktatási kabinetekben. Oktatástechnológusi támogatás biztosítása a tantermekben és előadókban oktatói/rendezvény igénye szerint.

(2) További technikusi feladatok: vásárolt számítógépek operációs rendszer telepítése, a belső biztonsági rendben meghatározott beállításai, jogtiszta felhasználói programok telepítése (pl. Office rendszer). Ügyeleti feladatok ellátása a szorgalmi időszakban eltolt műszakos munkarendben.

(3) A technikusok főbb feladatai az alábbiak:

a) Felhasználói bejelentésekre reagálás, rövid időn belül.

b) Számítógépek, nyomtatók, egyéb informatikai eszközök javítása, vagy szervizigény bejelentése.

c) Operációs rendszer, vírusvédelmi rendszer alapvető alkalmazások (pl.: Office) javítása a felhasználói munkaállomásokon.

d) Telefonos, vagy személyes segítség munkatársaknak, hallgatóknak.

e) Hálózati problémák felderítése, lehetőség szerinti javítása.

f) Kiadott munka elvégzésének visszajelzése, munkalap lezárása.

g) Oktatástechnológiai támogatás (projektor üzembe helyezés, hangosítás).

h) További feladatköreit a munkaköri leírása tartalmazza.

(4) Felelőssége:

a) A meghatározott feladatok elvégzése (a munkaköri leírással összhangban).

b) A telepített (karbantartott) alkalmazói rendszerek esetében a licencgazdálkodás figyelemmel kísérése.

c) Titok- és bizalmas adatkezelés szabályainak betartása.

(5) Hatásköre:

a) Eljárni a feladatait érintő ügyekben.

16.§ Felhasználó

(1) Információbiztonsági szempontból felhasználónak minősül minden egyetemi polgár (hallgató, oktató, dolgozó, vendég), akinek az IT eszközök és rendszerek használata tanulmányi és/vagy munkaköri feladatainak ellátásához szükséges. Az információbiztonsági kiemelt feladatotokat ellátó személyek egyúttal felhasználók is.

(2) Felhasználói státuszt hallgató a tanulmányi rendszerben való regisztrálást követően; oktató/dolgozó a HRSZK által történt regisztrációt és adatfelvételt követően; vendég felhasználó a fogadó szervezeti egység részéről az ISZK-hoz eljuttatott igénylés feldolgozása után kap.

(3) Felhasználó alanyi jogon rendelkezik:

a) Felhasználói nevét és jelszavát használva a jogosultsági szintjének megfelelő intézményi informatikai erőforrásokhoz való hozzáféréssel, valamint a „MINDENKI” (EVERYONE) jogosultsági csoportba sorolt hozzáféréssel.

b) Hallgatók a neptun-kód@hallgato.uniduna.hu személyes e-mail címmel és az ezen címet kiszolgáló levelező rendszer használati lehetőségével.

c) Oktatók, dolgozók a felhasználói-név@uniduna.hu és a vezetéknév.keresztnév@uniduna.hu e-mail címmel és az ezen címet kiszolgáló levelező rendszer használati lehetőségével.

d) Az Internet használatával az egyetem bármely vezetékes vagy vezeték nélküli hálózatra kapcsolt munkaállomásáról – kivéve azon munkaállomásokat, melyek a fokozott alkalmazásbiztonság érdekében a nyilvános hálózatokkal való kapcsolattól adminisztratív módon el vannak zárva.

(4) Felhasználó feladata:

a) A tanulási/ oktatási folyamathoz szükséges IT eszközök és rendszerek használata.

b) Az intézmény által rendelkezésre bocsátott, a munkaköre ellátásához szükséges IT eszközök és rendszerek használata.

c) Oktatók és nyilvánosságot igénylő feladatot ellátó dolgozók az intézményi nyilvános weboldalon (telefonkönyv) keresztül a legfontosabb elérhetőségi adatainak naprakészen tartása. Személyi adat változása esetén (pl.: név) a HJI-n kell kezdeményezni a változtatást, szoba vagy telefonmellék változása esetén pedig az ISZK-nak kell jelezni a változtatási igényt.

(5) Felhasználó felelőssége:

a) A hallgatói jogviszonya/munkaköre ellátásához szükséges IT eszközök és rendszerek felhasználói szintű ismerete és az alkalmazások használati szabályainak betartása.

b) Az Informatikai és Informatikai Biztonsági Szabályzatban megfogalmazottak betartása, különös tekintettel az információbiztonságra és adatvédelemre.

c) A tudomására jutott informatikai biztonságot sértő esemény jelzése közvetlen felettese és az ISZK számára.

(6) Felhasználó hatásköre:

a) A kiosztott jogosultságai alapján tanulmányi munka, hallgatói-, oktatói- és dolgozói munkavégzés az intézmény IT eszközeinek és rendszereinek igénybevételével.

17.§ Munkaállomások használata

(1) A felhasználók általában munkaállomásokon keresztül veszik igénybe az IT eszközök és rendszerek szolgáltatásait. A munkaállomás leggyakrabban egy asztali PC, típustól függetlenül, amely az oktatási kabinetekben, laborokban és a dolgozói munkahelyeken van elhelyezve. A munkaállomás operációs rendszerének telepítését az ISZK végzi, vagy – ahol a szervezeti egységnél erre rendelkezésre áll rendszergazda beosztású dolgozó – az ISZK-val egyeztetve történik. A munkaállomásokat a 23.§ -ban leírtak szerint az ISZK nyilvántartásában kell tartani. Nyilvántartásában nem szereplő munkaállomás hálózatra kapcsolását az ISZK hálózatfelügyeleti eszközök alkalmazásával megtilthatja.

(2) Mobil munkaállomásnak minősül az intézményi tulajdonú vagy magántulajdonú, de a munkavégzéshez rendszeresen használt hordozható számítógép (pl.: notebook, tablet).

(3) Az egyetemen használt, az egyetem tulajdonát képező munkaállomásokat rendeltetésszerűen, munkavégzés céljából, az egyetem érdekeinek szem előtt tartásával, az egyetem által meghatározott módon lehet használni. Az intézményi informatikai eszközök (pl.: számítógépek, tabletek, stb.) magán célú használata (magánanyagok tárolása) nem engedélyezett. Az intézményi informatikai eszközökön csak a munkavégzéssel szorosan összefüggő adatokat (állományokat) lehet tárolni.

(4) A munkaállomások hálózatbiztonsági feltételeknek megfelelő és a használat szempontjából feltétlenül szükséges jogosultsági rendje (policy beállítások) az ISZK javaslatára a szervezeti egységek vezetőivel egyetértésben kerül meghatározásra.

(5) Az intézmény épületeiben telepített vezetékes hálózatra kapcsolódó munkaállomásokon a központi felügyeleti rendszer a munkaállomásra meghatározott telepítési beállításokat, az operációs- és a vírusvédelmi rendszer frissítéseit, a munkaállomás használatához szükséges szoftvereket és alkalmazás-komponenseket, felhasználói beavatkozás nélkül telepítheti, a munkaállomáshoz rendelt jogosultsági rendet automatikusan beállíthatja.

(6) Munkaállomás csak az intézmény belső hálózatára csatlakozhat. A külső hálózatok elérése kizárólag a központi tűzfal funkciót ellátó berendezésen keresztül a hivatalos internet szolgáltató (ISP) vonalain a HBone hálózat irányába lehetséges. Olyan munkaállomás nem kapcsolható az egyetem hálózatára, amelyen más külső hálózati kapcsolatot is egyidejűleg igénybe vesz (pl. kábelhálózati szolgáltatás, bármely szolgáltatótól ADSL, mobil internet - GPRS/3G/EDGE, egyéb pl. WiFi kapcsolat más szolgáltatóval, stb.)

(7) Olyan munkaállomás, amely nem rendelkezik helyi (az eszközre telepített) vírusvédelmi szoftverrel, az intézményi hálózathoz nem csatlakoztatható. Az intézmény tulajdonában lévő munkaállomások részére a vírusvédelmi rendszert központi menedzsment alkalmazásával az ISZK biztosítja. A kollégiumi szobákban működő hallgatói (saját tulajdonú) munkaállomások vírusvédelméről a hallgató (tulajdonos és /vagy felhasználó) köteles gondoskodni.

(8) A vírusvédelmi előírás feltételeinek eleget nem tevő munkaállomás csatlakozását a hálózatfelügyeleti rendszer automatikusan megtilthatja.

(9) Az egyetemen telepített intézményi tulajdonú munkaállomások hardver integritásának megőrzése céljából a felhasználónak tilos a számítógépet fizikailag megbontani: alkatrészeket cserélni, be- és kiszerelni. A szükséges hardverváltoztatás a területei rendszergazda, ennek hiányában az ISZK hatáskörébe tartozik.

(10) Speciális oktató-kutató munkavégzéshez elengedhetetlen hardverbeépítés és csere esetén egyeztetni kell az ISZK-val. A végrehajtott módosítást az ISZK eszköznyilvántartásában is dokumentálni kell. Az ISZK csak központi összeférhetetlenség, hálózatbiztonsági okok miatt és/vagy jogi okokra (pl.: pályázati forrásból beszerzett eszköz, nem saját tulajdonú eszköz, stb.) hivatkozva ellenezheti a munkaállomás hardverének módosítását. Az ISZK által nem támogatott hardverrel és/vagy szoftverrel rendelkező munkaállomások zárt hálózatba szervezését az ISZK elrendelheti. Speciális kísérleti és tesztelési feladatokra, szolgáló munkaállomásokon, virtuális operációs rendszerkörnyezet létrehozásával, vagy az intézményi hálózatról leválasztott hálózati szegmensre való kapcsolódással végezhető munka. A virtuális rendszerkörnyezetnek a kísérleti munka alatt semmilyen közvetlen kapcsolata nem lehet az intézményi hálózattal.

