Informatikai szabályzat

Hatályba lépés napja: 2022. május 21.

I. könyv - Informatikai üzemeltetési és hálózati szabályzat

Tartalom

1. ÁLTALÁNOS RENDELKEZÉSEK

1.1 Az Informatikai üzemeltetési és hálózati szabályzat célja

A Semmelweis Egyetem (a továbbiakban: Egyetem) Informatikai üzemeltetési és hálózati szabályzatának (a továbbiakban: IÜHSZ) célja, hogy elősegítse az Egyetemen elérhető szolgáltatások használata, alkalmazása során az informatikai és infokommunikációs eszközök előírásoknak megfelelő és biztonságos használatát, az adott üzemeltetésre vonatkozóan útmutatást nyújtson, a szükséges felhasználói-, üzemeltetői-, vezetői teendők és felelősségi körök meghatározásával biztosítsa az informatikai rendszerek folyamatos és rendeltetésszerű működését.

1.2 Az Informatikai üzemeltetési és hálózati szabályzat hatálya

(1) Az IÜHSZ területi hatálya alá tartoznak:

a) az informatikai infrastruktúra eszközei és a hozzátartozó alépítmények, helyiségek,
b) számítógéptermek és a hozzájuk kapcsolódó helyiségek,
c) karok, intézetek, és a központi szervezeti egységek, beleértve az Informatikai Főigazgatóság (a továbbiakban: IFIG) mindazon helyiségei, amelyekben informatikai berendezések üzemelnek,
d) karok, intézetek kihelyezett, bérelt helyiségei, ahol informatikai berendezések üzemelnek,
e) az egyetemi munkavégzés céljára saját tulajdonú informatikai eszközök az Információbiztonsági szabályzatban meghatározott feltételek teljesülése esetén használhatók.

(2) Az IÜHSZ személyi hatálya kiterjed:

a) az Egyetemen foglalkoztatott munkavállalókra, egészségügyi szolgálati jogviszonyban álló, szerződéses jogviszonyban álló, jogi és természetes személyekre, jogi személyiséggel nem rendelkező szervezetekre,
b) az Egyetemmel szerződéses kapcsolat keretében információcserét (küldés és/vagy fogadás, tárolás/továbbítás) folytató szervezetekkel történő kommunikációra, függetlenül a szervezet betöltött szerepétől, szervezeti helyétől, elhelyezésétől és az Egyetemhez fűződő kapcsolatától,
c) az Egyetemmel hallgatói vagy más képzési jogviszonyban álló személyekre – a jelen szabályzatban meghatározott eltérésekkel,
d) az Egyetem tulajdonában lévő informatikai eszközök használóira.

(3) Az IÜHSZ tárgyi hatálya kiterjed az Egyetem tulajdonában lévő összes informatikai vagyontárgyra, szerződés alapján üzembe helyezett, nem egyetemi tulajdonban lévő eszközökre (vezérlő eszközök, szerverek, munkaállomások, stb.), külső, non-profit intézmények, szervezetek, valamint munkatársak, hallgatók saját tulajdonú eszközeire, számítógépeire, amelyek az Egyetem informatikai rendszerével kapcsolatban állnak vagy kapcsolatba kerülnek, ezen belül eszköztípusonként:

a) a számítógép-hálózatok aktív és passzív elemeire,
b) szerverekre és hálózati szolgáltatást nyújtó berendezésekre,
c) valamennyi munkaállomásra, nyomtatóra,
d) perifériákra és tartozékaikra,
e) hordozható számítógépekre,

f) adathordozókra az USB-flash-tárolók (pendrive) kivételével,
g) valamennyi szoftverre.

(4) Az IÜHSZ hatálya nem terjed ki azokra az egyéb speciális eszközökre, pl. diagnosztikai laborrendszerekre, amelyek használatához az Egyetem külön üzemeltetési szerződést kötött.

2. AZ EGYETEM INFORMATIKAI MŰKÖDÉSE

2.1 Az informatikai működés szintjei

Az Egyetem informatikai rendszereinek működése a következő szinteken valósul meg:

a) Egyetemi szint:
Az Egyetem Informatikai Főigazgatósága valamint a szervezet részét képező igazgatóságok és osztályok (továbbiakban együttesen: IFIG) biztosítja az Egyetem informatikai alapszolgáltatásait (hálózati infrastruktúra működtetése, felügyelete, fejlesztése, központi informatikai szolgáltatások biztosítása, központi informatikai rendszerek üzemeltetése, (pl. internet, intranet, központi címtár, levelezés, vírusvédelem, NEPTUN tanulmányi rendszer, SAP, MedSolution, PACS, Labor rendszerek, stb.).
Az IFIG szakemberei ezeken túl szakmai támogatást nyújtanak és koordinációt biztosítanak az informatikai szolgáltatások valamennyi területén a többi informatikai egység, helyi informatikusok számára.

b) Kari, területi szint:
A karok informatikai szempontból különbözőek, az alapszolgáltatások és egységes egyetemi alkalmazói rendszerek használatán túl a kari informatikai rendszerek egyediek, néhány esetben a feladatokat saját kari / tömbi szintű informatikai szervezet látja el.

c) Intézeti szint:
Intézeti szinten nincs különálló informatikai szervezet, csak alkalmazott informatikusok. Az üzemeltetési feladatokat a helyi informatikai szakemberek, a kari és az egyetemi szintű üzemeltetési központok támogatásával látják el.

d) Helyi szint:
Ezt a szintet a helyi hálózatba kapcsolt, valamint attól függetlenül működő számítógépek és a hozzá kapcsolt berendezések együttesen jelentik, egy épületen/tömbön belüli területet értjük alatta.

2.2 Az Egyetem informatikai működése

(1) Az informatikai szervezetek, a közös célok – az Egyetem szakmai feladatainak magas színvonalú teljesítése - megvalósításában együttműködnek.

(2) Az informatikai rendszerek működtetése, továbbfejlesztése valamennyi informatikai szervezet közös feladata. Az informatikai szervezetek kötelesek a közösen hozott döntéseket és az egyetemi szabályzatokat betartani, és betartatni (pl. névkonvenciók, IP-tartományok, vírusvédelem).

2.2.1. Az egyetemi informatikai szervezetek

(1) Az egyetemi informatikai szervezetek tevékenységeit és felelősségi körét a Szervezeti és Működési Szabályzat szabályozza.

(2) Egyetemi központi informatika – IFIG

a) Felelős a teljes egyetemi információtechnológiai alapinfrastruktúra működtetéséért, valamennyi informatikai és távközlési rendszer működési feltételeinek biztosításáért.

b) Kialakítja a fejlesztések koncepcióit, terveit, szakmai támogatást nyújt, konzultál, döntéseket készít elő és kapcsolatot tart az érintettekkel: vezetőkkel, felhasználókkal, informatikai szervezetekkel és külső partnerekkel.

c) Üzemelteti, és folyamatosan fejleszti az Egyetem központi információtechnológiai rendszerek erőforrásait.

d) Fogadja, menedzseli a szervezetek informatikai szolgáltatásokra vonatkozó jelzéseit, igénybejelentéseit, javaslatait.

e) A helyi felhasználói kéréseket a helyi informatikai felelős, a különböző rendszerekkel kapcsolatos problémákat a rendszergazdák, az alkalmazásokkal kapcsolatos ügyeket az alkalmazásgazdák továbbítják az IFIG-nek, továbbá központi egyetemi rendszerek esetén az egyetemi szintű üzemeltetésben résztvevő szervezeti egységeinek.

f) Az IFIG szakmailag koordinálja, optimalizálja, bonyolítja és felügyeli az informatikai és az infrastruktúrához kötődő beszerzéseket, beruházásokat és fejlesztéseket.

g) Az informatikai rendszerek szabályzatokban foglalt egységes működésének betartása érdekében az IFIG osztályvezetői közvetlenül utasíthatják a helyi informatikai felelősöket, a fent említett további egyetemi üzemeltetési szervezeteket, a rendszer-, és alkalmazásgazdákat és egyben ellátják szakmai felügyeletüket is.

