DUNAÚJVÁROSI EGYETEM

INFORMATIKAI ÉS INFORMATIKAI BIZTONSÁGI SZABÁLYZAT

2025.
Dunaújváros

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

Hatályos: 2019. 05. 28. napjától

Dunaújvárosi Egyetem Szenátusa által 30-2021/2022. (2022.03.22.) sz. határozatával elfogadva

Hatályos: 2022. 03. 23. napjától

Dunaújvárosi Egyetem Szenátusa által 52-2021/2022. (2022.05.17.) sz. határozatával elfogadva és egységes szerkezetbe foglalva

Hatályos: 2022. 05. 18. napjától

Dunaújvárosi Egyetem Szenátusa által 49-2024/2025. (2025.03.27.) sz. határozatával elfogadva

Hatályos: 2025. 04. 01. napjától

TARTALOMJEGYZÉK

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. Jelen szabályzat a hazai és a nemzetközi szakmai ajánlások alapján készült, különös tekintettel az intézmény közfeladat ellátására, valamint a nemzetbiztonsági védelem alá eső szervek és létesítmények köréről szóló 2009/2015. (XII.29.) számú Kormányhatározatra.

(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. A szabályzat hatálya kiterjed továbbá az Információbiztonsági Felügyelőre (a továbbiakban IB Felügyelő) is, akinek jogállása a jelen szabályzat 6. és 10. §-ban kerül szabályozásra. Ha az intézmény harmadik félnek is lehetőséget biztosít ezen infrastruktúrája használatára, akkor harmadik félre nézve is kötelező a szabályzatban foglaltakat betartani.

(5) A DUE Szervezeti és Működési Szabályzatának I. kötetét képező Szervezeti és Működési Rend (a továbbiakban: SZMR) 25/B. § (3) bekezdése szerint a Pályázati Iroda ellátja az Egyetem informatikai szolgáltatásaival kapcsolatos megrendelői feladatokat, tekintettel arra, hogy a szolgáltatás külső partnerrel kötött szerződés alapján kerül biztosításra. Ennek okán, a jelen szabályzat 13. §-ban meghatározott rendszermérnök és a 14.§ szerinti rendszergazda feladatkör ellátását a mindenkori szerződéses partner biztosítja.

(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 a Pályázati Iroda irodavezetői 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) Alkalmazottak fegyelmi szabályzata

e) Beszerzési és közbeszerzési Rend

f) 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, 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 eszköznek 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 a Pályázati Iroda (PI) 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 a Pályázati Iroda látja el. A Pályázati Iroda felelős a szolgáltató egység és a szolgáltatás igénybevevője között a szolgáltatás tartalmának és egyéb paramétereinek egyeztetéséért, a megállapodás betartásának ellenőrzéséért.

(3) A Pályázati Iroda irodavezetője jogosult az egyes szolgáltatások IIBSZ megfelelőségének ellenőrzésére.

(4) Az IB Felügyelőt a fenntartó bízza meg.. Az IB Felügyelő jogosult betekinteni az informatikai rendszerekbe - a tanulmányi rendszert kivéve -, onnan adatokat, információkat kikérni indokolt esetben javaslatokat tenni.

(5) Az IB Felügyelő a 6.§ (4) bekezdésben megjelölt ellenőrzési jogosultságát csak a munkáltatói jogkör gyakorlójának az előzetes engedélyével végezheti, a rendeltetésszerű működéssel összefüggésben.

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 használatának 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 rektorának dokumentáltan bejelentette a szankció elrendelését kiváltó eseményt (incidens). A bejelentés felelőse a szolgáltatást nyújtó szervezeti egység vezetője. A Jogi Iroda vezetőjének hatáskörébe tartozik az incidens kivizsgálása és a szankcionálás szintjének megállapítása érdekében teendő intézkedés.

(5) Nem büntetőjogi kategóriába tartozó incidensek bejelentése a Pályázati Irodához történhet, akinek kötelessége az incidens kivizsgálása. A Pályázati Iroda irodavezetőjének 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 egyetem minden informatikai rendszerét (a 9.§ alapján) biztonsági kategóriába kell sorolni. Ezek alapján kerülnek kidolgozásra 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 hardver 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. A feladatkörök a 11.§ - 15.§-ig kerülnek kifejtésre.

(2) Az IB Felügyelő a fenntartó Alapítvány alkalmazásában álló személy, aki a munkáltatói jogkör gyakorlójának előzetes engedélyével jogosult az informatikai rendszerekbe - kivéve a tanulmányi rendszert- betekinteni, onnan adatokat, információkat kikérni indokolt esetben javaslatokat tenni.

11.§ Pályázati Iroda irodavezető

(1) Feladata:

Az egyetem informatikai-szolgáltatási koncepciójának képviselete, az intézmény informatikai rendszerei üzemeltetésének, működésének irányítása és ellenőrzése, továbbá a Pályázati Iroda ügyrendben rögzített feladatokkal rendelkező Pályázati Iroda vezetése.

(2) Felelőssége:

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

b) Az egyetem informatikai és információ biztonsági szabályzatának 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 hozzáférési jogosultságok megadásának és visszavonásának kezdeményezése.

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

c) 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.

(2) Feladata a Pályázati Iroda irodavezető 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) Biztonsági szempontból a főbb rendszermérnöki feladatok:

a) Szolgáltatási rendszerek alapkonfigurációjának kialakítása.

b) Kiadott programjavítások végrehajtása.

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

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

e) Email szolgáltatás meghatározása, ellenőrzés.

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

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

h) Üzemviteli körülmények meghatározásában való részvétel.

i) Virtualszerver-környezet létrehozása, rendszeradminisztrálása.

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

k) Hálózati konfigurációk kialakítása, tűzfalszabályok kialakítása és felügyelete.

l) Logok elemzése, következtetések levonása, javaslattétel.

m) Jelszó és egyéb biztonsági házirendek konfigurálása.

n) A konkrét személy 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 tevékenysége során napi rendszerességgel látja el a HelpDesk feladatot, beleértve az informatikai eszközök hardver és szoftver javítását telefonos segítséggel, vagy a felhasználó munkahelyén, komolyabb probléma esetén a Pályázati Irodába történő beszállítással. Szükség esetén külső szervizszolgáltatás megrendelésének kezdeményezését végzi. Emellett feladata az informatikai eszközök időszakos karbantartása, vásárolt számítógépek, nyomtatók, szkennerek, stb. üzembe helyezése a felhasználói munkahelyeken, vagy oktatási kabinetekben, oktatástechnológusi támogatás biztosítása a tantermekben és előadókban az oktatói / a rendezvény igénye szerint.

(2) További rendszergazdai feladatok: vásárolt számítógépek operációs rendszer telepítése, a belső biztonsági rendben meghatározott beállításai, jogtiszta felhasználói programok telepítése (pl. Office rendszer).