(11) A felhasználónak a mindennapos munkája során a munkaállomás használat tekintetében a következő szabályok szerint kell eljárnia:

a) Munkaállomásra csak a saját felhasználói névvel és jelszóval hitelesítve léphet be. Ez alól kivételt képeznek azon oktatási kabinetekben telepített munkaállomások, ahol a kabinet/labor rendszeradminisztrátora nem személyre szabott bejelentkezési rendszert telepített. A munkaállomás felhasználói bejelentkezési rendszerének kiiktatása tilos.

b) Abban az esetben, amikor a felhasználók munkaállomásaikat felügyelet nélkül hagyják, kötelesek a munkaállomást zárolni úgy, hogy a zárolás csak az arra jogosult által legyen feloldható (pl. jelszóvédelemmel rendelkező képernyővédő használata).

c) A munkaállomás használatát nem szabad senkinek átengedni úgy, hogy eközben a munkaállomás funkcióinak illetéktelen használatával az informatikai biztonság sérülhessen.

d) A felhasználó a munkaállomás használata során csak a munkaállomásra telepített irodai, műszaki és egyéb adatfeldolgozó alkalmazásokat használhatja. Egyéb a munkakör ellátásához szükséges szoftver, alkalmazás, vagy hozzáférési módszer munkaállomásra való telepítését az illetékes szervezeti egység vezetője kezdeményezi az ISZK-hoz beadott igényléssel (papír vagy elektronikus úton).

e) Az igénylés pozitív elbírálása (szoftver feltételek, hardver feltételek és a licensz meglétének ellenőrzése) után az ISZK (vagy a helyi rendszergazda)

közreműködésével történik a telepítés. A telepítést az ISZK eszköznyilvántartásában is dokumentálni kell.

f) A munkaállomások merevlemezén személyes adat vagy annál magasabb osztályba sorolt adatot (érzékeny adat) csak a feldolgozás ideje alatt lehet tárolni. A munka befejezése, vagy hosszabb időre történő megszakítása esetén az adatokat a központi rendszerbe (pl.: fájl szerver, dokumentumtár, stb.) megfelelően továbbítani és a helyi merevlemezről törölni kell.

g) A számítógépes munka befejeztével a felhasználóknak a számítógépet ki kell kapcsolni. Indokolt esetben - munkaállomás esetében - folyamatos üzemelésre a szervezeti egység vezetője az ISZK-val konzultálva adhat engedélyt.

h) Otthoni munkavégzés, vagy bármely más célból adatot adathordozón, elektronikus levélben vagy egyéb más módon az intézmény informatikai rendszeréből kijuttatni csak a szervezeti egység vezetőjének írásos engedélyével szabad. Ez alól kivételt képez a felügyeleti szervek és egyéb külső szerződéses partnerek számára végzett adatszolgáltatás, kutatási, vagy más partnerkapcsolati, együttműködési feladatok során keletkezett és szükség szerint kicserélendő adatok. Szervezeti egység vezetőknek a rektor vagy a kancellár munkaköri jogon engedélyezi otthoni munkavégzés céljából a nem minősített adatok kivitelét. Tilos minősített adatot bármilyen formában az intézményen kívülre juttatni.

(12) Munkaállomásokra a távoli bejelentkezés csak az intézményi hálózaton belül lévő munkaállomásról engedélyezett. Belső munkaállomásnak minősül az Interneten bárhol elhelyezkedő a belső hálózathoz „virtuális privát hálózati” (VPN) kapcsolattal csatlakozott munkaállomás is.

18.§ Fokozott biztonságú munkaállomások

(1) Az egyetem magasabb vezető beosztású dolgozói által használt, az informatikai rendszereket és a számítógép hálózat felügyeletét ellátó munkaállomásokat, továbbá azon munkaállomásokat, melyek kritikus („A” biztonsági kategóriájú) rendszerek közvetlen munkaállomásai, és/vagy „minősített” adatot kezelnek, fokozott biztonsággal kell ellátni.

(2) Fokozott biztonságú munkaállomásra más felhasználó csak kivételes esetben a bejelentkezési jogosultsággal rendelkező személy engedélyével, a tulajdonos, vagy az általa megbízott személy jelenlétében jelentkezhet be.

(3) Ezen munkaállomásokon végzett rendszergazdai tevékenységet csak az ISZK munkatársai, munkalapon (papír vagy elektronikus alapú) részletesen dokumentálva végezhetnek.

19.§ Mobil munkaállomások használata

(1) Mobil munkaállomásnak minősülnek az intézményi, vagy személyes tulajdonban lévő hordozható eszközök típustól és modelltől függetlenül, amelyeket az intézményi informatikai hálózatra csatlakoztattak.

(2) Az ISZK-nak naprakész nyilvántartást kell vezetni az intézményi tulajdonú mobil munkaállomásokról, oktatni kell a felhasználókat a helyes és informatikai biztonsági

szempontból megfelelő használatról, és tudatosítani kell bennük a biztonsági kockázatokat.

(3) A mobil munkaállomások felhasználói felelősek az általuk használt eszközök biztonságos használatáért, ezen belül is különösen:

a) adatok kiszivárgása, elvesztése, megsérülése miatt bekövetkezett károk tekintetében;

b) a jogosulatlan szoftverhasználatból eredő jogi következményekre vonatkozóan;

c) vírusok és más rosszindulatú szoftverek okozta károk esetén;

d) lopás és az ebből származó károk esetén;

e) a felügyelet nélkül hagyott, vagy elvesztett eszköz biztonsági kockázatai miatt.

(4) Mobil eszközök az intézményi vezetékes számítógép hálózathoz csak az ISZK által meghatározott paraméterek beállítása estén csatlakoztathatók. A paraméterek ellenőrzését automatizált felügyeleti rendszer is végezheti.

(5) Az intézményi vezeték nélküli hálózatra való csatlakozás feltételeit a beállítási dokumentáció tartalmazza (http://www.uniduna.hu/iszk-wifi-szolgaltatas).

(6) Mobil munkaállomásokon tilos adatvédelmi szempontból „fokozott” vagy annál magasabb biztonsági osztályban lévő adatot tárolni. Oktatóknak a hallgatókkal kapcsolatos adataik kezelésére az Adatvédelmi szabályzat előírása vonatkoznak.

(7) Olyan mobil munkaállomás, amely nem rendelkezik helyi (a gépre telepített) vírusvédelmi szoftverrel, sem a vezetékes, sem a vezeték nélküli hálózathoz nem csatlakoztatható. A feltételnek eleget nem tevő munkaállomás csatlakoztatását a hálózatfelügyeleti rendszer automatikusan megakadályozhatja.

20.§ Munkaállomások adatainak mentése

(1) Minden olyan felhasználónak, aki munkája kapcsán adatkezeléssel, adatmódosítással foglalkozik, gondoskodnia kell a munkaállomásokon az általa létrehozott, kezelt intézményi állományok mentéséről (lásd 17.§(11)f).

(2) A felhasználó felelős a saját munkaállomásán bekövetkezett adatvesztésekért és az adatok sérüléséből keletkezett károkért.

(3) A felhasználó felelős továbbá:

a) Az általa készített mentésből visszaállíthatóak legyenek az adatok.

b) A mentéseket (vagy másolatot) központilag kijelölt tárhelyekre készítse („N” vagy „P” meghajtó). A központi tárhelyeket a rendelkezésre álló háttértároló kapacitások figyelembe vételével az Informatikai Szolgáltató Központ biztosítja.

(4) A felhasználó az adatmentés kivitelezéséhez az ISZK segítségét igénybe veheti.

21.§ Elektronikus levelezés és Internet használat információbiztonsági követelményei

(1) Az elektronikus levelezés, internet és intranet használat szabályai vonatkoznak minden felhasználóra, aki a megnevezett szolgáltatásokat használja.

(2) Hálózati munkaállomások az Internethez kizárólag az intézmény hálózati kijáratán (központi tűzfal) keresztül csatlakozhatnak. (Lásd még a 17.§(6) bekezdésbeli tiltásokat).

(3) Az Internetet és az elektronikus levelezést a felhasználók csak a hatályos DUE Informatikai Felhasználói Szabályzatban (jelen szabályzat 1. sz. melléklete) foglaltak szerint használhatják.

(4) Tilos tudatosan kihasználni az esetleg előforduló szoftverhibákat, védelmi hiányosságokat.

(5) Tilos az Informatikai Szolgáltató Központ által meghatározott rendszerbeállításokat megváltoztatni.

(6) Az elektronikus levelezésre vonatkozó további szabályok:

a) Dolgozók számára az intézményi postafiókok (névre szóló és a közös használatú fiókok) magán célú használata (magánanyagok tárolása) nem engedélyezett. Az intézményi postafiókokban csak a munkavégzéssel szorosan összefüggő leveleket lehet tárolni.

b) Hallgatók számára az intézményi postafiókok (névre szóló és a közös használatú fiókok) magán célú használata (magánanyagok tárolása) megengedett.

c) A DUE Adatkezelési és Adatvédelmi Szabályzatában „Különleges adat” biztonsági kategóriába sorolt adatok intézményen kívülre történő továbbításához az Adatkezelési és Adatvédelmi Szabályzatában meghatározott engedélyek szükségesek. Az ilyen adatot csak titkosított formában szabad elküldeni (pl.: HTTPS, S-MIME, jelszóval védett tömörített fájl, stb.).

d) Tilos a felhasználóknak olyan tartalmú elektronikus levelet az intézmény informatikai rendszeréből küldeni, amely az egyetem érdekeivel ellentétes.

e) Az Informatikai Szolgáltató Központ a felhasználók levelezési postafiókjainak méretét (mailbox), a rendszer által kezelt levelek méretét, technikai eszközökkel korlátozhatja a rendelkezésre álló központi erőforrások figyelembe vételével.

f) Dolgozók számára a postafiókjukba érkező elektronikus levelek automatikus átirányítása (továbbítása, forward) más levelező rendszerbe tilos.

g) Az intézmény által hivatalosan támogatott levelező rendszeren kívül más, elektronikus levelezést (pl.: freemail, hotmail, gmail stb.) hivatalos, egyetemet érintő ügyekre használni tilos (hivatalos levelet csak UNIDUNA.HU-s email címről lehet küldeni).

h) A levelezőrendszer és az abban forgalmazott üzenetek rendelkezésre állásának biztosítása az ISZK feladata. A saját munkaállomására letöltött (pl.: helyi személyes Outlook fájlba (PST-be) mozgatott) levelek kezelése, archiválása a felhasználók felelőssége.