(3) Decentralizált egyetemi informatika szervezetek

a) Az egységes egyetemi informatikai működés biztosítása érdekében szükség van egyes funkciók centralizációjára, melynek keretében az egyetemi üzemeltetési szervezetek szakmai irányítása, koordinációja és bizonyos feladatok, alapszolgáltatások központi, centralizált ellátása megvalósulhat.

b) A területi decentralizációt a helyi informatikai felelősök, a funkcionális decentralizációt az információk és rendszerek adat- és rendszergazdái biztosítják.

c) Decentralizált egyetemi informatika szervezetek az alábbi szervezeti egységekben működnek:

ca) Általános Orvostudományi Kar, Informatikai Osztály,

cb) Központi Könyvtár, Informatika,

cc) Városmajori Klinikai Tömbigazgatóság, Informatikai Csoport,

cd) Egészségtudományi Kar,

ce) Egészségügyi Közszolgálati Kar,

cf) Szakképző intézmények.

d) A (3) c) pontban felsorolt informatikai szervezetek:

da) javaslattal élhetnek az Egyetem informatikai szolgáltatásai kialakítására, módosítására;

db) nem jogosultak önállóan olyan új technológiát bevezetni, amelyet az IFIG előzőleg nem engedélyezett;

dc) nem használhatnak az egyetemi standardon kívüli eszközöket, nem térhetnek el a központilag meghatározott beszerzési alapelvektől, előírásoktól.

(4) Helyi informatikusok
a) Szervezeti egységenként, a helyi informatikusok üzemeltetik a helyi erőforrásokat.
b) Ellátják a helyi felhasználó-támogatási feladatokat.
c) Jogosultak közvetlenül kommunikálni az IFIG-gel és a többi informatikai szervezettel.
d) A helyi informatikai feladatokat önállóan látják el (pl.: felhasználók felvétele, helyi oktatások végzése).
e) Nem jogosultak önállóan olyan új technológiát bevezetni, melyet az IFIG-gel előzőleg nem egyeztettek.
f) Nem használhatnak az egyetemi standardon kívüli eszközöket, nem térhetnek el a központilag meghatározott beszerzési alapelvektől, közbeszerzési előírásoktól.
(5) Rendszergazdák
a) Az egyes informatikai eszközöket – melyek működése helyhez kötött és az egyes szervezeti egységeknél vannak elhelyezve (routerek, switchek, szerverek, stb.) – kötelesek az IFIG által meghatározott módon működtetni.
b) Kötelesek oktatások keretében és önképzéssel a rábízott eszközök használatával, üzemeltetésével megismerkedni.
c) Nem használhatnak olyan hálózati eszközöket, melyet az IFIG nem hagyott jóvá, továbbá nem térhetnek el a központilag meghatározott beszerzési alapelvektől, előírásoktól.

2.3 Szolgáltatási időszak, elérhetőségek

(1) Az egyetemi informatikai hálózat és a központi szolgáltatások (IT-üzemeltetés) egész évben folyamatos (7x24 óra) rendelkezésre állásúak. A szolgáltatói elérhetőségeket az Informatikai Főigazgatóság honlapja tartalmazza.
(2) Az informatikai osztályok munkarendje és elérhetőségi adatai az intraneten, valamint a rendszerhez kapcsolódó üzemeltetési dokumentumokban érhető el.
(3) A helyi informatikai szervezetek, felelősök elérhetőségét a helyi/tömbigazgatósági ügyrendek tartalmazzák, amelyet az IFIG titkárságára közzététel céljából kötelező megküldeni.
(4) AZ IFIG honlapján közzéteszi minden szervezeti egység vonatkozásában az informatikai támogatásáért felelős nevét és elérhetőségét.

2.4 Informatikai szolgáltatások

(1) Az Egyetem által vállalt szolgáltatási szintek, az informatikai üzemeltetők és az információkat felhasználók és az információkezelő eszközöket használók közötti megállapodásokban (SLA-kban) kerülnek meghatározásra.
(2) A teljes egyetemi informatikai infrastruktúra működését az IFIG folyamatosan (7*24 órában) biztosítja, kivételt képeznek a tervezett leállások és az esetleges meghibásodások.
(3) A hálózati alapinfrastruktúra és a központi informatikai rendszerek eszközeinek (szerverek, tárolók, mentőegységek, vezetékes- és vezeték nélküli hálózatok) munkaidőn kívüli felügyeletét az IFIG látja el távfelügyelet formájában, az esetleges hibák elhárítását készenléti szolgáltatással, szükség esetén helyszíni javítással biztosítja.

2.5 Az IFIG felhasználóknak nyújtott szolgáltatásai

(1) Az Egyetem felhasználói számára folyamatosan biztosítja (munkaidőben, vagy munkaidőn kívül készenléti ügyelettel támogatja) az informatikai rendszerek működését és a következő alapszolgáltatásokat:

a) informatikai infrastruktúra működtetése (Központi alkalmazás szerverek, vezetékes és WiFi hálózatok, stb.),
b) egyetemi levelezőrendszer működés (Novell GroupWise),
c) integrált medikai (MedSolution, e-MedSolution és alrendszerei) rendszer elérés,
d) internet és intranet elérés, web-szerver funkciók,
e) fájlszerver-funkciók (Novell, Linux).
f) vírusvédelem, automatikus vírusadatbázis-frissítés,
g) készenlét, sürgős hibák elhárítására.

(2) Folyamatosan biztosított, de csak munkaidőben támogatott szolgáltatások

a) integrált gazdasági rendszer (SAP) elérés,
b) egységes felsőoktatási tanulmányi rendszer (Neptun) elérés (az alkalmazás támogatást a Tanulmányi Nyilvántartó Osztály biztosítja),
c) iktató rendszer (Poszeidon) elérése, működtetése,
d) hibajelentő rendszer (GLPI),
e) egyedi intézeti alkalmazások,
f) IP menedzsment,
g) szerver fejlesztési igényekben tanácsadás,
h) virtuális szerver igények tervezése,
i) távoli hozzáférés VPN konfigurálás,
j) vezetékes és vezeték nélküli hálózati igények koordinálása,
k) központi tűzfal konfigurálási és DNS szolgáltatások,
l) központi levelezés, email címekkel kapcsolatos igények kezelése,
m) felhasználói támogatás szolgáltatások,
n) munkaállomások és perifériák installálása,
o) felhasználók közötti gépátadások bonyolítása, követése,
p) üzem közben észlelt hardver, szoftverhibák elhárítása,
q) adatvisszatöltés a munkaállomásra,
r) informatikai eszközök beszerzésének koordinációja, összefogása, szakmai kontrollja,
s) jogosultsági rendszer menedzselése,
t) a hálózati forgalmi adatok elemzése, közlése,
u) infrastruktúra fejlesztésében történő közreműködés.

(3) Eseti szolgáltatások

a) Eseti szolgáltatások igényének bejelentése személyesen, e-mailben, a hibabejelentő rendszeren keresztül, vagy telefonon történhet.
b) Az igényeket az IFIG illetékes osztályának kell bejelenteni.
c) Az igények teljesítése a probléma prioritása, beérkezési sorrendje, a rendelkezésre álló erőforrások alapján, az igénylővel egyeztetett módon történik.
d) Eseti szolgáltatásokat az informatikai főigazgató felhatalmazása esetén az informatikai szervezetek kijelölt dolgozói is elláthatnak.