(3) Biztonsági szempontból a főbb feladata:

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

d) Operációs rendszer, vírusvédelmi rendszer alapvető alkalmazások (Office) javítása a felhasználói munkaállomásokon.

e) A konkrét személy 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.§ 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 Munkaügyi Iroda által történt regisztrációt és adatfelvételt követően; vendég felhasználó a fogadó szervezeti egység részéről a Pályázati Irodához 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 Munkaügyi Irodán kell kezdeményezni a változtatást, szoba vagy telefonmellék változása esetén pedig a Pályázati Irodának 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 a Pályázati Iroda számára.

(6) Felhasználó hatásköre:

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

16.§ 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 a Pályázati Iroda végzi, vagy – ahol a szervezeti egységnél erre rendelkezésre áll rendszergazda beosztású dolgozó – a Pályázati Irodával egyeztetve történik. A munkaállomásokat a 22.§ -ban leírtak szerint a Pályázati Iroda nyilvántartásában kell tartani. Nyilvántartásában nem szereplő munkaállomás hálózatra kapcsolását a Pályázati Iroda munkatársai megtilthatják.

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

(3) Az egyetemi tulajdonú munkaállomások telepítését (újra telepítését) és a megfelelő működéshez szükséges beállítások elvégzését csak a Pályázati Iroda munkatársai és az általa megbízott szakemberek végezhetik.

(4) Az egyetemi tulajdonú munkaállomásokon csak a Pályázati Iroda munkatársainak lehet adminisztrátori jogosultsága. Ettől eltérni csak indokolt esetben, a Pályázati Iroda irodavezető jóváhagyásával lehet.

(5) Az egyetemen használt, az egyetem tulajdonát képező munkaállomásokat rendeltetésszerűen, munkavégzés, oktatás, illetve tanulmányi kötelezettségek teljesítése 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 (a felsorolt célokhoz nem kapcsolódó magánanyagok tárolása) nem engedélyezett. Az intézményi informatikai eszközökön csak a munkavégzéssel, oktatással, illetve tanulmányi kötelezettségek teljesítésével szorosan összefüggő adatokat (állományokat) lehet tárolni.

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

(7) 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.

(8) 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.)

(9) Olyan munkaállomás, amely nem rendelkezik helyi (az eszközre telepített) vírusvédelmi szoftverrel, az intézményi hálózathoz nem csatlakoztatható. Az intézmény tulajdonában lévő munkaállomások részére az intézményi tulajdonú vírusvédelmi rendszert központi menedzsment alkalmazásával a Pályázati Iroda biztosítja. A kollégiumi szobákban működő hallgatói (saját tulajdonú) munkaállomások vírusvédelméről a hallgató (tulajdonos és /vagy felhasználó) köteles gondoskodni. Amennyiben a nem megfelelő vírusvédelemből az Intézménynek kára származik, úgy azért a hallgató anyagi felelősséggel tartozik.

(10) A vírusvédelmi előírás feltételeinek eleget nem tevő munkaállomás csatlakozását a Pályázati Iroda munkatársai megtilthatják.

(11) 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 a Pályázati Iroda hatáskörébe tartozik.

(12) Speciális oktató-kutató munkavégzéshez elengedhetetlen hardverbeépítés és csere esetén egyeztetni kell a Pályázati Irodával. A végrehajtott módosítást a Pályázati Iroda eszköznyilvántartásában is dokumentálni kell. A Pályázati Iroda 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. A Pályázati Iroda által nem támogatott hardverrel és/vagy szoftverrel rendelkező munkaállomások zárt hálózatba szervezését a Pályázati Iroda 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.

(13) 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 a Pályázati Irodához beadott igényléssel (papír vagy elektronikus úton).

e) Az igénylés pozitív elbírálása (szoftver feltételek, hardver feltételek és a licensz meglétének ellenőrzése) után a Pályázati Iroda (vagy a helyi rendszergazda) közreműködésével történik a telepítés. A telepítést a Pályázati Iroda 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 a Pályázati Irodával 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 munkaköri jogon engedélyezi otthoni munkavégzés céljából a nem minősített adatok kivitelét. Tilos minősített adatot bármilyen formában az intézményen kívülre juttatni.

(14) Munkaállomásokra a távoli bejelentkezés (távoli asztal - RDP) csak az intézményi hálózaton belül lévő munkaállomásról engedélyezett, az internetről közvetlenül nem. Belső munkaállomásnak minősül az Interneten bárhol elhelyezkedő a belső hálózathoz „virtuális privát hálózati” (VPN) kapcsolattal csatlakozott munkaállomás is.

17.§ Fokozott biztonságú munkaállomások

(1) Az egyetem olyan munkaállomásait, amelyek az alábbiak közül legalább egy pontnak megfelelnek, fokozott biztonsággal kell ellátni. Az érintett munkaállomások az alábbiak:

a) Felsővezetők, szervezeti egység vezetők munkaállomásai.

b) Az informatikai rendszereket és a számítógép hálózat felügyeletét ellátó munkaállomások.

c) Azon munkaállomások, amelyek kritikus („A” biztonsági kategóriájú) rendszerek közvetlen munkaállomásai.

d) Olyan munkaállomások, amelyek „minősített” adatot kezelnek.

(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 a Pályázati Iroda munkatársai, munkalapon (papír vagy elektronikus alapú) részletesen dokumentálva végezhetnek.

18.§ 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 egyetemi tulajdonú mobil munkaállomások telepítését (újra telepítését) és a megfelelő működéshez szükséges beállítások elvégzését csak a Pályázati Iroda munkatársai és az általa megbízott szakemberek végezhetik.

(3) Az egyetemi tulajdonú mobil munkaállomásokon csak az Pályázati Iroda munkatársainak lehet adminisztrátori jogosultsága. Ettől eltérni csak indokolt esetben, a Pályázati Iroda irodavezető jóváhagyásával lehet.

(4) A Pályázati Irodának 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.

(5) 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.

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

(7) Az intézményi vezeték nélküli hálózatra való csatlakozás feltételeit a beállítási dokumentáció tartalmazza (https://www.uniduna.hu/it-wifi-szolgaltatas).

(8) 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.

(9) Olyan mobil munkaállomás, amely nem rendelkezik helyi (a gépre telepített) naprakész vírusvédelmi szoftverrel, sem a vezetékes, sem a vezeték nélküli hálózathoz nem csatlakoztatható. A feltételnek eleget nem tevő munkaállomás csatlakoztatását a Pályázati Iroda munkatársai megtílthatják.

19.§ 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 16.§(13)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 figyelembevételével a Pályázati Iroda biztosítja.

(4) A felhasználó az adatmentés kivitelezéséhez a Pályázati Iroda segítségét igénybe veheti.

20.§ 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 16.§(8) bekezdésben felsorolt 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 a Pályázati Iroda 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) A Pályázati Iroda a felhasználók levelezési postafiókjainak méretét (mailbox), a rendszer által kezelt levelek méretét, technikai eszközökkel korlátozhatja a rendelkezésre álló központi erőforrások figyelembevételével.

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 a Pályázati Iroda 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.