(7) Internet használatra vonatkozó további szabályok:

a) Minden felhasználó saját felelősségére használja az Internetet, mint szolgáltatást, betartva az ide vonatkozó szabályokat, utasításokat, különös tekintettel a DUE Informatikai Felhasználói Szabályzatában (1. sz. melléklet) és az abban hivatkozott külső szabályzatban foglaltakban leírtakra.

b) A szerzői jogvédelemmel kapcsolatos jogszabályok betartása mindenkire nézve kötelező.

c) Az Internetről letöltött fájlokat csak vírusellenőrzés után szabad megnyitni.

d) Tilos a felhasználóknak az intézmény érdekeivel ellentétes cselekményt végrehajtani az Internet használata közben. Az Internet használata és az által megvalósított bármely cselekmény kizárólag a törvények és egyéb szabályok keretei között megengedett.

22.§ Informatikai biztonsági követelmények az IT rendszerek szállítási szerződéseiben

(1) A szolgáltatásért felelős szervezeti egység vezetője felelős azért, hogy az IT rendszerekhez történő beszállítások során a szállítói szerződések minimálisan tartalmazzák az alábbi részeket

a) Hatályos jogszabályoknak való megfelelés

b) Átadás / átvételi jegyzőkönyv vagy teljesítési igazolás (mint a szerződés melléklete).

c) Kapcsolattartó neve és elérhetősége

d) Technikai feltételek, paraméterek, specifikációk

e) Támogatási és/vagy garanciális feltételek

f) A beszállítás részletei (mikor, mit, ki, hogyan végez el?)

g) Üzembe helyezés esetén a részleteket (mikor, mit, ki, hogyan végez el?)

h) Jogi nyilatkozat (tulajdonjog, szoftver használati jog, stb.)

i) Biztonsági kérdések

j) Felelősségi körök elhatárolása

23.§ Informatikai eszközök beszerzése nyilvántartása és javítása

(1) Az informatikai eszközök beszerzése központi feladat, amely az ISZK közreműködésével történik. A beszerzés menetét az intézményi Közbeszerzési szabályzat és a Beszerzési szabályzat határozza meg.

(2) Az informatikai eszközöknek a számviteli nyilvántartásokon kívüli kötelező műszaki nyilvántartása az ISZK feladata. A nyilvántartás célja az eszközök technikai adatainak rögzítése, a szervizeléshez, garanciális követelések érvényesítéséhez szükséges adatok rendelkezésre állásának biztosítása, továbbá eszköz adathálózati helyének azonosíthatósága. A nyilvántartás az „N:\ISZK\Nyomtatványok\” mappában található „Informatikai eszköznyilvántartó lapon” történik. Az ISZK a papír alapú helyett elektronikus eszköznyilvántartást is alkalmazhat, amennyiben az elektronikus nyilvántartás legalább a nyilvántartó lapon rögzíthető adattartalmat képes kezelni. A megvásárolt eszközök üzembe helyezésével egy időben a nyilvántartó lapok kitöltése, vagy az azzal egyenértékű elektronikus adatfelvétel az ISZK feladata. Az ISZK csak a nyilvántartás rögzítését dokumentáló azonosító számmal ellátott eszközt támogat.

(3) A beszerzett informatikai eszközök ISZK nyilvántartásba vételi eljárásának elindításáról az eszközöket átvevő személy köteles gondoskodni (pl.: pályázatoknál, ha nem az ISZK munkatársai veszik át az eszközöket).

(4) Az „A” és „B” biztonsági kategóriájú rendszerek működtető szoftvereinek beszerzése központi feladat, amely az ISZK központvezetőjének előterjesztése alapján történik. Egyéb kategóriába tartozó szoftverek beszerzését az ISZK központi célból saját hatáskörben, vagy a szervezeti egységek igénylése esetén a beszerzésben közreműködve az (1) pontban meghatározottak szerint történik.

(5) Nem szerver célú számítógépek (asztali, vagy mobil PC, önálló munkaállomás) – amennyiben nem ingyenes operációs rendszerrel kívánják használni – csak operációs rendszerrel (OEM) együtt vásárolhatóak (a jogtisztaság biztosítása miatt).

(6) A intézményi célra, vagy központi keretből beszerzett szoftverek nyilvántartását az ISZK végzi. A szervezeti egységek speciális célú, esetleg saját beszerzésű szoftvereit önállóan kötelesek nyilvántartani. A szoftverek nyilvántartásában legalább a következő adatoknak és mellékleteknek szerepelnie kell:

a) A szoftver pontos megnevezése

b) Felhasználó szervezeti egység megnevezése

c) Felhasználási cél

d) A beszerzés dátuma

e) Az adathordozó, vagy licenc formájában megjelenő szoftvertermék legutolsó használhatósági dátuma (lejárat napja)

f) Beszerzett példányszám

g) Telepíthető példányszám

h) Használhatósági példányszám (pl. felhasználószámhoz köthető)

i) Szállítói számla másolata

j) Licencigazolás (amennyiben létezik)

(7) A szervezeti egységek szoftvernyilvántartását az ISZK számára hozzáférhetővé kell tenni.

(8) Informatikai eszköz meghibásodását az ISZK-n be kell jelenteni. Bejelentés az iszk@uniduna.hu email címen vagy telefonon a 610-es melléken tehető meg. Ha a javítást az ISZK saját hatáskörben nem tudja elvégezni, a szakszervizbe szállítást megszervezi. Garanciaidőn túli szervizben történő javíttatás esetén az ISZK-nak kötelessége előzetesen árajánlatot kérni. A gazdaságtalan javítási feltételek esetén elállhat a javítás megrendelésétől.

24.§ Internet domain név adminisztráció

(1) Az interneten a szervezetek a domain nevükkel jelennek meg. A domain név a hierarchikus rendszeren belüli azonosító, egyedi és jellemző a használó szervezetre. A domain nevek kezelésére egy világméretű hierarchikus rendszer működik. Ebben a rendszerben megbízott szervezetek látják el a domain nevek regisztrálását és

nyilvántartását. A domain név használatának a használó szervezet számára adminisztratív és műszaki feltételei is vannak. A domain név jelentős értéket is képviselhet.

(2) A Dunaújvárosi Egyetem internet domain neve intézményi konszenzussal az „uniduna.hu”.

(3) A domain névvel kapcsolatos adminisztratív és műszaki feltételek folyamatos biztosításáért az Informatikai Szolgáltató Központ központvezetője felelős.

(4) A domain névvel rendelkező szervezet az interneten nyilvánossá tett szolgáltatásihoz való hozzáférést az ISZK által működtetett központi DNS szolgáltatás biztosítja („B” biztonsági kategóriás rendszer).

(5) Az intézmény domain név adminisztrációs szervezete nem zárkózik el önálló az „uniduna.hu” alá regisztrálható aldomain adminisztrációjának delegálásától. Erre vonatkozó igényt az Informatikai Szolgáltató Központ központvezetőjéhez kell eljuttatni, aki a technikai és jogi feltételek vizsgálata alapján jóváhagyja vagy elutasítja a kérést.

25.§ Gazdálkodás az IP címekkel

(1) Az interneten való forgalmazáshoz szükség van az Internet Protokoll által használt egyedi címekre. Az IP címeket a hálózatának méretétől függően igényelheti egy-egy szervezet a rendelkezésre álló címtartományokból. Az igénylést általában az internet szolgáltató számára kell benyújtani. A szolgáltató az igény elbírálását követően a címeket saját címteréből biztosítja. A Dunaújvárosi Egyetem 4 db C-osztályú nyilvános IPv4 címtérrel és egy darab /64-es IPv6-os címtérrel rendelkezik. Ezen címtereket a belső hálózat struktúrájához igazodóan használja fel.

(2) A szervezetek számára használható IP címek készlete erőforrás kategória, ezért nyilvántartani és gazdálkodni kell vele. Az IP-címgazdálkodás nem választható el a hálózat üzemeltetéstől.

(3) Az intézmény IP-cím gazdálkodásáért az Informatikai Szolgáltató Központ a felelős.

(4) A nyilvános IP-címeken kívül a belső hálózatban belső címeket (nem nyilvános, RFC-1918) is lehet használni. Belső címeket használó számítógépek, csak kiegészítő módszerek alkalmazásával tudnak kommunikálni a külvilággal. A Dunaújvárosi Egyetem a belső címekkel való nyilvános kommunikáció biztosítására hálózati címfordítást (Network Address Translation – NAT) és/vagy Internet Proxy Szerver használatát támogatja.

(5) Az IP-címek kiosztása statikusan (fix IP-cím beállítás), vagy dinamikusan (DHCP szerver szolgáltatás segítségével) történhet.

(6) Az IP-címek statikus, vagy dinamikus kiosztása mind a nyilvános, mind a belső címekre lehetséges. A kiosztás módjának meghatározása az ISZK kizárólagos hatásköre.

(7) Szervezeti egységek kizárólag az ISZK által biztosított IP-címeket használhatják. Azon szervezeti egységek, melyek címtartományokkal rendelkeznek, kötelesek naprakész nyilvántartást vezetni az általuk használt, vagy éppen használaton kívüli IP-címekről. A munkaállomások és IP-címek hozzárendelésének változtatása az ISZK felé jelentésköteles.