2.6 A Központi Könyvtár által nyújtott informatikai szolgáltatások

(1) A Központi Könyvtár informatikai szolgáltatásait a honlapja tartalmazza.
(2) A Központi Könyvtár online szakirodalmi forrásokat (adatbázisok, valamint online elérhető szakfolyóiratok és online könyvek) szerez be az Egyetem részére.
(3) Az ilyen módon előfizetett források fizikailag nem az Egyetem szerverein találhatók, online érhetőek el, az adott forráshoz csak az arra jogosultak férhetnek hozzá.
a) Az azonosítás jellemzően IP cím alapján történik. Ugyanakkor a legtöbb esetben az Egyetem teljes IP tartománya az engedélyezett tartományba esik, így az Egyetem összes számítógépéről az egyetemi hálózaton belülről engedélyezett a hozzáférés.
b) Egyes esetekben az előfizetett források felhasználónévvel és jelszóval férhetőek hozzá. A Központi Könyvtár honlapján közzétett hozzáférési információk kizárólag az egyetemi hálózat gépeiről érhetők el.
(4) A szolgáltatókkal kötött megállapodások határozzák meg, hogy az adott online forráshoz hozzáférő felhasználónak milyen jogosultságai vannak az ott található anyagokkal, valamint milyen tiltások, korlátozások vannak érvényben.
(5) Az online forrásokat használóknak a következő szabályokat kell betartaniuk:
a) A források a mindenkori szolgáltató tulajdonában állnak, így ezen adatbázisok, dokumentumok a szerzői jog védelmére vonatkozó jog szabályai szerint használhatók, a szolgáltató nem ruházza át a tulajdonosi jogot a szolgáltatás előfizetőjére, az előfizető nem reprodukálhatja, másolhatja le, jelentetheti meg máshol a szolgáltatás egészét, vagy részét.
b) A szolgáltatás hozzáférhetősége kizárólag a szerződésben említett felhasználók számára biztosítható, az előfizetőnek gondoskodnia kell a hozzáférési szabályok betartásáról. Ha a szolgáltatás felhasználó névvel és jelszóval érhető el, akkor ezen adatokat csak olyan módon szabad közölni a felhasználókkal, hogy azok nyilvánosan elérhető és indexelt weboldalakon ne jelenjenek meg.
c) Távoli hozzáférés az előfizetett intézmény tagjai számára engedélyezett, egyéni, valamint nem kereskedelmi célú használatból. A távoli hozzáférési kapcsolatnak biztonságosnak, más külső felhasználó által nem hozzáférhetőnek kell lennie. Távoli hozzáférés más intézmény tagjai számára nem megengedett.
d) A felhasználók a forrásokban található anyagokat szabadon letölthetik, kinyomtathatják, korlátozott számban reprodukálhatják, saját, vagy intézeten belüli használatra, valamint az adott anyag copyright licencében meghatározott feltételek szerint. A letöltött anyagok kereskedelmi célból nem használhatóak fel, valamint ezen anyagokat nem lehet publikálni.
e) A forrásokra mutató elektronikus linkek közzététele csak kizárólag az engedélyezett felhasználók számára elérhető módon lehetséges, ezen linkeket nyilvánosan közzétenni nem megengedett.
(6) A felsorolt szolgáltatások működtetését a Központi Könyvtár szervezeti ügyrendje határozza meg.

2.7 Az informatikai szervezeteknek nyújtott szolgáltatások

2.7.1. Hálózatmenedzsment

(1) Az elvárt magas rendelkezésre állás biztosítása érdekében az Egyetem több szintű központi hálózatmenedzsment rendszert alkalmaz, amely többek között biztosítja a rendszer naplófájlokat (syslog), szoftver image-t, konfigurációs fájlkezelést, topológiai térképet, a központilag menedzselt mentési funkciókat és a kritikus hálózati forgalmak mérését.
(2) A központi hálózatmenedzsment rendszereket az IFIG üzemelteti. Elsődleges célja, hogy a hálózat üzemeltetését, a hibakeresést és a hibák elhárítását megkönnyítse. A tárolt adatok aktualizálása és a változások követése kiemelt jelentőségű.

2.7.2. Szerverek, adatbázisok központi és helyi mentése

(1) A központi egyetemi rendszerek és szerverek rendszeres mentéséről az IFIG munkatársai, a további *egyetemi rendszerek és szerverek* mentéséről pedig az érintett üzemeltető informatikai szervezet gondoskodik. Kritikus szerverek és azok adatbázis adatainak mentése ütemezetten történik.
(2) Kari, valamint az intézeti helyi szerverek adatainak mentése - így a helyi, intézeti Novell szerverek adatainak mentése is - a kijelölt rendszergazdák feladata.

2.7.3. Távfelügyelet

(1) A távfelügyeletet az IFIG hálózatmenedzsment rendszergazdái látják el. A távfelügyelet az informatikai infrastruktúra komponenseit – optikai és mikrohullámú gerinchálózat, hálózatvezérlő eszközök, szerverek és ezek kiemelt szolgáltatásait, valamint az IFIG-en lévő egyéb kiemelt erőforrásokat (pl. központi UPS-ek) monitorozza.
(2) Hiba esetén a monitorozó rendszer e-mailben értesíti az IFIG készenlétet ellátó munkatársát, aki az adott hiba kezelésére vonatkozó eljárási utasítás alapján elvégzi a szükséges tevékenységeket.
(3) Azon szervezeti egységek, akik önállóan üzemeltetik a hálózatukat, az eszközei nincsenek integrálva a monitorozó rendszerekbe, így nincsenek bevonva a távfelügyeletbe sem.
(4) Az Egyetem kari/intézeti informatikai szervezeteinek távfelügyelettel kapcsolatos feladatai:
a) hibajelzés esetén segíteni a hiba behatárolását, elhárítását,
b) előre bejelenteni a tervezett leállásokat, továbbá az általuk monitorozott eszközökben és szolgáltatásokban bekövetkező változásokat.

2.7.4. Tervezett rendszerkarbantartás, leállás

(1) Tervezett rendszerkarbantartásról és leállásokról, áramszünetről legalább 2 munkanappal korábban írásban értesíteni kell az érintett felhasználói kört.
(2) Központi leállás esetén az IFIG értesíti a távfelügyeletet, a kari/intézeti informatikai szervezeteket és rendszergazdákat, akik a hozzájuk tartozó intézeteket és felhasználókat tájékoztatják.

3. SZOLGÁLTATÁS TÁMOGATÁS

3.1 Felhasználói Támogatás

(1) Egyetemi szinten az Informatikai Rendszertámogató Osztály munkatársai, kari szinten az adott kar informatikai szervezetei, intézeti szinten az informatikai felelősök biztosítják a kapcsolatot az informatikai szolgáltatások és a felhasználók között.
(2) Az informatikai felelősök feladata: incidensek, problémák kezelése, megoldása, kérdések megválaszolása, változáskérelmek fogadása, konfigurációkezelés, rendelkezésre állás menedzsment.
(3) A felhasználói támogatás első vonalbeli támogatást és hibaelhárítást is végezhet, háttértámogatást kérhet a szakmai csoportoktól, az IFIG-n működő szakértőktől, valamint a szerződéses kapcsolatban levő külső cégektől.
(4) Az Egyetem dolgozói az IFIG honlapján tájékozódhatnak a hiba esetén értesítendő IT munkatársak elérhetőségéről.

3.2 Rendszerek felhasználóinak kezelése

(1) Új felhasználók felvételét, a meglévő jogosultság törlését az érintett szervezeti egység vezetője írásban kezdeményezi a mellékletben felsorolt és formanyomtatványtárból elérhető űrlap kitöltésével.
(2) Kilépett dolgozókról az IFIG titkárság adatszolgáltatás útján kap értesítést az Emberierőforrás-gazdálkodási Főigazgatóságtól, ami alapján egy munkanapon belül gondoskodik a távozó munkatárs rendszerekből való kiléptetéséről. Kilépett dolgozó leveleinek időleges kezelését, átirányítását, mentését a korábbi munkahelyi vezető kérésére az informatikai szervezet végzi (a kilépett dolgozó postafiókja zárolásra, 30 nap elteltével pedig törlésre kerül).
(3) Központi alkalmazások eléréséhez a beérkezett kérelem alapján az IFIG biztosítja a felhasználók részére a hozzáférést. A nem központi alkalmazásokhoz igényelt jogosultság kezelését az IFIG honlapján közzétett útmutató tartalmazza.

3.3 Munkaállomások menedzselése

(1) Új munkaállomás rendszerbe állítását az adott szervezeti egység vezetője kezdeményezi. Az Informatikai Rendszertámogató Osztály munkatársa, vagy a helyi informatikai felelős telepíti az operációs rendszert és a szükséges alkalmazásokat, átvezeti a személyes beállításokat, valamint intézi a szükséges központi alkalmazásokhoz szükséges jogosultságok beállítását. Ezt követően átadja a munkaállomást a felhasználónak, és értesíti az IFIG-et, valamint a szervezeti egység gazdasági vezetőjét az új munkaállomás üzembe állításáról. Az Egyetem informatikai hálózatára csatlakoztatott valamennyi informatikai eszközt az IFIG által meghatározott vírusvédelemmel kell ellátni.
(2) Munkaállomás hardver konfigurációjának változását a munkahelyi vezető kezdeményezi, de a szakmai döntés joga a helyi informatikai felelősé. A helyi informatikai felelős a konfigurációs elemeket, egységeket beépíti, konfigurálja, majd a munkaállomást átadja a használójának. Az esetlegesen kivont/kiszerelt egységeket raktárban helyezi el tartalék alkatrészként történő hasznosításra. A munkaállomás

konfigurációjának módosítását át kell vezetni az eszközök nyilvántartásán és arról értesíteni kell a szervezeti egység gazdasági vezetőjét is.