21.§ 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 az intézmény beszerzési szabályzatában meghatározottakon túl tartalmazzák az alábbi részeket:

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

b) Támogatási és/vagy garanciális feltételek

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

d) A rendszer leszállításakor átadandó dokumentációk köre / jellege.

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

22.§ Informatikai eszközök beszerzése nyilvántartása és javítása

(1) A szoftverek és az informatikai hardverek beszerzése központi feladat, amely a Pályázati Iroda közreműködésével történik.

(2) Pályázatok írásakor, amennyiben az tartalmaz szoftvert és / vagy informatikai hardvert, a pályázat írója köteles bevonni a Pályázati Iroda irodavezetőt az érintett rész tervezési folyamatába. Olyan (szoftver és / vagy informatikai hardver beszerzését tartalmazó) pályázat nem nyújtható be, amelynek az érintett részét a Pályázati Iroda irodavezető nem hagyta jóvá.

(3) A szoftver és az informatikai hardver beszerzése csak a Pályázati Iroda irodavezető jóváhagyásával történhet meg.

(4) A beszerzés menetét az intézményi Beszerzési és közbeszerzési Rend határozza meg.

(5) Az informatikai eszközöknek a számviteli nyilvántartásokon kívüli kötelező műszaki nyilvántartása a Pályázati Iroda 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 Pályázati Iroda az eszköznyilvántartást elektronikusan kezeli. A megvásárolt eszközök üzembe helyezésével egy időben az elektronikus adatfelvétel a Pályázati Iroda feladata. A Pályázati Iroda csak a nyilvántartás rögzítését dokumentáló azonosító számmal ellátott eszközt támogat.

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

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

(8) 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).

(9) Az intézményi célra, vagy központi keretből beszerzett szoftverek nyilvántartását a Pályázati Iroda végzi. 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)

(10) A szervezeti egységek szoftvernyilvántartását a Pályázati Iroda számára hozzáférhetővé kell tenni.

(11) Informatikai eszköz meghibásodását a Pályázati Irodának be kell jelenteni. Bejelentés a https://ticket.net.uniduna.hu/ címen elérhető bejelentő rendszeren (ticketing) keresztül tehető meg. Ha a javítást a Pályázati Iroda saját hatáskörben nem tudja elvégezni, a szakszervizbe szállítást megszervezi. Garanciaidőn túli szervizben történő javíttatás esetén a Pályázati Irodának kötelessége előzetesen árajánlatot kérni. Az ajánlat alapján az egyetem dönt a javítás megrendeléséről vagy gazdaságtalan javítási feltételek esetén elállhat a javítás megrendelésétől.

23.§ 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 a Pályázati Iroda irodavezetője felelős.

(4) A domain névvel rendelkező szervezet az interneten nyilvánossá tett szolgáltatásihoz való hozzáférést a Pályázati Iroda 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 a Pályázati Iroda irodavezetőjéhez kell eljuttatni, aki a technikai és jogi feltételek vizsgálata alapján jóváhagyja vagy elutasítja a kérést.

24.§ Gazdálkodás az IP címekkel

(1) Az interneten való adatforgalmazáshoz 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 a Pályázati Iroda 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 a Pályázati Iroda kizárólagos hatásköre.

(7) Szervezeti egységek kizárólag a Pályázati Iroda 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 a Pályázati Iroda felé jelentésköteles.

25.§ 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) Felmondás 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 jogviszony megszüntetés 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 a Pályázati Iroda 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) és ezt a döntést jelzi a Pályázati Iroda felé.

(3) A 2. pontban leírt döntés és annak jelzésének hiányában a Pályázati Iroda az eszközt újra telepíti. A rajta lévő adatok törlésre kerülnek.

26.§ 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) Felmondás 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 jogviszony megszüntetés 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 a Pályázati Iroda segítségét a feladat informatikai támogatásában.

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

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

e) A postafiók ezután törlésre kerül.

(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 a Pályázati Iroda irodavezetőjének. A levél beérkezését és iktatását követően a Pályázati Iroda irodavezető gondoskodik az email-cím törléséről.

III. SZOLGÁLTATÁSSZINT MENEDZSMENT

27.§ Informatikai szolgáltatás menedzsment

(1) Szolgáltatások tervezése

a) Az üzemelő informatikai rendszereket szolgáltatásként kell kezelni. A felhasználói, üzleti igények megfogalmazását követően a szolgáltatástervezés folyamatai nyújtanak iránymutatást az egyes rendszerek kialakításának tervezési-fejlesztési teendőihez.

b) A szolgáltatás kialakítását célszerű projektként kezelni és projektmenedzsment eszközök és technikák alkalmazásával megvalósítani.

c) A szolgáltatások tervezése során figyelembe kell venni, hogy fontos szempont a szolgáltatás működtetésének átláthatósága és kiszámíthatósága.

(2) Szolgáltatások bevezetése

a) A szolgáltatás tervezését követő fejlesztés után a szolgáltatás használatba vétele (pl. az informatikai rendszer éles üzembe helyezése következik. Ennek lépéseit a változáskezelési folyamat írja le.

b) A már működő, üzembe helyezett szolgáltatások „életében” bizonyos időszakonként változásokat kell végrehajtani. Ezek a változások származhatnak a szolgáltatás funkcionalitásának módosítási igényéből, jogszabályi változásokból, biztonsági hiányosságok korrigálásából stb. A feladatokat a változáskezelési folyamat szerint kell elvégezni.

c) Az egyes rendszerelemek jellemzőit és adatait a konfigurációs adatbázisban kell tárolni, és gondoskodni kell róla, hogy az eszköz üzembe helyezésekor, módosításakor stb. a konfigurációkezelési folyamat lépései kerüljenek végrehajtásra.

(3) Szolgáltatások üzemeltetése

a) A működő rendszereket (szolgáltatásokat) felügyelni, monitorozni kell, amelyet az eseménykezelési folyamat szerint kell végezni. Amennyiben a szolgáltatások üzemeltetése során olyan események lépnek fel, amelyek részlegesen, vagy teljesen elérhetetlenné teszik a szolgáltatást a felhasználók számára, akkor az incidenskezelési folyamat szerint kell eljárni, és mielőbb visszaállítani a szolgáltatás működőképességét.

b) Az egyes üzleti alkalmazásoknál biztosítani kell, hogy mindenki hozzáférjen a feladatai ellátásához szükséges információkhoz. Ennek kontrollált megvalósítását a hozzáféréskezelési folyamaton keresztül lehet biztosítani.

28.§ Szolgáltatástervezés

(1) A szolgáltatástervezés során az igénylő által megfogalmazott elvárások alapján meg kell határozni, hogy milyen elérhetőségi, rendelkezésre állási kritériumoknak kell majd megfelelni. Ebbe beleértjük a szolgáltatás elérhetőségére vonatkozó rendelkezésre állási mutatókat is. A rendelkezésre állás mértékét jellemzően %-ban szokták meghatározni.

Ebben az esetben a tényleges elérhetőségi idő és az adott időszakra vonatkozó teljes időtartam hányadosa alapján képezhető ez az érték.