26.§ Munkaállomások adatkezelése jogviszony megszűnése esetén

(1) Az intézményi informatikai eszközök (pl.: számítógépek, tabletek, stb.) magán célú használata (magánanyagok tárolása) nem engedélyezett. Az intézményi informatikai eszközökön csak a munkájával szorosan összefüggő adatokat (állományokat) tárolhat. A dolgozó jogviszonyának megszűnése esetén az alábbi eseteket különböztetjük meg:

a) Lemondás esetén: a munkavégzés alóli felmentés napját megelőzően a dolgozó köteles a használatában lévő intézményi informatikai eszközökről az esetleges személyes (nem intézményi munkavégzéssel kapcsolatos) fájljait törölni.

b) Azonnali hatályú felmentés esetén: a munkavégzés alóli felmentés napján a dolgozó az adott szervezeti egység vezető által kijelölt kolléga felügyelete mellett köteles a használatában lévő intézményi informatikai eszközökről az esetleges személyes (nem intézményi munkavégzéssel kapcsolatos) fájljait törölni. Szükség esetén az adott szervezeti egység vezető kérheti az ISZK segítségét a feladat informatikai támogatásában.

(2) A fentiek végrehajtása után az adott szervezeti egység vezető dönt a dolgozó által használt intézményi informatikai eszközökön lévő intézményi adatok további sorsáról (pl.: a gépen marad vagy más kollégának a gépére kerül áthelyezésre).

27.§ Személyes postafiók (email) adatkezelése jogviszony megszűnése esetén

(1) Az intézményi postafiókok (névre szóló és a közös használatú fiókok) magán célú használata (magánanyagok tárolása) nem engedélyezett. Az intézményi postafiókokban csak a dolgozó munkavégzésével szorosan összefüggő levelek tárolhatóak. A dolgozó jogviszonyának megszűnése esetén a személyes postafiókban lévő adatok kezelése az alábbiak szerint történik:

a) Lemondás esetén: a munkavégzés alóli felmentés napját megelőzően a dolgozó köteles a személyes postafiókjából az esetleges személyes (nem intézményi munkavégzéssel kapcsolatos) leveleit törölni.

b) Azonnali hatályú felmentés esetén: a munkavégzés alóli felmentés napján a dolgozó az adott szervezeti egység vezető által kijelölt kolléga felügyelete mellett köteles a személyes postafiókjából az esetleges személyes (nem intézményi munkavégzéssel kapcsolatos) leveleit törölni. Szükség esetén az adott szervezeti egység vezető kérheti az ISZK segítségét a feladat informatikai támogatásában.

c) A személyes levelek törlése után a személyes fiók kiexportálásra (fájlba mentés) kerül (ebben szükség esetén az ISZK segítséget nyújt).

d) A kiexportált állomány a szervezeti egység vezetője által meghatározott személynek átadásra kerül (elektronikus dokumentum átadás).

e) A postafiók ez után törlésre kerül.

f) A távozó dolgozó e-mailcíme bekerül egy gyűjtőbe. Az itt tárolt e-mail címekre automatikus üzenet kerül beállításra amely tájékoztatja a levél küldőjét, hogy „az adott e-mailcím nem aktív, kérjük, hogy az adott tevékenységet/területet érintően nézze meg a telefonkönyvben, hogy kihez tud fordulni”. A gyűjtőből az email címek legkésőbb egy év múlva kerülnek ki.

(2) Az e-mail cím személyes adat és annak kezelése csak a jogviszony fennállásáig, illetve az egy éves megőrzési idő pedig adminisztratív érdekből indokolható. A dolgozónak lehetősége van az email címének (mint személyes adatnak) a törlését az egy éves adminisztratív időszak lejárta előtt kérni (akár a jogviszony megszűnésének napján is). Ezt levélben (papír alapon vagy email-ban) kell jeleznie az ISZK központvezetőjének. A levél beérkezését és iktatását követően az ISZK központvezető gondoskodik az email-cím törléséről.

III. SZOLGÁLTATÁSSZINT MENEDZSMENT

28.§ A szolgáltatásszint menedzsment folyamata

(1) „A" és „B" biztonsági kategóriájú rendszer csak az Informatikai Szolgáltató Központ által üzemeltethető. Indokolt esetben (az ISZK-val együttműködve) más szervezeti egység dolgozói is bevonhatóak az üzemeltetésbe.

(2) „C" biztonsági kategóriájú rendszer csak az Informatikai Szolgáltató Központ által, vagy engedélyével üzemeltethető. Az üzemeltetni kívánt szolgáltatás tartalmára a szolgáltatásszint megállapodásban (SLA) az üzemeltető szervezeti egység vezetője tesz javaslatot. A szolgáltatás indíthatóságáról a megállapodási javaslat alapján az ISZK központvezetője dönt. Elutasító döntés esetén a javaslattevő 15 napon belül panasszal élhet az intézmény kancellárjánál. Ilyen esetekben az I.6.§(4) bekezdésében meghatározott ad-hoc bizottság vizsgálatot végez és javaslatot tesz az intézmény kancellárjának. Végleges döntés meghozatala a kancellár hatásköre.

(3) „A", „B" és „C" biztonsági kategóriába nem sorolt rendszer esetében a rendszert üzemeltető szervezeti egység vezetője kérheti a szolgáltatás (2) szerint történő jóváhagyását. Az így jóváhagyott rendszerek „C" biztonsági kategóriájúnak minősülnek.

29.§ A szolgáltatási megállapodások (SLA) tartalma

(1) Az intézmény által nyújtott informatikai szolgáltatásokra szolgáltatási szint megállapodások készülnek (Service Level Agreement – SLA). A szolgáltatások nyújtása a megállapodások alapján történik. A szolgáltatási szint megállapodások minimális tartalma

a) Szolgáltatás neve (egyedi megnevezés)

b) Adminisztratív és technikai kapcsolattartó neve

c) SLA Verziószáma

d) Lezárás dátuma (Az SLA lezárásának dátuma)

e) A szolgáltató és a jóváhagyó megnevezése. (A szolgáltatás Igénybevevője, vagy ezek képviselője, illetve a szolgáltató, illetve képviselője mellett az ISZK részéről a jóváhagyó megnevezése)

f) Rövid szolgáltatás leírás / összegzés. (Pár mondatban, röviden összefoglalva a szolgáltatás célját, tartalmát.)

g) Érvényesség / megszűnés (általában évente felülvizsgálandó, automatikusan meghosszabbításra kerül)

h) Aláírások (név, beosztás, dátum)

i) Szolgáltatás leírása (részletes, technikai leírás)

- Kulcs funkciók
- Kiterjedés, hatókör
- Elhelyezés (fizikai elhelyezés, helyiség, eszközök, szerver, stb.)

- Kik vehetik igénybe
- Kategóriába sorolás (A-D, a II.9.§ alapján)

j) Szolgáltatási időszak (pl.: 7x24; 8-16 munkanapokon, stb.)

k) Szolgáltatás használata

- Ki a kapcsolattartó (szolgáltatás gazda) (hogyan érhető el)
- Hol igényelhető
- Hogyan, milyen módon igényelhető (pl.: írásban, formanyomtatványon, személyesen, stb.)
- Mekkora az átfutási időtartam.
- Milyen feltételekkel vehető igénybe. (Adott munkakör, adott tanszék, stb.)

l) A szolgáltatással kapcsolatos tájékoztatás módja.

m) Karbantartási időszakok (éves szinten megadva, pl.: minden hónap első hétfő 21-23h.).

n) Rendelkezésre állás (%)

- Milyen mérőszámokkal mérhető
- Hogyan történik a mérése

o) Megbízhatóság.

- Milyen mérőszámokkal mérhető. (MTBF)

p) Támogatás.

- Hogyan érhető el (Mi a teendő hiba észlelése esetén?).
- Milyen támogatást nyújt.
- Mi a teendő támogatási időszakon kívül (pl.: hétvégén, éjjel, stb.).

q) Biztonság, incidens-kezelés, csak a sajátosságokat / kivételeket kell említeni. (Pl.: egyedi/kiemelt biztonsági kockázat, illetve ennek kezelése.) Továbbá:

- Hol, hogyan lehet az incidenseket bejelenteni
- Mennyi időn belül kerül feldolgozásra a bejelentés
- Van-e és ha igen mekkora a javítási időablak
- Visszajelzés menete az incidens lezárásakor

r) Teljesítmény / minőség.

- Optimális teljesítményadatok (pl.: elérési idő, válaszidő, ami értelmezhető az adott szolgáltatás esetében, stb.)

s) Funkcionalitás (ha értelmezhető).

- Mennyi és milyen jellegű hiba tolerálható a szolgáltatáson belül

t) Változáskezelési eljárások.

- Normál esetben hivatkozás a szervezet változáskezelési eljárására. Itt csak a sajátosságokat / kivételeket kell említeni.

u) IT üzletmenet folytonosság.

- A DRP/BCP –re hivatkozás, itt csak a sajátosságokat / kivételeket kell megemlíteni.

v) Felülvizsgálat ideje / időszak (az SLA felülvizsgálatára, módosítására minden a szolgáltatásban, illetve a szolgáltatás nyújtásának feltételeiben bekövetkezett érdemi változás esetében szükség van.)

w) Technikai szójegyzék. (azon speciális kifejezések, amelyek szerepelnek az SLA-ban és magyarázatra szorulnak.)

(2) Az SLA mintaűrlap az „N:\ISZK\Nyomtatványok\" helyen található.

30.§ Megfigyelés, jelentés és áttekintés

(1) Az előre ütemezett (scheduled) szolgáltatás-kieséseket az SLA-ban meghatározott módon publikálni kell, ennek felelőse az adott szolgáltatást nyújtó szervezeti egység vezetője.

(2) Az SLA-kban megadott szolgáltatási paraméterek monitorozásért az adott szolgáltatást nyújtó szervezeti egység vezetője a felelős.

(3) Az SLA-k tartalmazzák az adott szolgáltatás monitorozási feltételeit. Az SLA-kban rögzített méréseket és jelentéseket az ISZK kijelölt felelőse, illetőleg a szolgáltatás üzemeltetője áttekinti, és a fejlesztési tennivalók közé felveszi a teljesítési problémákat mutató területeket.

(4) Az SLA-kban foglaltak betartása csak az alkalmazott műszaki/technikai feltételek rendelkezésre állása esetén követelhető meg.