3.4 Szoftvertelepítés

(1) A központilag beszerzett szoftver licenceket az IFIG kezeli (telepítések kontrollja, licencek nyilvántartása, jogszerű használat biztosítása, stb.). A telepítéshez szükséges kódokat a kijelölt rendszergazdák személyesen veszik át az IFIG-től, a munkaállomás szoftverek telepítő készleteit a telepítésre jogosultak részére az IFIG elérhetővé teszi.
(2) Egyedi beszerzésű szoftverek telepítése: a licencek ellenőrzése és nyilvántartása a szervezeti egység kijelölt rendszergazdájának feladata és felelőssége.
(3) Szerverek és szerveralkalmazások telepítése előtt a helyi rendszer-, vagy alkalmazásgazda köteles konzultálni az IFIG-gel.
(4) A napi működéshez szükséges szoftvereket (beleértve az ingyenes és szabad szoftvereket is – pl. Java környezet, média lejátszó) az informatikus munkatársak telepítik a felhasználók gépeire.
(5) A szoftverekhez tartozó végfelhasználói licencszerződések tartalmáról a szoftvereket használó felhasználók számára minden esetben a helyi rendszergazda ad tájékoztatást, azokat az IFIG nyilvántartásában fel kell tüntetni.
(6) Egyéb, licenccel nem rendelkező szoftvert telepíteni tilos. Szabad, ingyenes programok telepítése is kizárólag szakmai indoklással lehetséges. Az e körbe tartozó szoftverek telepítését az érintett informatikai vezető, valamint az IFIG engedélyezheti. Kizárólag azok a felhasználók rendelkeznek szoftvertelepítési jogosultsággal, akiknek a munkavégzéséhez az szükséges. A jogosultságot a felhasználó munkahelyi vezetőjének javaslata alapján az IFIG hagyja jóvá, és a telepítést követően azt nyilvántartásba veszi.
(7) Az egyetemi munkavégzéshez használt informatikai eszközökre történő szoftvertelepítések során az Információbiztonsági Szabályzat rendelkezéseit be kell tartani.

3.5 Problémamegelőzés

Az egyes szolgáltatások üzemeltetői reaktív és preventív intézkedéseket tesznek a szolgáltatás zavartalansága érdekében. Ezek lehetnek általános és az adott szolgáltatásra speciálisan jellemző feladatok, így különösen:

a) igény szerinti újraindítás, alapállapotba hozás,
b) javítócsomagok, patchek telepítése,
c) jelszavak és hozzáférési kódok rendszeres cseréje,
d) naplóállományok rendszeres kiértékelése,
e) vírusvédelem működésének ellenőrzése.

3.6 Incidens-kezelés

(1) Az informatikai rendszer leállását követő incidenskezelés elsődleges célja az érintett szolgáltatás mielőbbi visszaállítása. Az incidenskezelés felelőse az informatikai szervezet az incidens teljes életciklusa alatt.
(2) Az IFIG az incidensekről felhasználói, a helyi informatikai felelős bejelentése útján vagy rendszer felügyeleti eszköz segítségével szerez tudomást.

(3) Az incidensek információit a hibabejelentő rendszerben rögzíteni kell, minden olyan adat megadásával, ami az incidens elhárításához szükséges.
(4) Az információk értékelésekor az IFIG szakemberei felmérik az incidens sürgősségét és hatását, ennek alapján határozható meg az elhárítás prioritása.
(5) Incidens megoldása történhet úgy is, hogy a szolgáltatást biztosítása csökkentett szinten valósul meg. A probléma végleges megoldása után a szolgáltatás működőképességének, vagy eredeti színvonalának visszaállítása a rendszergazda és az IFIG szakembereinek a feladata.
(6) Az incidens lezárása minden esetben az érintett felhasználók értesítése után történhet.
(7) A védelmi intézkedés bejelentésének elmulasztásából, valamint a nem szabályszerű üzemeltetésből következő károk az üzemeltető informatikai szervezeti egység felelősségi körébe tartoznak.
(8) Személyes adatot érintő incidensről az adatvédelmi tisztviselőt haladéktalanul tájékoztatni kell és az elhárítását vele együttműködve szükséges biztosítani.

3.7 Hibakezelés

(1) A felhasználók az informatikai jellegű hibákat (helyi hálózat, helyi szerver, munkaállomások, nyomtatók, stb.) az IFIG Informatikai Rendszertámogató Osztályán, vagy az Infrastruktúra Üzemeltetési Osztályon, vagy a helyi informatikai felelősnek jelentik be. Amennyiben a helyi informatikus nem tudja elhárítani a hibát, azt jelzi az IFIG Informatikai Rendszertámogató Osztályának vagy az Infrastruktúra Üzemeltetési Osztályának.
(2) Az intézetek az IT infrastruktúrával, központi szolgáltatásokkal kapcsolatos hibákat közvetlenül az IFIG felé jelzik.
(3) A kari hatáskörbe tartozó hibák elhárítása a kari informatikai szervezetek feladata. A kari informatikai szervezetek a hatáskörükbe tartozó hibákat eszkalálhatják az IFIG felé, valamint a velük, vagy az Egyetemmel szerződésben levő partnerek felé.
(4) Az intézeti hatáskörbe tartozó hibák elhárítása a helyi informatikai felelős feladata.
(5) Az IFIG a felhasználók, valamint az intézetek által bejelentett IT infrastruktúrával, központi szolgáltatásokkal, alkalmazásokkal és az internet, intranet szolgáltatással kapcsolatos hibák elhárítását menedzseli. Amennyiben a hibát nem tudja elhárítani, akkor az Egyetemmel szerződésben levő külső partnerek felé eszkalálja a problémát.
(6) Az informatikai alkalmazói rendszerekkel kapcsolatos hibák elhárítása az üzemeltetést végző alkalmazásgazdák/rendszergazdák feladata. A hibák kezelésére, az eszkaláció módjára vonatkozóan a rendszerek üzemeltetési szabályzataiban foglaltak az irányadók.
(7) Az egyetemi kari/intézeti hibakezelés folyamatát a 2. sz. melléklet tartalmazza.

3.8 Változáskezelés

A változáskezelés gazdái az informatikai szervezeti egységek, valamint az IFIG. A változáskezelési kérelmekről, a változásokról nyilvántartást vezetnek.

3.9 Konfigurációkezelés

A konfigurációkezelés célja az informatikai infrastruktúra komponenseinek azonosítása, adatainak követése, segítve ezzel az incidens-, probléma- és változáskezelést, biztosítva a gazdaságos üzemeltetés lehetőségét (pl. licencgazdálkodás).

3.10 Katasztrófa-elhárítás

Katasztrófahelyzet bekövetkezhet elháríthatatlan ok, vagy szándékos károkozás következtében is. A katasztrófa bekövetkezte után az informatikai szervezetnek képesnek kell lennie a szolgáltatás helyreállítására. Ennek érdekében katasztrófa-elhárítási terveket kell kidolgozni minden olyan területre, amelyek az Egyetem főbb funkcióinak ellátásában, végzésében nélkülözhetetlenek. A katasztrófa-elhárítási tervek az egyes rendszerek üzemeltetési szabályzatának részei.

4. AZ INFORMATIKAI SZOLGÁLTATÁSOK ALAPJAI

4.1 A géptermekre vonatkozó intézkedések

A géptermek tűzvédelmi, továbbá a helyiségekbe való belépés és benntartózkodás általános szabályai részletesen az Információbiztonsági Szabályzatban találhatóak.

4.2 Felhasználókra vonatkozó szabályok és kötelességek

(1) Felhasználó az Egyetem informatikai rendszereit használó, a szabályzat személyi hatályánál meghatározott személy vagy szervezet.
(2) A felhasználókra vonatkozó általános szabályok az *Információbiztonsági szabályzatban* találhatóak.