(2) A szolgáltatási szintre vonatkozóan az ügyfél (igénylő) és a szolgáltató (IT szervezet) között megállapodás kell, hogy létrejöjjön: ezt nevezzük SLA-nak (Service Level Agreement) azaz „szolgáltatási szint megállapodásnak.

(3) A szolgáltatási szinttel kapcsolatos megállapodás során rögzíteni kell, hogy milyen időszakra vonatkoztatva kerül megállapításra ez az érték. A leggyakrabban a havi szinten történő SLA meghatározást alkalmazzák, de esetenként előfordulhat, hogy a megállapodás eredményeként valamely szolgáltatási szintet éves időszakra vonatkoztatva állapítják meg.

(4) Az SLA rögzítésekor, tisztázni kell, hogy mi az az időtartomány, amikor biztosítani kell a szolgáltatás elérhetőségét (mely napokon, mettől-meddig). Az adott időszakra vonatkozó tényleges rendelkezésre állás meghatározásánál csak ezt az időszakot kell alapul venni. A Szolgáltatási megállapodás szempontjából a megállapodásban meghatározott időszakon kívül bekövetkező kiesés nem minősül SLA sértésnek, vagyis a rendelkezésre állási mutató meghatározásakor nem kell figyelembe venni.

(5) A szolgáltatások minőségi mutatóinál a rendelkezésre állás mellett gyakran használják azokat, amelyek az egyes szolgáltatások kiesése esetén a szolgáltatás kiesés megszűntetésének időtartamára (hibaelhárítási idő), vagy a hibaelhárítás megkezdésére (reakció idő) vonatkoznak. Egy adott szolgáltatás esetében akár több minőségi mutatót is szoktak alkalmazni (pl. rendelkezésre állás, hibaelhárítási idő) a Szolgáltatási szint megállapodásban.

29.§ A Szolgáltatás architektúrájának tervezése

(1) A szolgáltatás minőségi jellemzőinek egyeztetését követően a következő lépésben a szolgáltatás architektúrájának megtervezése történik. Itt az elvárt rendelkezésre állási értékek és egyéb minőségi jellemzők figyelembevételével kell meghatározni a szolgáltatás nyújtásához szükséges technológiai architektúrát.

30.§ Kapacitástervezés

(1) A szolgáltatás tervezésekor, az igénylővel együttműködve fel kell mérni, hogy az adott szolgáltatást milyen mennyiségben kell nyújtani a jelenben és a jövőben. Mivel az információtechnológiai eszközök technológiai elavulásának jellemző ideje 3-4 év, a kapacitások tervezésekor is ilyen időtávra kell elkészíteni a terveket.

(2) Az informatikai szolgáltatásokért felelős személy fel kell, hogy mérje, hogy vállalati szinten várhatóan hogyan fog változni az adott szolgáltatásra vonatkozó igény volumene.

(3) A szolgáltatás nyújtásához kapcsolódó technológia tervezésekor figyelembe kell venni az induláskor szükséges kapacitásokat és a várható növekedési, azaz bővítési igényeket. Pl. adattárolási igények növekedése, feldolgozó (számítási) kapacitás növekedése, adatátviteli sebesség (sávszélesség) növekedése stb.

(4) A kapacitások tervezésekor, az igénylő üzleti területekkel tisztázni kell, hogy a szolgáltatás igénybevétele „egyenletesen” történik, vagy vannak-e olyan időszakok,

kiugró mértékű terhelésre kell felkészülni. A szolgáltatás nyújtásához szükséges technológiai komponensek, illetve az architektúra tervezésekor ezeket a „csúcsokat” figyelembe kell venni.

31.§ Rendelkezésre állás tervezése

(1) A szolgáltatás nyújtásához szükséges technológiai architektúra tervezésénél figyelembe kell venni az igénylő üzleti területek által megfogalmazott rendelkezésre állási, elérhetőségi elvárásokat.

(2) A rendelkezésre állás tervezésekor figyelembe kell venni, hogy az üzleti oldal által megfogalmazott rendelkezésre állás több tényezőtől függ. Gyakori, hogy egy-egy szolgáltatás elérhetősége több szolgáltatáskomponens, vagy támogató szolgáltatás elérhetőségének függvénye. Pl. Ha egy adott szolgáltatás 3 szolgáltatási komponensből épül fel, amelyek garantált rendelkezésre állási értéke 99%, 99% ill. 98%, akkor az ezekből összeállított szolgáltatás garantált rendelkezésre állási mutatója 0,99x0,99x0,98=0,9605, azaz a szolgáltatás garantált rendelkezésre állási ideje 96,05% lesz. Ettől természetesen eltérhet a rendelkezésre állás mért értéke.

(3) Amikor a szolgáltatásrendelkezésre állására vonatkozóan megfogalmazásra kerülnek az üzleti igények, azt is vizsgálni kell, hogy az adott szolgáltatás biztosításához szükséges-e külső támogató szolgáltatást igénybe venni valamely beszállító partnertől, vagy nem. Ha igen, akkor a beszállítóval kötendő szerződésnél figyelembe kell venni az elvárt rendelkezésre állási, hibaelhárítási, vagy reakció időket. Amennyiben ez valamilyen okból nem lehetséges (pl.: DKÜ), úgy a rendelkezésre állást a szerződében foglaltak figyelembevételével módosítani szükséges.

32.§ Szolgáltatás pénzügyi tervezése

(1) A szolgáltatások tervezésekor fel kell mérni, a szolgáltatások elvárt szintű nyújtásához kapcsolódó költségeket. A szolgáltatás pénzügyi hátterének tervezésekor első lépésként tisztázni kell, hogy ki viseli a szolgáltatáshoz kapcsolódó költségeket. Ez az intézmény működési stratégiájának függvénye. A szolgáltatás ráfordításainak és a kialakított szolgáltatás kapacitásainak (elérhető volumenek, mennyiségek) figyelembevételével lehet meghatározni a szolgáltatás ellenértékét.

(2) A ráfordítások tervezésekor jellemzően az alábbi költségelemeket szükséges figyelembe venni:

a) A szolgáltatáshoz kapcsolódó szoftver licenckköltségek,

b) szoftvertámogatási költségek (pl. terméktámogatás, verziókövetés, jogszabálykövetés stb.),

c) hardver költségek,

d) hardverek szerviz, ill. karbantartási költségei,

e) a szolgáltatás működtetéséhez szükséges emberi erőforrások költségei,

f) egyéb háttér- vagy támogató szolgáltatások költségei.

(3) A szolgáltatások árának kalkulálását követően az igénylő üzleti terület képviselőjével, vagy a szolgáltatások költségeinek „viselőjével” kell egyeztetni azok mértékéről. Az egyeztetés célja, hogy a szolgáltatás nyújtása mindegyik fél által elfogadott áron történjen. Amennyiben a szolgáltatás kalkulált díja nem elfogadható a költségek viselőjének, akkor meg kell határozni, hogy a szolgáltatás mely jellemzőjét (pl. elvárt rendelkezésre állás, vagy elvárt hibaelhárítási idő, stb.) célszerű módosítani.