IV. ÜGYFÉLSZOLGÁLAT, INCIDENSKEZELÉS

31.§ Központi ügyfélszolgálat (Help Desk)

(1) Központi ügyfélszolgálatot az ISZK látja el. A központi ügyfélszolgálatra az „A” és „B” biztonsági kategóriájú rendszerekre vonatkozó hiba és/vagy incidens (továbbiakban csak incidens) bejelentése csak írásban történhet (papír, e-mail vagy web űrlap útján). A bejelentés adattartalmára egy mintaűrlap a 4. sz. mellékletben található. A bejelentés aktuális módját és a megadandó adatokat a szolgáltatás SLA-ja tartalmazza.

(2) Az ügyfélszolgálatnak minden bejelentést regisztrálnia kell és ennek tényéről (egy, az esetre egyedi hivatkozást lehetővé tevő azonosítóval ellátva) értesítenie kell a bejelentőt (konfirmáció). A konfirmáció automatikusan is létrehozható (válaszlevél). Szintén értesíteni kell a bejelentőt az ügy lezárását követően az üggyel kapcsolatos eredményekről.

(3) A központi ügyfélszolgálat csak a hatáskörébe tartozó rendszerekkel összefüggő szoftver és műszaki problémákat rögzít, megoldását kezdeményezi. Nem vesz részt harmadik féllel felmerült vitás kérdések rendezésében.

(4) A „C” biztonsági kategóriájú nem ISZK üzemetetés alatt álló rendszerekre beérkező hibajelzéseket az ISZK továbbítja a rendszer üzemeltetőjének.

32.§ Incidenskezelés

(1) Incidens-kezelést az adott szolgáltatás SLA-ja alapján, az abban leírtaknak megfelelően köteles végezni a szolgáltató.

33.§ Incidensosztályozás és prioritás hozzárendelés

(1) A bejelentett incidensek kezelésére a rendszer biztonsági besorolásától („A”-„D”) függően priorizálva kerül sor. A prioritás hozzárendelése az ügyfélszolgálat feladata és felelőssége. Több incidens fellépésekor a magasabb prioritású incidens megoldása elsőbbséget élvez.

V. PROBLÉMAKEZELÉS

34.§ Probléma és az ismert hiba kezelése

(1) Az üzemeltetés során felmerült problémákat az üzemeltető személyzet, és/vagy a felhasználók jelezhetik, illetve ahol erre műszaki lehetőség van és kiépített felderítő rendszer üzemel, ott automatikus jelzés is történhet. Az ISZK központvezetője által megbízott szervezeti egység vagy munkacsoport automatikus incidens és/vagy probléma felderítő rendszereket üzemeltethet az SLA-ban rögzített esetekben, és az ott leírt szankciókkal élhet.

(2) A visszatérő, több incidenst kiváltó okként megjelenő problémáknak a probléma-adatbázisba való felvétele manuális, amit az üzemeltető személyzet vagy az ügyfélszolgálat végez.

(3) Az ismert hibák kiszűrése a hibafelvétel során történik.

(4) Az adott szolgáltatáshoz tartozó és meghatározott időn túl fennálló ismert hibákat a szolgáltató az SLA-ban meghatározott hivatalos információs csatornákon (levelezési lista, web portál) publikálja.

35.§ Trend-azonosítás

(1) Ahol a műszaki feltételek ezt lehetővé teszik az SLA-kban előírt teljesítménymutatók figyelése során a szolgáltatónál statisztikai értelemben vett idősorok jönnek létre, melyek elemzése az adott szolgáltatást nyújtó szervezeti egység vezetőjének a feladata. Az ilyen módon képződött adatokat a szolgáltató illetőleg a szolgáltató egység vezetője felhasználja a fejlesztési irányok és projektek kijelölésekor. (PL. forgalmi, terhelési adatok változása, stb.)

36.§ Probléma megelőzés

(1) Az egyes szolgáltatások üzemeltetőinek nem csak reaktív, hanem preventív intézkedéseket is kell foganatosítaniuk a szolgáltatás zavartalan működtetésének érdekében. Ezek lehetnek általános és az adott szolgáltatásra speciálisan jellemző feladatok, mint:

a) Igény szerinti újraindítás, reset/reload

b) A javítócsomagok, patchek, fixek telepítése

c) A jelszavak és hozzáférési kódok rendszeres cseréjének előírása

d) A naplóállományok rendszeres kiértékelése

(2) Az ISZK biztosíthatja a probléma megelőzés alapinfrastruktúráját, de az intézmény egyes szervezeti egységei jogosultak további megelőző intézkedéseket végrehajtani, azonban az intézkedési tervet kötelesek előzőleg bejelenteni az ISZK központvezetőjének, akinek a jóváhagyása után az intézkedések foganatosíthatóak.

(3) A védelmi intézkedés bejelentésének elmulasztásából illetve a saját – nem megfelelő – üzemeltetésből következő károk (káresemények, rendszerleállások) az adott szervezeti egység felelősségi körébe tartoznak.

(4) A probléma megelőzés érdekében az ISZK legalább évente, de kiugró probléma jelentkezése estén akár alkalomszerűen is (pl. veszélyes vírustámadás előjelzés, fontos biztonsági frissítések megjelenése, stb.) konzultációt szervez a rendszerüzemeltető szervezeti egységek rendszergazdái részére.

VI. KONFIGURÁCIÓKEZELÉS

37.§ Alapelvek és terminológia

(1) Minden szolgáltatás és szolgáltató rendszer esetében az üzemeltetőnek teljes körű leírással kell rendelkeznie a szolgáltatás működéséhez szükséges hardver és szoftver komponensekről, valamint azok konfigurációjáról (üzemeltetési dokumentáció).

(2) Az üzemeltetési dokumentáció vázlata a 2. számú mellékletben található.

38.§ A konfigurációkezelés adatbázisa

(1) Az adott rendszer üzemeltetőjének minden szolgáltatás és szolgáltató rendszer esetében időrendben vezetnie kell a felépítő komponensek változását leíró adatbázist. Minden változás esetén az alábbiakat kell megadni:

a) A változó komponensek egyértelmű azonosítását lehetővé tevő adatok

b) Változás szükségességének indokai

c) Tesztelésre vonatkozó adatok

d) A visszaállási teendőket tartalmazó hivatkozást.

(2) A konfigurációkezelés adatbázisa elektronikus úton is előállítható.

VII. VÁLTOZÁSKEZELÉS

39.§ Központosított változás-felügyelet

(1) Az „A”, „B” és „C” biztonsági besorolású informatikai rendszerek esetében az ISZK központi változásfelügyeletet gyakorol.

40.§ Változáskezelési folyamatok

(1) A központi változás-felügyelet menete:

a) „A”, „B” biztonsági kategóriájú rendszer esetén az ISZK saját hatáskörben, „C” biztonsági kategóriájú rendszer esetén a szolgáltatás üzemeltetője engedélyezteti a megvalósítandó hardver és szoftver konfigurációt az adott terület ISZK-n belül illetékes szakértőjével a változtatás megkezdése előtt.

b) A területi szakértőket az ISZK központvezetője jelöli ki. A területi szakértő személye nem eshet egybe a szolgáltatás üzemeltetőjével.

c) Területei szakértői feladatot külső, megbízásos jogviszonyú személy is elláthat.

d) Az engedélyezett változtatásokat a szolgáltatás üzemeltetője az üzemeltetési leírásban foglaltak alapján végrehajthatja, sikeres végrehajtás esetén a rendszerdokumentációt módosítja.

41.§ Szerepkörök és felelősségek

(1) A szolgáltatás üzemeltetője teljes felelősséggel tartozik minden olyan beavatkozásért, amit a felelős területi szakértő nem engedélyezett, illetve amelyek esetében a rendszerüzemeltetési leírást nem tartották be.

(2) A területi szakértő felelősséggel tartozik a hardver vagy szoftver konfigurációk engedélyezéséért, abban az esetben is, ha ezek működőképességéről nem győződött meg.

(3) Az ISZK központvezetője tartozik felelősséggel azon területekért, amelyekre területi szakértőt nem jelölt ki.

VIII. KIADÁSKEZELÉS

42.§ Kiadáskezelés - új szolgáltatás indítása

(1) Központi szolgáltató rendszerek megvalósítását a rendszer dokumentálását, valamint a szolgáltatás tesztelését az ISZK végzi. Az auditálási tevékenységre szakértői közreműködést is igénybe lehet venni, amennyiben a szükséges ismeretekre nem áll rendelkezésre megfelelő szakember az ISZK-n belül. A sikeres tesztüzem után a szolgáltatás üzembe állítását az ISZK központvezetője engedélyezi. Az „A”, „B” és „C” kategóriás rendszerek esetében a szolgáltatás elindításának feltétele, hogy az ISZK központvezetője jóváhagyja az SLA-t, az üzemeltetési dokumentációt, a rendszerkonfigurációt és a változáskezelési folyamatot. Vitás esetekben a III.28.§(2) pontban foglaltaknak megfelelően kell eljárni.

43.§ A hiteles szoftver tár

(1) Az ISZK központilag hozzáférhető módon létrehozza és karbantartja a központilag beszerzett szoftverek eredeti példányainak és az installációs csomagjainak tárát. Amennyiben a beszerzett szoftver korlátozott hozzáférésű, meg kell határozni a hozzáféréssel rendelkezők körét.

(2) A szoftvertár kezelésével kapcsolatos felelősség:

a) Legfrissebb verziók letöltése, a csomagok frissítése.

b) Patchek, hotfixek letöltése, közzététele.

c) Programok, programcsomagok vírusellenőrzése.

d) Hozzáférési jogosultságok kezelése.

e) Kizárólag jogtiszta szoftverek közzététele.

(3) A szoftvertár automatikus mechanizmusokat is tartalmazhat, amelyek a biztonsági szempontból szükséges frissítéseket, védelmi programokat felhasználói beavatkozás nélkül telepíthetik a felhasználók számítógépeire.

44.§ Licencek kezelése

(1) Minden szolgáltató rendszer esetében a törvényes működés bizonyítását lehetővé tevő licencek tárolása az üzemeltető szervezeti egység vezetőjének kötelezettsége. Azon programok esetében, amikre az intézmény Campus licenccel (Tisztaszoftver Program), vagy intézményi korlátozott licenccel rendelkezik, az ISZK végzi a licencek tárolását és a kiadás elbírálását (kiadható, telepíthető).