4.3 Üzemeltetőkre vonatkozó előírások

4.3.1. Üzemeltető szervezet

(1) Az Egyetem IT infrastruktúrájának üzemeltetési feladatait az IFIG látja el, amelynek meghatározott feladatait a helyi informatikai felelősökre átruházhatja. Az egységes koncepció mentén kialakított hálózati és szerver infrastruktúra biztonságos és költséghatékony üzemeltethetősége érdekében szakmai szempontból minden fejlesztési igényt az IFIG hagy jóvá. Nem telepíthetők olyan hálózati eszközök, melyet az IFIG nem engedélyezett.
(2) Az egyes karok/intézetek, szervezetek a hatáskörükben működő informatikai rendszerek üzemeltetési feladatait az arra kijelölt informatikai szervezet (csoport, osztály, személyek) látja el. „Kihelyezett” informatikai eszközök alatt értjük az oktatótermek, laboratóriumok több munkatárs, vagy hallgató által használt eszközállományát, amelyeket minden esetben erre kijelölt személyek üzemeltetnek.
(3) Üzemeltető szervezet feladatai
a) Irányítja a hozzá tartozó terület informatikával kapcsolatos szolgáltatói, üzemeltetői tevékenységet.
b) Fogadja a szakmai területekről érkező fejlesztési igényeket, és jóváhagyás esetén gondoskodik azok megvalósításának előkészítéséről.
c) Üzemelteti a szervezeti egység helyi alkalmazásait.

d) Gondoskodik a hozzá tartozó terület rendszergazdai feladatainak ellátásáról.
e) Gondoskodik az incidenskezelés, a problémakezelés és a konfiguráció kezelés működtetéséről.
f) Elkészíti, és folyamatosan aktualizálja a katasztrófa-elhárítás tervét.
g) Gondoskodik a hozzá tartozó terület infrastruktúrájának fejlesztéséről és üzemeltetéséről.
h) Gondoskodik az IÜHSZ aktualizálásáról.
i) Érvényesíti az informatikai biztonsági, adatbiztonsági elvek betartásáról szóló rendelkezéseket.
j) Részt vesz a hatáskörébe rendelt informatikai vonatkozású beszerzések előkészítésében és végrehajtásában.
k) Kapcsolatot tart az egyetemi szervezetekkel, felhasználóival, felhatalmazás esetén szakmai kapcsolatot tart más szervezetek informatikai szervezeteivel,
l) Az üzemeltető szervezet munkatársai a külső szerződéses munkatársakkal, valamint egyéb eseti megbízással munkát végző munkatársakkal együtt (továbbiakban: üzemeltetők) működtetik az adott szervezeti egység számítógépes hálózatát, géptermét, elhárítják a fellépő hibákat, gondoskodnak azok megszüntetéséről.
m) Véleményezi, továbbá megvalósítja az informatikai fejlesztéseket.

4.3.2. Üzemeltetés vezető

(1) Az egyetemi informatikai infrastruktúra és a központi szolgáltatások üzemeltetésének vezetését az IFIG vezetője, az egyetemi szintű rendszerek üzemeltetésének koordinációját az üzemeltető informatikai szervezet vezetője által kijelölt személy(ek), a karnál/intézetnél az illetékes informatikai szervezet vezetője, vagy az általa kijelölt személy(ek) látják el.
(2) Feladatai
a) Az Egyetem feladatait támogató informatikai tevékenységek szakmai irányítása.
b) Az Egyetem hardver és szoftver eszközeinek folyamatos karbantartásának szervezése, működőképességük biztosítása.
c) A szerverszobák és géptermek tevékenységének, szolgáltató munkájának irányítása, megszervezése.
d) Az informatikai rendszerek működésének felügyelete, és biztonságuk szempontjából lényeges paramétereinek folyamatos figyelemmel kísérése.
e) Javaslattétel a rendszerek szűk keresztmetszeteinek megszüntetésére.
f) Az IÜHSZ, valamint az Információbiztonsági szabályzat betartatása, a végrehajtás megvalósulásának ellenőrzése.
g) Felelős a szerveren lévő adatok biztonsági másolatainak elkészítéséért és megőrzéséért.
h) Együttműködik az adatvédelmi és az információbiztonsági felelőssel.
i) Az informatikai infrastruktúra és az egyetemi központi rendszerek üzemeltetésről az IFIG igazgatója rendszeresen beszámol a műszaki főigazgatónak.

4.3.3. Rendszergazda

(1) A rendszergazdák az üzemeltető szervezet speciálisan képzett belső munkatársai, akik ellátják a szerverek és rendszerek üzemeltetési feladatait, konfigurálják a

munkaállomások, kliens gépek, nyomtatók és egyéb eszközök rendszerhez tartozó beállításait, továbbá gondoskodnak a rendszerhez tartozó szoftverek telepítéséről és azok frissítéséről.

(2) Feladatai

a) Rögzíti és karbantartja a felhasználók - adott rendszer használatához szükséges adatait – bejelentkezési neveit. Kikényszeríti a jelszavak a jelszópolitikában meghatározottak használatát.
b) A hozzáférési szinteknek megfelelően beállítja a megfelelő jogosultságokat.
c) Az adatok reprodukálhatóságának érdekében rendszeres mentést és archiválást végez a vonatkozó helyi előírások szerint. A mentéseket és archívumokat tartalmazó adathordozót zárható, tűzbiztos helyen tárolja, amelyhez az üzemeltetés vezetőjén és a rendszergazdán kívül csak feletteseik férhetnek hozzá.
d) Feladata jogtiszta szoftverek telepítése a szervereken, jogtiszta kliensszoftverek telepítéseinek irányítása, azok felhasználása során felmerülő felhasználói igények, kérdések kezelése.
e) Kijelölés alapján kapcsolatot tart más szervezetek rendszergazdáival.
f) A rendszergazda dokumentál minden, a rendszeren végzett módosítást (az operációs rendszer beállításait érintő változtatásokat).
g) Amennyiben az IFIG rendszergazdája bármely, IFIG-en kívül eső szerveren változtatást végez, előre írásban értesíti a szervert üzemeltető helyi informatikai szervezetet és csak annak jóváhagyását követően végzi el a változtatást.

4.3.4. Alkalmazásgazdák

(1) Az alkalmazásgazdák az egyes alkalmazások vonatkozásában ellátják a rendszergazdáknál ismertetett feladatokat.

(2) Az informatikai rendszerek üzemeltetésében résztvevő szervezeti egységek a működtetett informatikai alkalmazáshoz alkalmazásgazdákat neveznek ki. Több szervezeti egységet érintő alkalmazás esetén a helyi szakmai (nem informatikai, pl. orvos szakmai, gazdasági,) problémák hatékony és koncentrált kezelése érdekében a szervezeti egység vezető helyi alkalmazásfelelőst is kijelölhet.

4.3.5. Helyi informatikai felelős

Feladatai:

a) A helyi informatikai hálózat, az informatikai hardver és szoftver eszközök rendeltetésszerű és hatékony működésének biztosítása, továbbá közreműködés az IFIG-gel azok működtetésének támogatásában, felügyeletében, szervízelésében és karbantartásában.
b) Az informatikai eszközök, hálózati elemek, hardver konfigurációk, szoftvereszközök nyilvántartása (IP címek, konfigurációk, a szervezeti egységek által beszerzett desktop szoftver licencek).
c) Felhasználók támogatása, hibajelzések fogadása, kezelése, megoldása, ennek hiányában a problémák továbbítása.
d) Szervezet által használt informatikai rendszerek, alkalmazások informatikai támogatása azok üzemeltetési szabályzataiban foglaltak szerint.

e) Rendszergazdai feladatok ellátása a helyi szerverek és helyi szinten működtetett rendszereket illetően (szerverfelügyelet, levelezés, vírusvédelem, stb.).
f) Informatikai probléma esetén konzultál, hibajelentést tesz az IFIG-nek, rendszerekkel, alkalmazásokkal kapcsolatos problémák esetén a rendszergazdák, alkalmazásgazdák, valamint a helyi szakmai felelősök felé.
g) Javaslattétel informatikai eszközök áthelyezésére, nem megfelelő kapacitás, minőség esetén azok cseréjére, beszerzésére és szükség szerint közreműködés annak előkészítésében, kivitelezésében, telepítésében.