(4) Ezt követően a szolgáltatástervezési folyamatot addig érdemes ismételni, amíg megállapodás nem születik a felek között az árak elfogadásáról.

33.§ Szolgáltatás tesztelése

(1) A szolgáltatástervezést követő implementálás befejeztével tesztelni kell a szolgáltatásokat. A tesztelésben részt kell vennie a szolgáltatást igénylő szervezet képviselőjének. A tesztelés során a szolgáltatás funkcionális megfelelősége mellett tesztelni kell a szolgáltatás minőségi jellemzőit is.

34.§ Szolgáltatás élesbe állítása

(1) Egy új szolgáltatás élesbe állításakor, vagyis a bevezetésekor a változáskezelési folyamat szerint kell eljárni.

35.§ A szolgáltatásszint menedzsment folyamata

(1) „A” és „B” biztonsági kategóriájú rendszer csak a Pályázati Iroda által üzemeltethető. Indokolt esetben (a Pályázati Irodával együttműködve) más szervezeti egység dolgozói is bevonhatóak az üzemeltetésbe.

(2) „C” biztonsági kategóriájú rendszer csak a Pályázati Iroda 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 a Pályázati Iroda irodavezetője dönt. Elutasító döntés esetén a javaslattevő 15 napon belül panasszal élhet az intézmény rektoránál. Ilyen esetekben a rektor ad-hoc bizottságot hív össze, amely vizsgálatot végez és javaslatot tesz az intézmény rektorának a kérdéses szolgáltatás indíthatóságáról. A bizottság állandó tagja a Pályázati Iroda irodavezetője. Végleges döntés meghozatala a rektor hatásköre.

36.§ 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 a Pályázati Iroda 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) Szolgáltatási szint mutató

- 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.)

37.§ 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 a Pályázati Iroda 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

38.§ Központi ügyfélszolgálat (Help Desk)

(1) Központi ügyfélszolgálatot a Pályázati Iroda 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 Pályázati Iroda üzemetetés alatt álló rendszerekre beérkező hibajelzéseket a Pályázati Iroda továbbítja a rendszer üzemeltetőjének.

39.§ Incidens észlelése

(1) Felhasználói észlelés esetén, amennyiben a felhasználó nem tervezetten az informatikai rendszer normálistól eltérő működését tapasztalja, be kell jelentenie a Pályázati Iroda ügyfélszolgálatán:

a) az ügyfélszolgálat által biztosított webes portálon (https://ticket.net.uniduna.hu/).

b) Amennyiben az (a.) pontban leírt mód nem elérhető, úgy e-mailben.

c) Amennyiben az (a. és b.) pontban leírt módok nem elérhetőek, úgy telefonon.

(2) Üzemeltetői észlelés esetén, amennyiben a Pályázati Iroda informatikai üzemeltetéssel foglalkozó munkatársa az informatikai rendszer normálistól eltérő működését tapasztalja, akkor az incidenst rögzítenie kell az ügyfélszolgálat informatikai alkalmazásában, hibajegyet kell nyitnia.

40.§ Incidens rögzítése

(1) Alapelvek:

a) Az incidensek elhárításának nyomon követése érdekében biztosítani kell azok dokumentálását, mely dokumentumban minden olyan adatot rögzíteni kell, ami az incidens kivizsgálásához, megoldásához és a felhasználó értesítéséhez és az incidens későbbi visszakereséséhez szükséges.

b) Amennyiben az incidens észlelése felhasználói bejelentés útján történt, olyan technikai megoldást kell alkalmazni és olyan módon kell dokumentálni, hogy az támogassa az incidens lezárása után a felhasználó értesítését. Ennek érdekében a

felhasználó köteles az észlelt incidenst az ügyfélszolgálat által biztosított webes portálon (https://ticket.net.uniduna.hu/) bejelenteni.

c) Amennyiben az incidenst észlelő felhasználó technikai okokból nem tudja a bejelentést a (b.) pontban meghatározott módon elvégezni, úgy az incidens egyéb módon /39.§(1)/ történő bejelentése után az ügyfélszolgálat munkatársának kötelessége a legrövidebb időn belül rögzíteni a Pályázati Iroda által használt bejelentő (ticketing) alkalmazásban.

(2) Incidens rögzítése során minimálisan az alábbi információk kerülnek az adott incidens hibajegyére:

a) az incidens egyedi azonosítója,

b) a bejelentő neve,

c) a bejelentő elérhetősége, egyéb elérhető információ- szervezet, intézmény,

d) a bejelentés időpontja,

e) az incidens típusa,

f) az érintett szolgáltatás neve,

g) az incidens részletes leírása,

h) egyéb, az érintett konfigurációs elemhez kötődő műszaki információ.

(3) Amennyiben az incidens megfelelő rögzítéséhez nem áll rendelkezésre elegendő információ, úgy az ügyfélszolgálati munkatárs feladata, hogy a felhasználóktól irányított kérdésekkel megszerezzen az incidens rögzítéséhez szükséges minden adatot.

41.§ Incidens priorizálása

(1) Az incidenseket olyan módon kell priorizálni, hogy az segítse a megoldási folyamatot. Az priorizálásnak kiemelt szerepe van abban, hogy az IT szolgáltató szervezet teljesíteni tudja a rendelkezésre állási elvárásokat.

(2) Az incidens priorizálásának az alábbi szempontokat kell figyelembe venni súlyozott, előre meghatározott módon,

a) a szolgáltatási szint megállapodásban (SLA) rögzített állás idők,

b) az incidens becsült hatása,

c) hány felhasználót érint az incidens,

d) incidens, szolgáltatásra gyakorolt hatását,

e) hány szolgáltatást érint az incidens,

f) időszak kritikussága (a mennyiben a szolgáltatás szempontjából jelentősége van).

(3) Amennyiben a fenti információkat a bejelentés pillanatában nem lehet megadni, akkor legkésőbb az incidens lezárása előtt mindenképp szükséges ezeket megadni.

42.§ Incidens vizsgálata

(1) Az incidens megoldása során az alábbi feladatokat kell az elsőszintű támogató (HelpDesk) munkatársaknak elvégezni:

a) elhárítani a hibát/megkerülő megoldást alkalmazni,

b) meghatározni a hiba okát,

c) meghatározni az események időbeliségét, az okozatot,

d) hasonlóságot keresni az adott incidens és a korábbi incidensek, problémák és ismert hibák között.

(2) A másodszintű támogató munkatársak (rendszergazda, rendszermérnök, alkalmazásgazda) az alábbi lépéseket teszik meg a hiba felmérésekor (kivizsgálás és diagnosztizálás):

a) meghatározni, hogy mi történt/mi romlott el,

b) meghatározni az események időbeliségét,

c) meghatározni, hogy mely esemény(ek) idézhették elő az incidenst,

d) megerősíteni az érintett felhasználók számát,

e) hasonlóságot keresni az adott incidens és a korábbi incidensek, problémák és ismert hibák között,

f) tudásbázis építés.