(2) Az elbírálás és technikai kiadás munkáját Az ISZK központvezetője termékenként más munkatársakra is átruházhatja.

IX. IT SZOLGÁLTATÁSFOLYTONOSSÁG BIZTOSÍTÁSA

45.§ Kockázatkezelés

(1) Minden „A” illetve „B” kockázati besorolású szolgáltató rendszer esetében rendelkezni kell olyan kockázatelemzéssel, ami a rendszer által nyújtott szolgáltatások részleges vagy teljes kimaradásának az intézmény működőképességére (működési folyamataira) tett hatásait tartalmazza.

(2) Külön kell kezelni a szolgáltatás elérhetetlenségéből, illetőleg az adatok sérüléséből származó hatásokat. A kockázatelemzési dokumentum előállítása és karbantartása a szolgáltatás üzemeltetőjének és a szolgáltatás gazdájának az együttes feladata.

(3) A kockázatelemzésnek tartalmaznia kell azt a javaslatot, amely meghatároz egy hardver és szoftver környezetet, amelynek alkalmazása esetén a kockázat jelentősen csökkenthető, esetleg meg is szüntethető (ajánlott hardver és szoftver környezet).

46.§ Vészhelyzetek kezelése és az IT szolgáltatásfolytonossági terv

(1) Az „A” illetve „B” kockázati besorolású szolgáltató rendszer esetében az informatikai vészhelyzetek kezelésére az „Informatikai katasztrófa-elhárítási kézikönyv” ad iránymutatást. A kézikönyv az alábbi teendőket rögzíti:

a) Milyen helyettesítési lehetőségek (műszaki, technológiai és szervezési megoldások) állnak rendelkezésre az adott szolgáltatás kiesése esetén (vészhelyzet)

b) Milyen intézkedéseket kell megtenni a működés folytonosságának fenntartása érdekében.

c) Vészhelyzet esetén kik az intézkedésre jogosultak.

d) Vészhelyzet, illetve súlyos szolgáltatás folytonossági kiesés estén ki(ke)t kell értesíteni az intézkedésekről.

(2) A dokumentum előállítása és karbantartása a szolgáltatás üzemeltetőjének és a szolgáltatás gazdájának az együttes feladata.

X. RENDELKEZÉSRE-ÁLLÁS BIZTOSÍTÁSA

47.§ Rendelkezésre-állás, megbízhatóság, szervízelhetőség

(1) Az intézmény működése szempontjából kritikus szolgáltatások („A” és „B” kategóriájú rendszerek) esetében az ISZK központvezetője a szolgáltatást igénybevevő terület felelős vezetőjével egyetértésben határozza meg azt a rendelkezésre állási intervallumot, amiben a szolgáltatásnak elérhetőnek kell lennie.

48.§ Karbantarthatóság, biztonság szintjei

(1) Az adott szolgáltatás üzemeltetőinek a szolgáltatás aktuális üzemeltetői dokumentációjában fel kell tüntetni azon műszaki megoldásokat, amelyek a szolgáltatás meghatározott elérhetőségi (rendelkezésre állási) paramétereit hivatottak biztosítani (pl. redundanciát, failover-t biztosító rendszerkomponensek). Az üzemeltetőknek a szolgáltatás következő éves fejlesztési tervében rögzíteniük kell az elavult, nem szervizlehető komponensnek a cseréjére vonatkozó javaslatot.

49.§ A magas szintű rendelkezésre-állás tervezése

(1) „A” és „B” és „C” kategóriájú rendszerek esetében a rendelkezésre-állás biztosítását tervezni kell. A terv elkészítése a szolgáltató egység vezetőjének és a szolgáltatás gazdájának együttes feladata. A tervezés ellenőrzéséért az ISZK központvezetője felelős.

XI. KAPACITÁSOK BIZTOSÍTÁSA

50.§ Kapacitáskezelés

(1) Az ISZK központvezetője a felelős azért, hogy a felhasználóktól beérkező igények, a szolgáltatói környezet változása, a technikai fejlődés figyelembe vételével tervezze, és az elfogadott intézményi költségvetés keretin belül javaslatot tegyen az intézmény működéséhez szükséges IT-kapacitások meghatározására.

51.§ Kapacitástervezés

(1) A szolgáltatást biztosító rendszer várható terhelését az üzemeltető szervezeti egység vagy munkacsoport az elmúlt időszakok használati trendje alapján évente előrejelzi a következő egy éves időtartamra.

(2) Az elkészített következő évi terhelés előrejelzés alapján az üzemeltetők kapacitástervet készítenek, aminek tartalmaznia kell az összes olyan rendszerkomponens listáját, amit a szolgáltatás zavartalan biztosítása érdekében a várható terhelést figyelembe véve módosítani vagy bővíteni kell.

(3) A kapacitásterv részét képezi a technikai és műszaki tervezés.

52.§ A kapacitáskezelés eleme

(1) A nem ISZK által üzemeltetett szolgáltatások esetében az üzemeltető az adott szolgáltatás kapacitásterve alapján fejlesztési tervet készít, amelyet a következő évi költségvetés tervezetével együtt benyújt az ISZK központvezetőjének.

(2) A kapacitástervek és a fejlesztési tervek összegyűjtése után az ISZK központvezetője döntés-előkészítő anyagot készít a kancellár részére. A kancellár az intézményi lehetőségeket figyelembe véve szolgáltatásonként külön-külön, döntést hoz a fejlesztésekről vagy azok elutasításáról.

XII. ZÁRÓ RENDELKEZÉSEK

53.§ Az IIBSZ változásmenedzsmentje

(1) Az IIBSZ-el kapcsolatos észrevételeket, változtatási javaslatokat az ISZK központvezetőjének címzett, a 3. sz. mellékletben található változáskezelési lapon (vagy vele megegyező tartalmú elektronikus levélben) lehet benyújtani.

(2) Az ISZK központvezetője megvizsgálja a változtatási javaslatot és dönt annak elfogadásáról.

a) Elfogadás esetén előkészíti a módosítást az egyetem szenátusának.

b) Elutasítás esetén a javaslattevő kezdeményezheti a kancellárnál az I.6.§(4) bekezdésben meghatározott ad-hoc bizottság összehívását. A bizottság véleményezi a beadványt és javaslatot teszt a szenátusi jóváhagyásra vagy elutasításra.

(3) Az ISZK központvezetője a szenátusi határozatot követő 8 munkanapon belül írásban köteles tájékoztatni az indítványozót a javaslat vagy beadvány sorsáról és a jogorvoslati lehetőségekről.

(4) Az IIBSZ mellékleteinek módosítását az ISZK központvezetője saját hatáskörben végzi konzultálva az érintett szervezeti egységek vezetőivel.

(5) Az IIBSZ mellékletek ISZK központvezetői utasítások formájában készülnek és módosulnak.

54.§ Hatályba lépés

(1) Jelen szabályzatot a Dunaújvárosi Egyetem Szenátusa 98-2018/2019. (2019.05.28.) sz. határozatával fogadta el, amely 2019.05.29. napján lép hatályba.

(2) Jelen szabályzat közzétételérő az Egyetem a helyben szokásos módon gondoskodik, honlapján hozza nyilvánosságra.

(3) Jelen szabályzat elérési útvonala: N:\-Szervezeti Egységek - Nyitott\3 - Szabályzatok\ÉRVÉNYES SZABÁLYZATOK

Dunaújváros, 2019 május 28.

Dunaújvárosi Egyetem 1. Dunaújváros

Dr. habil András István
rektor
Szenátus elnöke

Kiss Ádám Sándor
kancellár

Az Informatikai és Információbiztonsági Szabályzat mellékletei

1. *sz. melléklet:* A Dunaújvárosi Egyetem Informatikai Felhasználói Szabályzata (DUE-AUP)
2. *sz. melléklet:* Üzemeltetési dokumentáció vázlat
3. *sz. melléklet:* IIBSZ változáskezelési lap
4. *sz. melléklet:* „A” és „B” biztonsági kategóriájú rendszerek incidens bejelentés űrlap/sablon

1.sz. melléklet.

A Dunaújvárosi Egyetem Informatikai hálózatának Felhasználói Szabályzata (DUE-AUP)

1. Bevezetés

(1) A jelen szabályzat a Dunaújvárosi Egyetemen (DUE) belül működő magáncélú helyi adathálózat (DUENET) használatát szabályozza a hálózati szolgáltatásokat igénybe vevő felhasználók számára. A Dunaújvárosi Egyetemet ezen szabályzat tartalmának érvényesítése közben a hálózat üzemeltetésért felelős Informatikai Szolgáltató Központ (ISZK) képviseli. A képviselő szervezeti egység különösen a hálózat működési állapotainak ellenőrzésére hálózat-felügyeletet gyakorol. Jelen szabályzat értelmezése szerint felhasználó az intézmény polgára (hallgató, oktató, egyéb dolgozó), valamint az intézménnyel szakmai kapcsolatban álló egyéb szervezetek munkatársa, amennyiben a DUE számára a felhasználói jogosultságot megadta.

(2) Jelen szabályzat a Nemzeti Információs Infrastruktúra Fejlesztési Program működtetéséről szóló 5/2011. (II. 3.) Korm. rendelet keretében működtetett számítógép-hálózat (a továbbiakban: KIFÜ hálózat) Felhasználói Szabályzatára épül, és az abban lefektetett elveket a helyi sajátosságokkal kiegészítve követi.

2. A DUENET hálózat célja

(1) A DUENET hálózat célja helyi, országos és nemzetközi számítógépes hálózati kapcsolatok, információs szolgáltatások biztosítása a DUE felhasználói kör részére oktatási, tudományos és kulturális célokra. A hálózatot a végfelhasználók első sorban a fenti célokra használhatják. Ebbe beleértendő a hálózatnak az intézmény alaptevékenységéhez kapcsolódó adminisztratív és információs feladataival összefüggő célokra történő használata is. Korlátozott mértékben megengedett a hálózat magáncélra történő felhasználása, amennyiben a használatból kizárható az üzleti célú felhasználás. A hálózat ezen belül minden olyan tevékenységre használható, amelyet a 3. pont nem tilt.