4.4 Az üzemeltetés biztonsága

4.4.1. Rosszindulatú szoftver ellenei védelem, vírusellenőrzés és - védelem

(1) A számítógépes kártevő programok mennyisége folyamatosan növekszik, és időről időre új típusok terjednek el. Az ellenük való védekezés víruskereső programnak nevezett szoftverekkel történik.
(2) A vírusvédelem az Egyetem informatikai rendszerei egészére kiterjedő, folyamatos tevékenység. A vírusvédelmi stratégiában az elsődleges hangsúlyt a megelőzés jelenti, olyan üzemeltetési rendet, felhasználói magatartást kell megkövetelni, amely a vírusok bejutásának esélyét minimalizálja.
(3) Vírusvédelemmel kapcsolatos teendők:
a) A munkaállomásokat az egyetem hivatalos vírusvédelmi rendszerével kell védeni, ezeket mindenkor bekapcsolt állapotban kell tartani.
b) Munkaállomásokon külső adathordozókat csak vírusellenőrzés után szabad használni, ezt a védelmi rendszer beállításai útján kötelezővé kell tenni.
c) Kommunikációs csatornákon (internet, e-mail, stb.) átvett fájlok felhasználói vírusellenőrzését minden esetben el kell végezni.
d) Az ismeretlen feladótól érkező e-mailekkel szemben fokozott óvatossággal kell eljárni. Amennyiben ezek a levelek csatolmányokat is tartalmaznak, azok megnyitása előtt a helyi rendszergazdát, vagy az IFIG-et értesíteni kell, mert a számítógépes vírusok aktiválásának leggyakoribb formája a mellékletekbe ágyazott programok elindítása.
e) E-mail-ekben érkező, az informatikai rendszerek hozzáférését lehetővé tévő kódok, a felhasználó személyhez kötődő PIN kódok átadására vonatkozó kéréseket minden esetben vissza kell utasítani.
f) A munkaállomásokon kizárólag megbízható forrásból származó, jogtiszta licencű szoftverek futtathatók.
(4) Felhasználói magatartásból eredő, kártevői fertőzésből származó adatvesztésekért a munkaállomás felhasználója felelős.

4.5 Az egyetemi informatikai hálózat távoli elérése

(1) A távoli elérés típusai:
a) felhasználók számára biztosított hozzáférés,
b) adminisztratív célú hozzáférés (Csak az informatikai rendszerek üzemeltetői számára, távfelügyeleti céllal).
(2) Minden távoli elérés esetében az Információbiztonsági szabályzat – A távoli eléréssel kapcsolatos biztonsági szabályok pontjában leírt szabályok betartása kötelező.

5. INFORMATIKAI FEJLESZTÉSEK ÉS BESZERZÉSEK

Az informatikai beruházások előkészítésére, jóváhagyására és megvalósítására vonatkozóan az Egyetem vonatkozó szabályzatai szerint kell eljárni.

5.1 Források, beszerzés menete

(1) Az informatikai eszközök beszerzésére fordítható összegeket az Egyetem és a szervezeti egységeinek mindenkori éves költségvetése szabja meg. A szervezeti egységek kötelesek informatikai igényeiket a kari/intézeti költségvetés összeállítása előtt az informatikai szervezettel és az IFIG-gel szakmai konzultáció keretében megtárgyalni. Amennyiben az előzetes konzultáció nem történt meg, akkor a beszerzendő eszköz hálózatba telepítését az IFIG megtagadhatja, továbbá ha nem engedélyezetten lett telepítve az eszköz a hálózatba, akkor kitilthatja az egyetemi hálózatból, mindenfajta előzetes egyeztetés nélkül.
(2) Az informatikai eszközök beszerzésének eljárásrendjét a Beszerzési Szabályzat tartalmazza.

5.2 Szoftverek kiválasztása

Szoftverek kiválasztása az IFIG hatáskörébe tartozik. A felhasználói igények megfelelő szintű kielégítése érdekében a vásárolni kívánt szoftver kiválasztása előtt a kezdeményező szervezeti egységnek kötelező konzultálni az IFIG szakembereivel.

5.3 Megvalósítási módok

A kiválasztott szoftverek beszerzése történhet kész szoftver megvásárlásával, vagy szoftver fejlesztésével. A megvalósítás módjáról az IFIG, továbbá a decentralizált informatikai szervezet dönt.

5.4 Szoftver

(1) Szoftvert a megfelelő számú felhasználói jogosultságot biztosító licenccel kell megvásárolni.
(2) Külső fejlesztés csak az IFIG előzetes jóváhagyásával, szakmai közreműködésével történhet, melyhez az információbiztonsági felelős bevonása is szükséges.

5.5 Hálózati eszközök és szerverek beszerzése

Az egyetemen minden hálózati eszköz és szerver beszerzés a hálózati és szerver infrastruktúra biztonságos működése érdekében kizárólag az IFIG előzetes jóváhagyásával, szakmai közreműködésével történhet.

5.6 Külső cégek bevonása

Az IFIG jogosult külső céggel olyan szerződés előkészítésére is, amely több informatikai szervezet által üzemeltetett eszköz támogatására vonatkozik (pl. szerverek). Az ilyen központilag támogatott eszközökre a decentralizált informatikai szervezet is csak az IFIG-gel egyetértésben és közösen köthet más céggel szerződést.

6. HÁLÓZATI SZABÁLYZAT

6.1 Az Egyetem adatátviteli hálózata

(1) Az Egyetem hálózatának működtetését az IFIG végzi.
(2) A hálózat feladata az Egyetemen üzemelő számítógépek között az információátvitel lehetőségének megteremtése és az internettel való kapcsolattartás biztosítása.
(3) A gerinchálózat alhálózatokra osztható, az alhálózatok között IP és IP feletti protokollok továbbítása lehetséges.
(4) Az adatátviteli hálózat részét képezik:
a) az épületeket összekötő vezetékes és vezeték nélküli hálózatok,
b) az épületek belső hálózata,
c) a fenti hálózatrészek összekapcsolására szolgáló aktív eszközök, függetlenül attól, hogy kinek a tulajdonában vannak.

6.2 A hálózat felépítése, üzemeltetése

(1) Az egyetemi gerinchálózat optikai kábelalapú hálózat. Az egyes épületeket és az épületeken belül az egymástól nagyobb távolságra levő pontokat mono- és multimódusú optikai kábelek kötik össze. Az optikai kábelek végpontjaiban hálózati aktív eszközök találhatók, ezekből indul ki az épületek adott részeit összekötő kábelhálózat (továbbiakban felhasználói kábelek). A gerinchálózat magját öt egyetemi Tömbben levő (BKT, KKT, NET, KUT, EOK) kialakított csomópontban elhelyezett központi vezérlőeszközök alkotják.
(2) Azon épületek esetén, ahol az optikai kábeles bekötés nem kivitelezhető:
a) mikrohullámú (analóg, menedzselt),
b) vezeték nélküli kapcsolat (ISM sávban),
c) külső internetszolgáltató igénybevétele is lehetséges.
(3) A felhasználói kábelek lehetnek:
a) Cat5e, Cat6A, Cat7 vagy magasabb minőségi követelményeknek eleget tevő, megfelelő védelemmel ellátott UTP/FTP kábelek (sodrott érpáras, twisted pair, árnyékolt vagy árnyékolatlan kivitelben). Új végpontok kiépítése a Cat6A szabvány szerint történhet.
b) optikai kábelek.
(4) A felhasználói kábelhálózatot csak az IFIG szakembereivel konzultálva, azok útmutatásai alapján lehetséges kiépíteni. Felhasználói kábelhálózathoz tartoznak a vezeték nélküli (wifi, wireless) hálózatok is. Ezek kiépítése, tervezése előtt egyeztetni kell az IFIG munkatársaival, akik specifikálják a menedzselési és hálózatbiztonsági szempontból minősített berendezéseket.
(5) A kábelhálózat bővítése az IFIG-hez eljuttatott, kötelezettségvállalás alapján, külső kivitelező által történhet.
(6) Újonnan kiépített és már meglevő hálózatrészek összekapcsolását kizárólag az IFIG szakembere, vagy megbízottja végezheti el. Az IFIG munkatársa az összekapcsolást megtagadhatja, amennyiben az újonnan kiépített hálózatrész nem felel meg az adott hálózati szegmens műszaki előírásainak, vonatkozó szabványának vagy veszélyeztetné a kábelezésre adott gyártói garanciát.