43.§ Az incidens megoldása

(1) Alapelvek:

a) Az incidenseket a lehető legrövidebb időn belül meg kell megoldani.

b) Az incidens elhárítása, a rendszer helyreállításáig, vagy a zavartalan működést biztosító áthidaló megoldás biztosításáig, a hiba végleges lezárásáig tart.

c) Az incidens megoldásával kapcsolatos felelősség a feladat átszignálásával az adott szervezeti egységhez vándorol, amelyre a feladatot kiszignálták.

d) Minden, az incidens megoldásával kapcsolatos információt rögzíteni kell az Ügyfélszolgálati alkalmazásban (ticketing rendszer).

e) Minden feladat megoldási ideje a regisztrálás időpontjától a készre jelentés időpontjáig tart.

(2) A feladatot megoldó munkatárs felelőssége, hogy

a) a hibajegyet a feladat megoldását követően azonnal lezárja,

b) helytelen vagy téves hiba/igény felvitel esetén a jegyet lezárja és a helyes feladattal az új hibajegyet megnyissa.

44.§ Lezárás

(1) Az adott incidens lezárásnál az alábbi lépéseket kell elvégezni:

a) Meg kell győződnie arról, hogy az incidens teljes mértékben megoldódott és hogy az ügyfél elégedett a nyújtott megoldással és egyetért az incidens lezárásával.

b) Ellenőriznie kell, hogy az incidens dokumentálása az előírásoknak megfelelően történt és teljes körű.

c) Le kell zárnia a kategorizálást, mely során ellenőriznie kell, hogy a kezdeti kategóriába sorolás megfelelő volt-e.

d) Formálisan le kell zárni az incidens dokumentációját (készre kell jelenteni).

e) Értesíteni kell a bejelentőt az incidens elhárultáról és megoldásról.

Fontos, hogy az ügyfélszolgálati alkalmazásban rögzített megoldási idő tükrözze a valós megoldási időket.

V. KONFIGURÁCIÓKEZELÉS

45.§ Alapelvek és terminológia

(1) Az működési folyamatok és az informatikai szolgáltatások folyamatos fejlődésével az IT infrastruktúra is folyamatosan változik. A változások követéséhez elengedhetetlenül fontos az IT infrastruktúra elemeinek és az azokra épülő szolgáltatások egységes nyilvántartása és nyomon követése.

(2) A konfigurációkezelés biztosítani tudja, hogy az IT infrastruktúra éles üzemi környezetébe csak jóváhagyott elemek kerülhessenek be, megfelelő módon dokumentálva. Továbbá naprakész információkat biztosít a szolgáltatások nyújtásához szükséges infrastruktúráról és a struktúrában található logikai elemek kapcsolatairól. Ezáltal a konfigurációkezelés támogatni tudja az incidens-, és változáskezelési folyamatokat.

(3) A konfigurációmenedzsment célja,

a) az elemek beazonosítása,

b) az életciklusban bekövetkezett változások nyomon követése,

c) a szolgáltatások, hardver, szoftver konfigurációk, dokumentációk bekerülése az egységes nyilvántartásba.

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

46.§ 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.

47.§ A hiteles szoftver tár

(1) A Pályázati Iroda 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.

48.§ 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, a Pályázati Iroda végzi a licencek tárolását és a kiadás elbírálását (kiadható, telepíthető).

(2) Az elbírálás és technikai kiadás munkáját a Pályázati Iroda irodavezetője termékenként más munkatársakra is átruházhatja.

VI. VÁLTOZÁSKEZELÉS

49.§ A folyamat meghatározása, alkalmazási területe

(1) E folyamat célja, hogy a szervezet képes legyen az informatikai szolgáltatásokat érintő folyamatos változtatások egységes kezelésére úgy, hogy közben a lehető legalacsonyabb szinten tartsa az ezekkel kapcsolatban felmerülő költségeket, az incidensek előfordulásának valószínűségét, és biztosítsa a szolgáltatások zavartalanságát és optimalizálja a változtatásokkal járó kockázatokat. Valamint biztosítva legyen, hogy a változások az előírtaknak megfelelően:

a) nyilvántartásba lettek véve,

b) megvizsgáltak,

c) jóváhagyottak,

d) prioritást rendeltek hozzá,

e) tervezettek,

f) teszteltek,

g) megvalósítottak,

h) dokumentáltak,

i) később értékeltek.

(2) Változásnak nevezzük azokat az eseményeket, amelyek az informatikai rendszerek (beleértve az informatikai IT szolgáltatásokat vagy a szolgáltatások működtetésében érintett konfigurációs elemeket) konfigurációjában módosítást eredményeznek.

50.§ Szerepkörök, felelősségek

(1) A változáskezelési folyamatban alkalmazandó szerepkörök az alábbiak:

a) Változás bejelentő az a személy, aki a változást kezdeményezi.

b) Változásmenedzser az a személy, aki az egész változáskezelési folyamatot menedzseli, változtatási kérelmeket összefogja és felügyeli azok végrehajtását.

Feladatai:

- Változáskérelem átvétele, naplózása, kezdeményezővel meghatározni a fontosságát.
- napirendre javasolni a változáskezelési bizottség (CAB) valamelyik ülésére,
- CAB tagoknak megküldeni a kérelmet, napirendet jóval az ülés előtt,
- elnököl az összes CAB ülésen,
- tanács által mérlegelt változtatások végrehajttatása,
- változtatási ütemterv kibocsátása,
- kapcsolattartás minden érintett résztvevővel,

- megvalósult változtatások felülvizsgálata, hogy elérték-e a céljukat,
- változáskérelmek lezárása,
- rendszeres vezetői jelentések készítése

c) Változásgazda olyan szakember vagy szervezet, aki jól ismeri az adott területet mind folyamat-, mind alkalmazás szempontból. Részt vesz a változtatási kérelem felülvizsgálatában és felmérésében, aki az adott változás végrehajtásáért felel.

d) Változáskezelési Bizottság (CAB (Change Advisory Board)): Az érintett területi vezető és az érintett rendszer(ek) üzemeltetéséért felelős személyek bevonásával létrejövő ad-hoc bizottság. A bizottság feladata a változtatások jóváhagyásának, engedélyezésének támogatása, valamint segít a változások felmérésében, rangsorolásában és döntést hoz. Az egyeztetés és a jóváhagyás történhet elektronikus formában is. A Pályázati Iroda irodavezető a bizottság állandó tagja.