(2) Aki a DUENET hálózatából más hálózatba kilép, az idegen hálózatra érvényes szabályokat is köteles betartani. Az intézményen kívüli hálózathasználat tekintetében elsősorban a KIFÜ hálózatának felhasználói szabályait kell figyelembe venni. (https://kifu.gov.hu/document-library/document/felhaszn%C3%A1l%C3%B3i-szab%C3%A1lyzat)

3. A DUENET hálózat használata

(1) A hálózat nem használható az alábbi tevékenységekre, illetve az ilyen tevékenységekre irányuló kísérletekre:

a) Az érvényes magyar törvényekbe ütköző cselekmények, ideértve: a mások személyiségi jogainak megsértése; a tiltott haszonszerzésre irányuló tevékenység; a szerzői jogok megsértése; a szoftver termékek illegális terjesztése.

b) Más hálózatok közötti átmenő forgalom bonyolítása.

c) A DUENET hálózathoz kapcsolódó más - hazai vagy nemzetközi - hálózatok szabályaiba ütköző tevékenységek, amennyiben ezek a tevékenységek az adott hálózatokat érintik.

d) A DUENET hálózat szolgáltatásainak nem DUENET felhasználók számára való továbbítása, kivéve az érvényes kutatás-fejlesztési, vagy innovációs szerződéses kapcsolatot ezen szervezetekkel.

e) Profitszerzést célzó direkt üzleti célú tevékenység, reklámok terjesztése, intézményi nyilvános megjelenésű weboldalakon való megjelenítése.

f) A hálózat, illetve erőforrásai normális működését megzavaró, veszélyeztető tevékenység, ilyen információk, programok terjesztése.

g) A hálózatot, illetve erőforrásait indokolatlanul, vagy szándékosan túlzott mértékben, pazarló módon igénybevevő tevékenység (pl. levélbombák, vírusok terjesztése).

h) A hálózat erőforrásaihoz, a hálózaton elérhető adatokhoz történő illetéktelen hozzáférés, azok jogosulatlan használata, számítógépekhez, hálózat aktív eszközökhöz, szolgáltatásokhoz való hozzáférés szisztematikus próbálgatása, szolgáltatás felderítés (pl.: portscan).

i) A hálózat erőforrásainak, a hálózaton elérhető adatoknak illetéktelen módosítására, megrongálására, megsemmisítésére, eltulajdonítására irányuló tevékenység (hacking).

j) Másokra nézve sértő, mások vallási, etnikai, politikai, vagy más jellegű érzékenységét bántó, zaklató tevékenység (pl.: pornográfia, pedofil anyagok közzététele, az ilyen tartalmak böngészése).

k) Mások munkájának indokolatlan és túlzott mértékű zavarása, vagy akadályozása (pl.: kéretlen levelek - spam, hirdetések, lánclevelek), az ilyen tartalmak továbbítása.

l) A hálózati erőforrások magáncélra való túlzott mértékű használata.

m) A hálózati erőforrásoknak, szolgáltatásoknak az erőforrás/szolgáltatás eredeti céljától idegen használata (pl.: hírcsoportokba/levelezési listákra a csoport/lista témájába nem vágó üzenet küldése).

n) A hálózati üzenetek, hálózati eszközök címeinek hamisítása - olyan látszat keltése, mintha egy üzenet más gépről, vagy más felhasználótól származna (spoofing).

o) A DUENET hálózathoz való személyes hozzáférési adataik (felhasználói név, jelszó) más személy számára való átruházása.

4. A felhasználók jogai és kötelességei

a) Az intézmény a felhasználóknak alanyi jogon lehetővé teszi a hálózathoz való hozzáférést. Ehhez a felhasználó intézményi statusának megfelelő jogosultsági kategóriát megtestesítő felhasználói azonosítást biztosít.

b) Minden felhasználó rendelkezhet saját kizárólagos használatú elektronikus levélcímmel és az ezt biztosító központi email rendszerben postafiókkal, amelyet bárhonnan lehetősége van használni (levelei lekérdezése).

c) A felhasználók a központi címtárban nyilvántartott adataikat megismerhetik, a nyilvánosságra hozható adataik körét meghatározhatják. Az intézményi előírások szerint kötelező nyilvános adataikat aktuális állapotban kell tartaniuk. (Elsősorban oktatók elérési adatai, telefonszám, hivatali cím, email cím, stb.)

d) Nem az intézmény állományába tartozók (vendégek, egyéb jogosultak) hálózathasználatát a fogadó szervezeti egység kezdeményezi az ISZK-nál. Nagyobb szabású rendezvény, konferencia rendezése esetén a rendezvény szervezője igényli a résztvevők számára a hálózati hozzáférést az ISZK-nál.

e) Föderatív szolgáltatások igénybevételéhez (pl.: Eduroam) nem szükséges a DUENET hálózathoz való hozzáférési azonosítókkal rendelkezni.

f) A felhasználóknak joga van a hálózati szolgáltatások használatához szükséges alapismeretek megszerzéséhez.

g) A felhasználónak joga van megkövetelni a személyiségi jogok és a levéltitok tiszteletben tartását a hálózat üzemeltetői részéről.

h) A felhasználóknak joga van esetleges zaklatás ellenei védelem kérésére.

i) A felhasználónak joga van értesülni a tervezett vagy rendkívüli technikai problémákról a helyi korlátozásokról.

j) Az intézmény felhasználói az Internet és az intranet használata során tanúsított magatartásukkal feleljenek meg a hivatalosnak elfogadott Netikett (RFC 1855) előírásainak.

k) A felhasználók kötelesek oly módon használni a hálózatot, hogy magatartásukkal az intézmény hitelét, jó hírét és érdekeit ne sértsék.

5. A szabályzat betartatása, megsértésének szankcionálása

a) A felhasználók személyesen felelnek az általuk generált hálózati forgalomért. Az ISZK jogosult a hosszabb időn át fennálló indokolatlanul magasnak tartott forgalom vizsgálatára és a forgalmazó számítógép/felhasználó ellenőrzésére. A legnagyobb forgalmat generáló munkaállomások toplistáját az ISZK nyilvánosságra hozhatja. (Indokolatlan forgalmat generálhat egy vírusfertőzött, vagy hackertámadással feltört számítógép, akár a használó tudta nélkül is.)

b) A szabályzat szándékos és durva megsértésének szankcionálása a hálózati szolgáltatásokból való ideiglenes vagy végleges kizárás. Ha a szabályzat megsértése kismértékű, vagy nem tekinthető szándékosnak, akkor az elkövetőt figyelmeztetni, és a szabályzatról tájékoztatni kell. A figyelmeztetés

utáni ismételt elkövetést szándékosnak kell tekinteni. Szükség esetén az ISZK jogi felelősségre vonást kezdeményezhet, a kancellárnál.

c) A használati szabályok betartatására a hálózatfelügyelet figyel. E célból a hálózatbiztonság és megbízható működés érdekében technikai eszközöket, felügyeleti programokat helyezhet üzembe.

6. A felhasználókra és az egyes szolgáltatásokra vonatkozó további szabályok

a) Az ISZK saját hatáskörében az optimális és biztonságos üzemvitel érdekében a hálózat forgalmát szabályozó intézkedéseket vezethet be, melyek meghirdetésre kerülnek. Ezek betartása kötelező.

b) Az ISZK hálózatfelügyelet a nagyobb károkozás elkerülése végett az érintett hálózati rész (alhálózat) forgalmát korlátozhatja, vagy szüneteltetheti. A szabályokat megsértő személy címének ismeretében a megadott cím részleges vagy teljes szűrését is elvégezheti.

c) Az Interneten tapasztalható fenyegetettség mértékének csökkentése érdekében a DUENET a szolgáltatói hálózathoz tűzfalon keresztül csatlakozik. A tűzfal a szokásos és felhasználók számára leggyakoribb forgalmak szempontjából transzparens. Speciális felhasználói igényeket az ISZK-val kell egyeztetni, az ilyen forgalom engedélyezését az ISZK a hálózatbiztonsági és a rendelkezésre álló technika lehetőségek, szempontok figyelembe vételével engedélyezi, vagy elutasíthatja.

d) Az intézményi be- és kimenő levélforgalom, csak egy megbízható levelező átjárón keresztül bonyolódhat. A levelező átjárón vírus, spam, és a levélhez csatolt tartalomra vonatkozó speciális tartalomszűrés működik.

e) A hálózatfelügyelet nem gyűjt adatokat a felhasználók forgalmából, még mintavételesen és tesztelési célokra sem. A hálózatfelügyelet a hálózati eszközökön keletkezett forgalmi és log-adatok összesítése alapján készít forgalmi grafikonokat, von le következtetéseket.

f) A hálózatfelügyelet a rektor és/vagy a kancellár utasítására kizárólag hivatalos szervek által történt megkeresés alapján adhat ki információt a hálózati forgalom részleteiről a rendelkezésre álló technikai lehetőségek mértékéig.

g) Az ISZK alkalmazottait, büntetőjogi felelősségük köti abban, hogy az adatokhoz való hozzáférési jogosultságuk birtokában sem tekintenek bele sem az elektronikus levelek tartalmába, sem a felhasználók személyes adataiba.

h) Az ISZK a károkozás megelőzésére és a bekövetkezett károk következményeinek a felszámolására törekszik, de nem áll módjában felelősséget vállalni a szabályzat megsértéséből eredő esetleges károkért. A hálózat menedzsment a mindenkor rendelkezésre álló műszaki lehetőségeknek megfelelően törekszik arra, hogy a hálózaton áthaladó, illetve a hálózaton elérhető információkhoz, adatokhoz illetéktelenek ne férjenek hozzá. Amíg a műszaki lehetőségek ennek teljes garantálását nem biztosítják, a felhasználók ennek tudatában helyezzenek el vagy küldjenek információkat a hálózatban.

i) A hálózat használata közben tapasztalt rendellenességeket, incidensre utaló eseményeket az ISZK HelpDesk-nek kell bejelenteni. A HelpDesk az I-épület földszintjén az Informatikai Szolgáltató Központ hivatali helyiségében található. Bejelentő telefonszám munkaidőben a +36 25 551610. Az ISZK HelpDesk e-mail címe: iszk@uniduna.hu.