(7) A hálózati aktív eszközöket (switch-ek, routerek, AP-k, ASA-k, stb.) kizárólag az IFIG szakembere, vagy annak megbízottja csatlakoztathatja és kötheti le a hálózatról.
(8) A hálózatra kizárólag olyan eszköz kapcsolható, amely nem veszélyezteti annak működését. Az IFIG megtagadhatja azon eszközök elhelyezését és működtetését, amelyek nem illeszkednek a hálózat rendszerébe.
(9) Az IFIG a hálózat továbbfejlesztésével kapcsolatos kérdésekben konzultációs lehetőséget biztosít.
(10) A hálózati aktív eszközök feszültségmentesítését, kikapcsolását az alábbi eseteket kivéve kizárólag az IFIG szakembere, vagy annak megbízottja végezheti:
a) áramszünet,
b) tűz-, vízbetörés, egyéb elemi csapás,
c) áramütés, vagy annak gyanúja,
d) egyértelmű készülék meghibásodás (pl. füst, zárlat, stb.).
(11) A kábelhálózatot megbontani, azon módosításokat végezni, csak az IFIG engedélye alapján (lehetőség szerint jelenlétében) lehetséges.

6.3 Az egyetemi hálózat adminisztrálása

(1) A hálózat adminisztrálását és teljes körű hálózat-felügyeletét az IFIG szakemberei végzik.
(2) Az IP címek teljes körű nyilvántartását és kezelését az IFIG végzi az elfogadott LAN-WAN koncepcióban szereplő egységes IP címzés szerint.
(3) A kiszolgáló központi és helyi szerverek az egyetemi géptermekben helyezkednek el.
(4) A LAN-okban a külső IP címek használata nem javasolt. Lehetőség van egyedi kérelmek alapján a belső IP címekhez külső IP címet rendelni. A publikus IP címek igénylése az IFIG-hez címzett igénybejelentő lapon történik (4. számú melléklet). https://semmelweis.hu/informatika/egyeb-szolgaltatasok/hozzaferes-igenylese-modositasa/
(5) Az IFIG domain adminisztrátora kérésre létrehozhat aldomaint, az alábbi feltételek teljesülése esetén:
a) rendelkezésre áll legalább egy megbízhatóan üzemelő, megfelelő operációs rendszerrel rendelkező gép névszerver céljára;
b) az aldomaint kérő szervezeti egység vállalja annak üzemeltetését;
c) az aldomain üzemeltetéséért egy megbízott személy felelős;
d) Az aldomain üzemeltetés részletes szabályait az IFIG adminisztrátorának javaslatai alapján az IFIG vezetője adja ki;
e) A domain adminisztrátor a fenti feltételek nem teljesítése esetén megtagadhatja az aldomain létrehozását, valamint létező aldomain esetén az érintett felelős tájékoztatása után azt megszüntetheti.

6.4 Helyi informatikus, rendszergazda tájékoztatása

(1) A helyi informatikus, rendszergazda - az adott szervezeti egység területén található hálózatrész, valamint az ide tartozó gépek adminisztrálásában segíti az IFIG szakembereit, szakmai kérdésekben képviseli a szervezeti egységet.
(2) Az informatikai felelősökről az IFIG nyilvántartást vezet.
(3) Az informatikai felelős személyének változásáról az IFIG-et értesíteni kell.

(4) Az informatikai felelős feladata az IFIG-től kapott információk eljuttatása az érintettekhez, a szervezeti egység által meghatározott eljárásrend szerint.

6.5 Routing, tűzfal

(1) Az egyetemi hálózat routereit, központi vezérlőeszközeit az IFIG üzemelteti, konfigurálja.
(2) A routing policy-t az IFIG határozza meg. A felhasználókat érintő változásról a helyi informatikai felelősöket tájékoztatni kell (levelező lista, intranet).
(3) Az Egyetem elsődleges internet kijáratán, valamint a tartalék útvonalakon az egyetemi hálózatot tűzfal védi a támadástól.
(4) Külső, intézményekhez, szervezetekhez kapcsolódó hálózatrészek forgalmában a külső intézményekkel kötött kétoldalú szerződésekkel összhangban az IFIG paraméterezi a meghatározott intranet szolgáltatások elérését.
(5) Bejegyzetlen gépek a hálózatot nem használhatják. A bejegyzetlen gépek hálózati forgalmát az IFIG műszaki eszközökkel korlátozhatja.
(6) Egyetemi, belső hálózatról érkező támadások kivédése az egyetemi tűzfalak megfelelő konfigurálásával történik. A különböző biztonsági kockázatú alhálózatok (kollégiumok, intézetek, klinikák) és a kiemelt kritikus rendszerek (pl. szerver farmok) alhálózatai a központi tűzfalon átvezetve felügyelhetők és szükség szerint szeparálhatók is egymástól. Az Egyetem belső hálózatán intézeti tűzfalak üzemeltetése az egységes hálózatmenedzsment biztosítása miatt tilos.
(7) A tűzfalak működtetése az IFIG felelőssége, egyedi beállításokat kizárólag az IFIG-gel írásban egyeztetve lehet megtenni.

6.6 Hálózati vírusvédelem

(1) A hálózat védelmének érdekében a vírusvédelmi szoftverek központi forrásból kerülnek beszerzésre, felelőse és kezelője az IFIG. A szoftver használata szigorú előfeltétele a munkaállomások és szerverek rendszerbe állításának.
(2) A vírusvédelmi rendszer központilag frissített és menedzselt. A helyi informatikusok és rendszergazdák az üzemleltetési területükön lévő gépekért felelnek.

6.7 Elektronikus levelezésszolgáltatás

6.7.1. Elektronikus levelezési címek képzése

(1) Az elektronikus levelezés során minden, használatra jogosított felhasználó egyedi elektronikus levelezési címet kap. A levelezés során használható címek képzése az alábbiak szerint történik: vezetéknév.keresztnév@semmelweis.hu
(2) Az Egyetem karain korábban alkalmazott e-mail címek domain neve, amelyek jelen szabályzat érvényessége ideje alatt még használhatóak, tükrözik a kar angol nyelvű elnevezését:
a) med.semmelweis-univ.hu
b) pharma.semmelweis-univ.hu
c) dent.semmelweis-univ.hu

(3) Amennyiben két vagy több azonos nevű felhasználó kap levelezési címet, a belépés időpontjának függvényében a felhasználó címe sorszámozással megkülönböztető jelzéssel és a szervezeti egységre utaló kiegészítéssel történik.
(4) Az elektronikus levelezés biztonsága érdekében a fogadható és küldhető levelek maximális megengedett mérete: 20Mb.
(5) 20 MB-nál nagyobb levelek a Kormányzati Informatikai Fejlesztési Ügynökség erre vonatkozó biztonságos szolgáltatásának segítségével küldhetők ki. (Részletes információ: https://seka.semmelweis.hu/hu/info/filesender).

6.8 Számítógépek üzemeltetésével, felhasználásával kapcsolatos szabályok

(1) A hálózatba kapcsolt számítógépeken csak az Egyetem céljaival (oktatás, kutatás, betegellátás) szorosan kapcsolatos tevékenységek végezhetők.
(2) Az egyetemi számítógépek rendszeradminisztrációs feladatait az üzemeltetéssel megbízott személy üzemelteti. Az operációs rendszer állományai az ő felügyelete alá tartoznak, azokért, valamint a gép rendeltetésszerű működéséért ő a felelős.
(3) A felhasználó felelős a tevékenységéért, fájljainak tartalmáért.
(4) A hálózatot üzemeltető személy az üzemeltetéssel kapcsolatban
a) bármely felhasználó adatait, tevékenységét ellenőrizheti. A felhasználók hálózat használata során keletkezett személyes adatai megismerésére az Információbiztonsági szabályzat és az adatkezelési szabályzat az irányadó;
b) a hálózat forgalmát monitorozhatja, azonban az így tudomására jutott adatokat csak a jelen szabályzat szerinti célok elérése érdekében és az adatvédelmi vagy egyéb jogszabályokban meghatározott módon és terjedelemben használhatja fel.
(5) Az IFIG munkatársai hibaelhárítás, hibakeresés céljaira a hálózatra kapcsolt összes számítógépet igénybe vehetik, azonban:
a) az üzemeltető, az informatikai felelős (helyi informatikus, rendszergazda) tudta és engedélye nélkül nem változtathatják meg sem a szoftver, sem a hardver konfigurációt;
b) a felhasználók adataiba nem tekinthetnek bele.
(6) Az IFIG által üzemeltetett gépek, szolgáltatások esetén a felhasználás rendjét, a jogosult felhasználók körét az IFIG vezetője az általa kijelölt rendszergazdákkal konzultálva határozza meg.
(7) Az Egyetem informatikai hálózatán üzemelő egyéb számítógépek felhasználásának rendjét, a használatra jogosultak körét az adott szervezeti egység vezetője határozza meg.