(2) Felelősség és hatáskör mátrix

a) STANDARD változtatás eljárás

Fő tevékenységek	**Változás bejelentő**	**Változásmenedzser**	**Változásgazda**	**CAB**
Változáskérelmek fogadása	E,Tk	D, T		
Változáskérelem besorolása		V		
Változás végrehajtása	E	D, Tk	V,T	
Változtatás lezárása	Tk	D, T		

D: dönt; V: végrehajt; E: együttműködik; T: tájékoztat; Tk: tájékoztatást kap

b) SÜRGŐS változtatás eljárás

Fő tevékenységek	**Változás bejelentő**	**Változásmenedzser**	**Változásgazda**	**CAB**
Változáskérelmek fogadása	E,Tk	D, T		
Változáskérelem besorolása		V		
Változtatás kiértékelése		E	E	
Változás végrehajtása	Tk, E	Tk	V	
Változtatás lezárása	Tk	Tk,V	T	

D: dönt; V: végrehajt; E: együttműködik; T: tájékoztat; Tk: tájékoztatást kap

c) NORMÁL változtatás eljárás

Fő tevékenységek	Változás bejelentő	Változásmenedzser	Változásgazda	CAB
Változáskérelmek fogadása	E,Tk	D, T		
Változáskérelem besorolása		V		
Változáskérelem felülvizsgálata és felmérése	Tk	V,T	E	
Változtatás kiértékelése	Tk	E	E	V, D,T
Változtatás tervezése	Tk	V,T	V	Tk
Változás végrehajtása	Tk, E	Tk	V,T	Tk
Változtatás lezárása	Tk	Tk,V	T	Tk

D: dönt; V: végrehajt; E: együttműködik; T: tájékoztat; Tk: tájékoztatást kap

51.§ A változáskezelés folyamata

(1) Ahhoz, hogy a folyamatos változtatások kezelését eredményesen és hatékonyan tudja a szervezet végezni, az alábbiakban ismertetett tevékenységeket kell elvégezni, illetve jelen dokumentumban meghatározott módon (ticketing rendszer) dokumentálni.

(2) Változáskérelmek fogadása

a) Az informatikai szolgáltatások nyújtása során fogadni kell az informatikai eszközökkel, az informatikai alkalmazásokkal kapcsolatos változtatási kérelmeket.

b) A változtatási kérelmet az adott informatikai rendszer kulcsfelhasználója, az alkalmazás gazdája vagy az adott rendszer üzemeltetéséért felelős személy nyújthat be. A beérkezett változtatáskérelmeket előre meghatározott és a visszakereshető módon dokumentálni kell. A változtatáskérelmek naplózása során javasolt rögzíteni a következőket:

- a kérelem egyedi azonosítóját,
- a kérelmezés beérkezésének időpontját,
- kérelem tárgya,
- kérelem bejelentője.

c) A változáskérelem benyújtását az ügyfélszolgálati rendszerben kell rögzíteni.

(3) Változáskérelem besorolása

a) A beérkezett változási kérelmet a változásmenedzser besorolja, aszerint, hogy milyen változási eljárás vonatkozik rá továbbá milyen kockázatot jelent.

b) Változtatási eljárások az alábbiak:

- Sürgősségi változtatási eljárás.

- Standard változtatási eljárás.
- Normál változtatási eljárás.

c) Sürgősségi változtatási eljárásba soroljuk azokat a változtatásokat, amelyek olyan hibák kijavítására irányulnak, amelyek veszélyeztetik az informatikai szolgáltatást, és amely változtatásokat ezért a lehető leghamarabb végre kell hajtani, sürgősségi változtatás eljárás keretében kell megvalósítani. A sürgősségi változtatás eljárás keretében az alábbi tevékenységeket kell elvégezni:

- Az érintettek tájékoztatása.
- A sürgősségi változtatás végrehajtása.
- A sürgősségi tesztek elvégzése.
- A sürgősségi változtatás bevezetése és dokumentálása.

Javasolt a sürgősségi változtatások számát a minimumon tartani.

d) Standard változtatási eljárás keretében kell megvalósítani azokat a változtatási kérelmeket

- amelyek gyakran és előreláthatóan jelentkeznek (pl.: standard javítócsomagok, patch-ek),
- ahol a kockázat jól körül határolt és alacsony,
- ahol az elvégzendő tevékenységek előre meghatározhatóak,
- ahol a változás, a rendszer egésze szempontjából jól definiálható.

Ezen eljárás elindítására, a CAB tehermentesítése érdekében, elégséges a változásmenedzser jóváhagyása.

e) Normál változtatási eljárást kell alkalmazni azoknak a változtatásoknak a kezelésére, amelyek egyediek, a standard és sürgősségi változtatás eljárás egyikébe sem sorolhatók.

(4) Változáskérelem felülvizsgálata és felmérése

a) A beérkezett változáskérelem a változásmenedzserhez kerül, aki azt felülvizsgálja annak érdekében, hogy kiszűrhetők legyenek az alábbiak:

- teljesíthetetlen kérelmek,
- azok a kérelmek, amiket korábban már elfogadtak, elutasítottak vagy még vizsgálnak,
- azok a kérelmek, amiket tartalmilag hiányosan nyújtottak be.

b) Amennyiben a változásmenedzser úgy dönt, hogy a változás nem végrehajtható, a kérelem elutasításáról a változás kezdeményezőjét értesíti; az értesítésben szerepelnie kell az elutasítás okának. Lehetőséget kell biztosítani arra, hogy a változás kezdeményezője kezdeményezhesse az elutasítás felülvizsgálatát részletes indoklással a változásmenedzser felé, aki köteles erről a CAB-ot tájékoztatni. A felülvizsgálati kérelmet a CAB bírálja el.

c) Amennyiben a változásmenedzser, a változásgazdával együtt úgy dönt a beérkezett változáskérelemről, hogy beterjeszthető a CAB elé, elkészíti a döntéselőkészítő anyagot a szükséges szakterületek bevonásával. A döntés előkészítő anyagnak legalább a következő kérdéseket kell vizsgálnia:

- Mi az oka a változtatás kezdeményezésének?
- Mik a várható hatásai a változtatásnak?
- Mik az előnyei a változtatásnak?
- Mik a kockázatai a változtatásnak, vagy elmaradásának?
- Mennyire sürgős a változtatás?
- Milyen erőforrások szükségesek a változtatáshoz?
- Sikertelenség esetén milyen javító/visszaállító intézkedések lehetségesek?
- Mi az összefüggés az adott változtatás és a többi folyamatban lévő, jóváhagyás alatt álló változtatás között?
- A változtatás hatását szolgáltatás(ok)ra, és kapcsolódó rendszerelemeire.
- A változtatás hatását a szolgáltatást támogató infrastruktúrára.
- A változtatás hatását a felhasználókra.

d) Standard változtatási eljárás esetén a c) pontban leírtak a Pályázati Iroda irodavezető jóváhagyásával elhagyhatóak.

(5) A változtatás kiértékelése

a) A változtatás megvalósításáról való döntés meghozatala érdekében a változtatásokat ki kell értékelni.

b) A változtatások kiértékelésére változáskezelési bizottságot kell felállítani.

c) A bizottságban legalább az alábbi személyeknek kell szerepelnie:

- változásmenedzser,
- változásgazda (alkalmazástámogatás),
- a változással érintett területek képviselői,
- infrastruktúra üzemeltetéséért felelős vezető (amennyiben a változásban érintett),
- IT biztonságért felelős vezető (amennyiben biztonsági vonzata is van a változásnak),
- pénzügyi vezető (amennyiben a változtatásnak pénzügyi vonzata is van).

d) A változtatás kiértékelésének eredményeképpen döntést kell hozni a változtatás megvalósításáról, illetve elvetéséről. Amennyiben a változtatási kérelmet elutasítják, a változás kérelmezőjét értesíteni kell, a változtatást pedig le kell zárni (lsd.: A változtatás lezárása tevékenység). Amennyiben a változtatás megvalósításáról születik döntés, a változásmenedzser, a változásgazdával együtt elkészíti a kiviteli tervet a szükséges szakterületek bevonásával.

e) Standard változtatási eljárás esetén az a)-d) pontban leírtak a Pályázati Iroda irodavezető jóváhagyásával elhagyhatóak.