7. A szabályzat hatálya

Jelen szabályzat kihirdetésekor lép hatályba és visszavonásig érvényes.

2. sz. melléklet.

Üzemeltetési dokumentáció vázlata

1. Bevezetés
    1.1 Verzió, lezárás dátuma
2. A szolgáltatás alapfunkciója
    2.1. Alapvető szolgáltatások
    2.2. Kiegészítő szerverfunkciók és szolgáltatások
3. A rendszer architektúrája
    3.1 Külső és belső kapcsolatok
    3.2 Elhelyezés, hardver
4. Üzemeltetési feladatok
    4.1 Rendszeres üzemeltetési feladatok
    4.2 Eseti üzemeltetési feladat
    4.3 Jogosultság kezelés
5. Az üzemmenet felügyelete, eseménykezelés
    5.1 Szolgáltatási szint paraméterek és felügyeletük
    5.2 A szolgáltatás üzemképességi felügyeletének eszközei
        5.2.1 Felügyeleti eszközök
            5.2.1.1 A rendszer által küldött Email-ek
            5.2.1.2 Az alkalmazás saját felügyeleti eszköze
            5.2.1.3 A naplóállományok helye, megőrzési ideje
        5.2.2 Újraindítás, leállítás
        5.2.3 Incidenskezelés
        5.2.4 Biztonsági mentések
        5.2.5 Katasztrófa elhárítási terv
        5.2.6 Működés folytonossági terv
6. Az üzemeltetés személyi feltételei
    6.1 Az alkalmazás üzemeltetéséhez szükséges ismeretek
    6.2 Az alkalmazás használatához szükséges ismeretek
    6.3 Szakmai adminisztrátorok, felelősségi körök
    6.4 Támogató személyzet

3. sz. melléklet.

IIBSZ változáskezelési lap

Benyújtó adatai

Név:
Beosztás:
e-mail:
Telefon:

Benyújtás dátuma: :_____ benyújtó aláírása

Igényelt változtatás adatai

A változtatás indoklása:

Javasolt szövegváltozat:

Intézkedési szakasz

Beérkezés dátuma:_____ Iktatószám:_____ átvevő aláírása

Bírálói megjegyzések:

Határozat:

Indoklás:

Dátum: ……

aláírás

4. sz. melléklet.

”A” és ”B” biztonsági kategóriájú rendszerek incidens bejelentése

Bejelentő adatai

Név:
Beosztás:
e-mail:
Telefon:

Bejelentés dátuma: :_____ bejelentő aláírása

Incidens bejelentési szakasz

Észlelt incidens, esemény rövid leírása:

Egyéb azonosító adatok:

Csatolt mellékletek:

Intézkedési szakasz

Beérkezés dátuma:_____ Iktatószám:_____ átvevő aláírása

Vizsgálati megjegyzések:

Megtett Intézkedés:

Dátum: ……

aláírás

Fogalommagyarázat

Aldomain: egy regisztrált domain-en belül a regisztrációs eljárás delegálásával átadott jogkörben létrehozott, hierarchikusan a domain alá rendelt név.

DUE: Dunaújvárosi Egyetem.

DNS: Domain Name Service. Az internen használható neveket és címeket (IP-cím) egymáshoz rendelő adatbázisa.

Domain: A felhasználó szervezet által meghatározható emlékeztető név, technikai és használati okokból szükséges. Használhatósága hierarchikus regisztrációs folyamatot igényel. Magyarországi hatáskörű domain regisztrációját az Internet Szolgáltatók Tanácsa által felsorolt cégek végeznek.

Felhasználó: az informatikai infrastruktúrát használó személy, általában az intézmény munka-vállalója, hallgatója (intézmény polgárai), vagy az intézménnyel kapcsolatban álló külső személy, aki a rendelkezésére bocsátott informatikai infrastruktúrát használja.

Fizikai szerver: egy létező számítógép (eszköz), amely az informatikai alkalmazások szempontjából kiszolgáló/szerver funkciót lát el. Egy fizikai szerver több szerverfunkció ellátását is végezheti.

IIBSZ: Informatikai és informatikai biztonsági szabályzat

Incidens: A szolgáltatás szabályos működésétől eltérő esemény, mely fennakadást vagy minőségcsökkenést okoz vagy okozhat a szolgáltatásban.

Internet, net: a világméretű hálózat, amely számítógépet kapcsol össze. A DUE informatikai hálózata része az internetnek.

Intranet: az intézményi hálózaton létrehozott munkakörnyezet, amely részben lehet nyilvános, de jellemzően az intézmény polgárainak számára zárt hálózati környezetet biztosít, amely a szokásos internet használati eszközökkel érhető el.

IP-cím: Az interneten kommunikáló eszközök (nem csak számítógépek) egyedi azonosítására szolgáló jellemző adat. Az IP-címeket világméretű hierarchikus adminisztrációs rendszerben kezelik. A szervezetekhez a Domain adminisztrációs folyamat során kerülhet kisebb-nagyobb címtartomány, amelyből a szervezet saját adminisztrációs rendszerében oszt ki a kommunikációba bevont eszközöknek IP-címeket.

ISZK: Informatikai Szolgáltató Központ

ITIL: Information Technology Infrastructure Library – egy olyan nemzetközileg elfogadott keretrendszer (de facto szabvány), mely a magas szintű IT szolgáltatások nyújtását a „legjobb gyakorlatok gyűjteménye” elv mentén szabályozza. Az ITIL olyan üzleti (működési) folyamatokat ír le, melyek mind a minőségi mind a gazdaságos szolgáltatás elérését támogatják az informatika területén.

KIFÜ-NIIF (Kormányzati Informatikai Fejlesztési Ügynökség Nemzeti Információs Infrastruktúra Fejlesztési Program): országos hatáskörű állami felügyeletű szerv, amely a magyar felsőoktatás, kutatás és a közintézmények számára komplex adathálózati, tartalmi és internet szolgáltatást nyújt.

Kiszolgáló/Szerver: olyan számítógép, amely más számítógépek számára valamilyen szolgáltatást nyújt.

Licensz: egy szoftver termék felhasználását szabályozó szerződés. Számos megjelenési formája létezik. Jogilag tisztázott szoftver használatot a szoftver licenszének rendelkezésre állásával lehet bizonyítani.

Mail, email, e-mail: számítógépek segítségével továbbított elektronikus levél.

Mobil eszköz: olyan számítógép és/vagy kommunikációs eszköz, amely az intézmény informatikai infrastruktúráját használni képes (notebook/laptop, mobiltelefon, nyomtató, projektor, stb.)

MTBF (Mean Time Between Failures): A rendszer két egymást követő meghibásodása között eltelt átlagos idő. Jellemzi a rendszer megbízhatóságát.

NAT (Network Address Translation): olyan mechanizmus, amely az Interneten nem használható un. belső címekkel rendelkező számítógépek számára is biztosítja a teljes értékű internet használatot.

Notebook/laptop: hordozható számítógép.

PC: személyi számítógép, amely lehet asztali PC, amely egy meghatározott munkahelyen telepített, vagy mobil számítógép (notebook, laptop), amelyet használója rendszerint magával visz.

Probléma: A probléma egy állapot, mely gyakran több hasonló tünetet produkáló incidens alapján ismerhető fel. A probléma azonosítható lehet egyetlen jelentős incidens alapján is, mely valamilyen hibára utal, melynek oka nem ismert, de hatása jelentős.

Protokoll: a számítógépes rendszerek közötti kommunikáció módját leíró szabályok gyűjteménye.

Rendelkezésre állás: százalékban kifejezett viszonyszám, amely megmutatja azt, hogy egy meghatározott időszakban (hónap, év) üzemeltetésre előírt időnek hány százaléka a tényleges üzemszerű működés ideje. Az üzemeltetés a szerverek esetében folyamatos, így az előírt idő a naptári időnek felel meg – megadása óra/hó, vagy óra/év történik.

SLA (Service Level Agreement): Szolgáltatási szint megállapodás, egy olyan írásos megállapodás, mely két fél között - a szolgáltató és a szolgáltatás igénybevevője között jön létre. Ez az alapkoncepciója az IT szolgáltatások menedzselésének. Az SLA meghatározza a két fél között nyújtandó szolgáltatás pontos tartalmát és feltételeit.

Szoftver: a számítógépen használt programok és adatok.

TCP/IP: az internet működéséhez, eléréséhez szükséges protokoll.

Campus Licenc (Tisztaszoftver Program): a Microsoft Magyarország és a Hungarnet Egyesület által kötött szerződés, amely a felső- és közoktatásban meghatározott Microsoft szoftver termékek használatát legalizálja.

Tűzfal, web-proxy, proxy: az intézményi hálózat és az internet közötti forgalmat szabályzó és megfigyelő eszközök.

Virtuális szerver: fizikai szerverekkel azonos funkcionalitású, amely a rendelkezésre állási szint növelése érdekében manuálisan, vagy automatizáltan mozgatható a fizikai szerverek között.

VPN (Virtual Private Network (Virtuális magánhálózat)): Az intézményi adathálózat kiterjesztése az interneten keresztül úgy, hogy a belső adatbiztonság nem sérül, mert a nyilvános hálózatokon keresztül az adatok erős titkosítással közlekednek.

Web: az internetnek az elektronikus levelezés mellett az egyik leggyakrabban hasznát szolgáltatása.

WiFi: olyan szabványos vezeték-nélküli adatátviteli technika, amely szabad frekvenciatartományt használ és átviteli sebessége nagymértékben függ a rádióhullámok terjedési környezetétől (akadályok, távolság) és a felhasználók számától. A mobile eszközök nagy része rendelkezik ilyen kapcsolódási lehetőséggel.