6.9 A felhasználók tájékoztatása

(1) Az IFIG köteles az érintett informatikusokat értesíteni minden nagyobb hálózati- és rendszerhibáról.
(2) A hálózati forgalmat befolyásoló tervezett karbantartásokról az érintetteket előzetesen kell értesíteni.
(3) Az értesítés a karbantartás tervezett időpontja előtt legkésőbb 72 órával elektronikus tájékoztatásával történik (levelező lista, honlap).
(4) Az egyetem egészét érintő karbantartás esetén az értesítés legkésőbb egy héttel a tervezett időpont előtt történik.

(5) A tervezett karbantartás halasztását az érintettek indokolt esetben az IFIG vezetőjénél írásban (levélben, faxon, e-mailen) kérhetik, de az értesítést követő 72 órán túl (munkanapokat tekintve) már csak az esetlegesen felmerülő költségek vállalása mellett.

(6) Az értesítés az esemény súlyától és kiterjedésétől függően történhet:

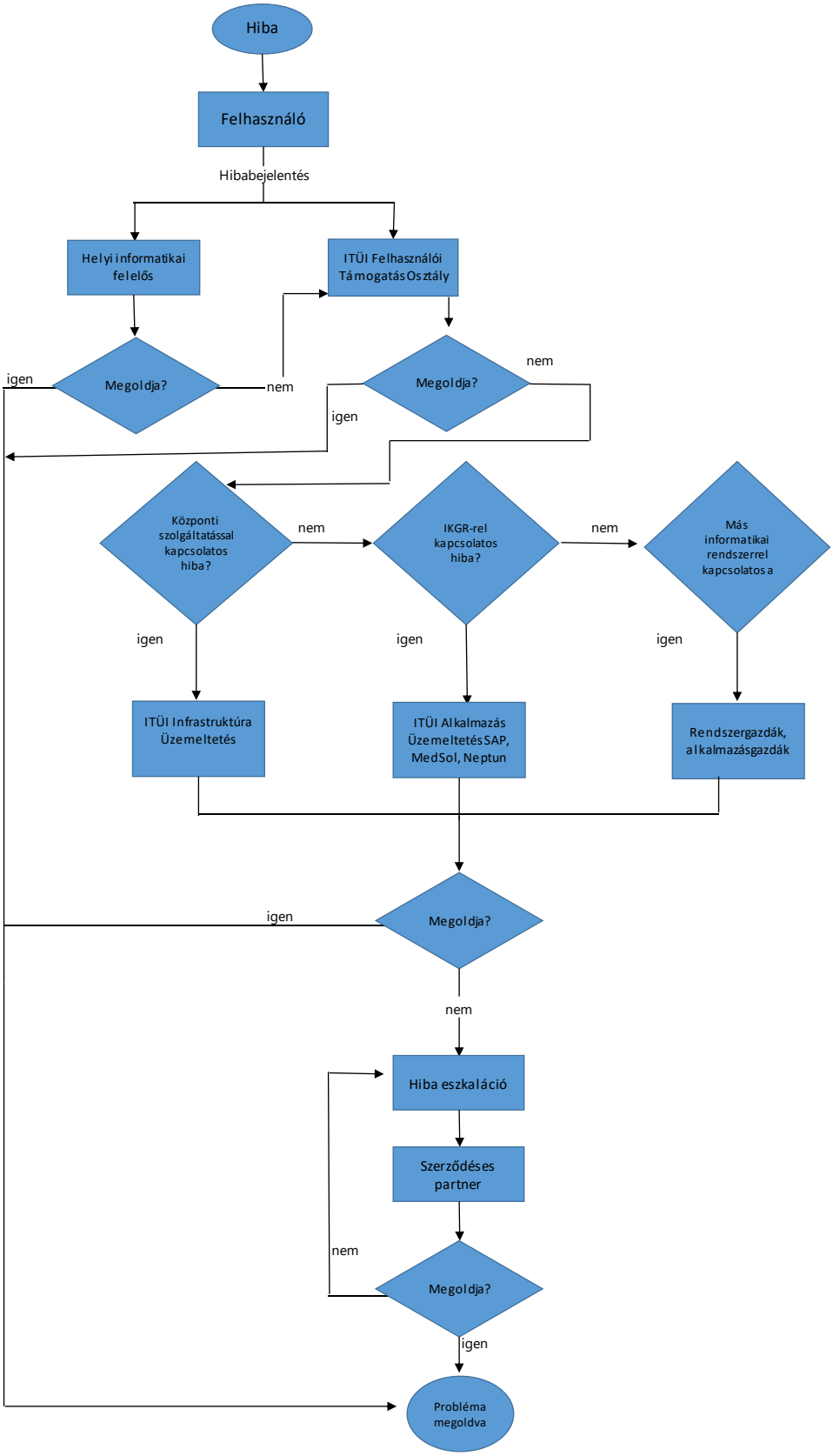
a) elektronikus úton,
b) IFIG internetes honlapján,
c) műszaki főigazgatói tájékoztatóban,
d) rektori/kancellári tájékoztatóban.

(7) Az értesítés módját az IFIG vezetője határozza meg.

7. MELLÉKLETEK:

1. sz. melléklet: Egyetemi, kari/intézeti hibakezelési folyamata
2. sz. melléklet: Ellenőrzési nyomvonal
3. számú melléklet: Jogosultságkérő űrlap – formanyomtatványtárból érhető el
4. számú melléklet: Publikus IP cím igénylő űrlap - formanyomtatványtárból érhető el

1. sz. melléklet: Egyetemi, kari/intézeti hibakezelési folyamata



2. sz. melléklet: Ellenőrzési nyomvonal

	folyamat lépései	**előkészítés lépései**	**felelősségi szintek**					**folyamat eredményeként keletkezett dokumentum**
			feladatgazda	**ellenőrző**	**ellenőrzés módja**	**jóváhagyó**	**jóváhagyás módja**	
1.	Támogatási folyamatok ellenőrzése: Hibabejelentő rendszer nyitott ügyek kontrollja	Hibabejelentő rendszer lekérdezések lefuttatása	IFIG osztályvezetők	IFIG osztályvezetők	egyedi (megoldatlan, lezáratlan) ügyek kezelése	IFIG főigazgató	tájékoztatás	a nyitott Hibabejelentő rendszer ügyekre vonatkozó rendszeres statisztikák
2	Támogatási folyamatok ellenőrzése: a szállítók felé nyitott ügyek kontrollja	SAP és MedSolution	alkalmazás üzemeltetés ov	alkalmazás üzemeltetés ov.	egyedi (megoldatlan, lezáratlan) ügyek kezelése	IFIG főigazgató	tájékoztatás	a nyitott ügyekre vonatkozó rendszeres statisztikák
3	Üzemeltetési paraméterek ellenőrzése	naplófájl elővevése	rendszergazda	infrastruktúra üzemeltetési ov	naplófájlok ellenőrzése	infrastruktúra üzemeltetési ov	tájékoztatás	naprakész nyilvántartás
5	Mentések ellenőrzése	naplófájl elővevése	rendszergazda	infrastruktúra üzemeltetési ov	naplófájlok ellenőrzése	infrastruktúra üzemeltetési ov	tájékoztatás	naprakész nyilvántartás
6	Informatikai incidensek elemzése	eseti vizsgálat	érintett rendszergazda	érintett ov	összes rendelkezésre álló információ mérlegelése	IFIG főigazgató	tájékoztatás	incides jelentés, rendelkezésre állási mutatók frissítése

ov.: osztályvezető

n.é.: nem értelmezhető

Ellenőrzési módok: beszámoltatás, jóváhagyás, egyeztetési