(6) A változtatás tervezése

a) A változtatás sikeressége érdekében az engedélyezett változtatás végrehajtását meg kell tervezni, ehhez el kell készíteni a kiviteli tervet.

b) A kiviteli tervben az alábbiakat kell legalább szerepeltetni:

- a változtatás prioritását figyelembe véve ütemezni kell annak megvalósítását,
- meg kell tervezni a változtatás megvalósításának lépéseit,
- meg kell határozni a változtatáshoz szükséges (emberi és anyagi) erőforrásokat,
- sikertelenség esetére pontosan ki kell dolgozni a javító/visszaállító intézkedés(ek) lépéseit,
- fel kell készülni a változtatás során felmerülő incidensek kezelésére,
- tesztelni kell a változtatást.

c) A változtatásokat úgy kell ütemezni, hogy az a lehető legkevésbé zavarja a felhasználók napi munkáját és a rendszer működését.

d) A változtatásokat javasolt előre meghatározott időszakokban végrehajtani. Az alacsony prioritású változtatások ütemezésénél javasolt több változtatás egyszerre történő megvalósítása. Ebben az esetben azonban figyelemmel kell lenni arra, hogy a túl sok változtatás egyszerre történő megvalósítása ne okozzon függőségi problémákat.

e) Standard változtatási eljárás esetén az a)-b) pontban leírtak a Pályázati Iroda irodavezető jóváhagyásával elhagyhatóak.

(7) A változtatás végrehajtása a kiviteli tervben meghatározott módon történik.

(8) A változtatás végrehajtása után a változtatást le kell zárni. A lezárás során a változásmenedzsernek a következő lépéseket kell elvégeznie:

a) Meg kell győződni arról, hogy a változtatás elérte a célját, vagy amennyiben sikertelen volt, megtörténtek a megfelelő visszaállító intézkedések.

b) Tájékoztatni kell a változtatást igénylőjét, és meg kell győződni arról, hogy az elégedett az eredménnyel és egyetért a változás lezárásával.

c) Ellenőrizni kell, hogy a változás megfelelően van-e dokumentálva.

VII. IT SZOLGÁLTATÁSFOLYTONOSSÁG BIZTOSÍTÁSA

52.§ 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).

53.§ 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.

VIII. RENDELKEZÉSRE-ÁLLÁS BIZTOSÍTÁSA

54.§ Rendelkezésre-állás, megbízhatóság, szervizelhetőség

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

55.§ 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.

IX. KAPACITÁSOK BIZTOSÍTÁSA

56.§ Kapacitáskezelés

(1) A Pályázati Iroda irodavezetője a felelős azért, hogy a felhasználóktól beérkező igények, a szolgáltatói környezet változása, a technikai fejlődés figyelembevételével tervezze, és az elfogadott intézményi költségvetés keretin belül javaslatot tegyen az intézmény működéséhez szükséges IT-kapacitások meghatározására.

57.§ 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.

(4) A nem Pályázati Iroda által üzemeltetett szolgáltatások esetében az üzemeltető az adott szolgáltatás kapacitásterve alapján fejlesztési tervet készít, amelyet a következő évi költségvetés tervezetével együtt benyújt a Pályázati Iroda irodavezetőjének.

(5) A kapacitástervek és a fejlesztési tervek összegyűjtése után a Pályázati Iroda irodavezetője döntés-előkészítő anyagot készít a rektor részére. A rektor az intézményi lehetőségeket figyelembe véve szolgáltatásonként külön-külön, döntést hoz a fejlesztésekről vagy azok elutasításáról.

X. ZÁRÓ RENDELKEZÉSEK

58.§ Az IIBSZ változásmenedzsmentje

(1) Az IIBSZ-szel kapcsolatos észrevételeket, változtatási javaslatokat a Pályázati Iroda irodavezetőjének címzett, a 3. sz. mellékletben található változáskezelési lapon (vagy vele megegyező tartalmú elektronikus levélben) lehet benyújtani.

(2) A Pályázati Iroda irodavezetője megvizsgálja a változtatási javaslatot és dönt annak elfogadásáról.

a) Elfogadás esetén előkészíti a módosítást az egyetem szenátusának.

(3) A Pályázati Iroda irodavezetője 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 a Pályázati Iroda irodavezetője saját hatáskörben végzi konzultálva az érintett szervezeti egységek vezetőivel.

(5) Az IIBSZ mellékletek Pályázati Iroda irodavezetői utasítások formájában készülnek és módosulnak.

59.§ Hatályba lépés

(1) Jelen szabályzatot a Dunaújvárosi Egyetem Szenátusa a 49-2024/2025. (2025.03.27.) számú határozatával fogadta el, amely 2025.04.01.napján lép hatályba.

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

Jelen szabályzat elérési útvonala: N:\1 - Szabályzatok

Dunaújváros, 2025.03.28.

Dunaújvárosi Egyetem 1. Dunaújváros

dr. András István
rektor

dr. Hegedüs Ágnes

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 Pályázati Iroda (PI) 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 a Pályázati Irodánál. Nagyobb szabású rendezvény, konferencia rendezése esetén a rendezvény szervezője igényli a résztvevők számára a hálózati hozzáférést a Pályázati Irodánál.

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. A Pályázati Iroda jogosult a hosszabb időn át fennálló indokolatlanul magasnak tartott forgalom vizsgálatára és a forgalmazó számítógép/felhasználó ellenőrzésére. A legnagyobb forgalmat generáló munkaállomások toplistáját az Pályázati Iroda 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 a Pályázati Iroda jogi felelősségre vonást kezdeményezhet, a Rektornál.

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

b) A Pályázati Iroda 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 a Pályázati Irodával kell egyeztetni, az ilyen forgalom engedélyezését a Pályázati Iroda a hálózatbiztonsági és a rendelkezésre álló technika lehetőségek, szempontok figyelembevételével 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 utasítására kizárólag hivatalos szervek által történt megkeresés alapján adhat ki információt a hálózati forgalom részleteiről a rendelkezésre álló technikai lehetőségek mértékéig.

g) A Pályázati Iroda 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) A Pályázati Iroda 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 a Pályázati Irodának kell bejelenteni (HelpDesk). A bejelentést első sorban a https://ticket.net.uniduna.hu/ webcímen kell megtenni. A HelpDesk az I-épület földszintjén található. A Bejelentő telefonszám munkaidőben a + (30) 013-4209. A 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.

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 használt 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.