

AZ EÖTVÖS LORÁND TUDOMÁNYEGYETEM

INFORMATIKAI SZABÁLYZATA

2007.

Tartalom

1	Az Informatikai Szabályzat (IT-Sz) kiadásának célja, hatálya, szerkezete	- 4 -
2	A kiadás dátuma, érvényessége.....	- 4 -
3	A kötelező felülvizsgálat (revízió) időpontja	- 4 -
4	Kapcsolódó szabályozások (hivatkozások).....	- 4 -
5	Általános rendelkezések.....	- 5 -
5.1	Az Intézmény átfogó informatikai menedzsmentje	- 5 -
5.2	Feladat-, felelősség- és hatáskörök az informatikai biztonság területén	- 5 -
5.3	Jogszabályi, törvényességi megfelelés.....	- 5 -
5.4	IT rendszerek biztonsági osztályai, besorolás	- 5 -
5.4.1	Kritikus rendszerek (A).....	- 5 -
5.4.2	Kiemelt rendszerek (B)	- 6 -
5.4.3	Normál rendszerek (C).....	- 6 -
5.4.4	Egyéb rendszerek (D).....	- 6 -
5.5	Az IT-SZ hozzáféréseinek általános szabályai	- 6 -
6	Az IT-SZ Változásmenedzsmentje.....	- 6 -
7	Informatikai biztonsági követelmények az IT rendszerek szállítási szerződéseiben (beszállítók)	- 6 -
8	Az IT-rendszerek biztonsági ellenőrzése	- 7 -
9	Szolgáltatásszint menedzsment	- 7 -
9.1	A szolgáltatásszint menedzsment folyamata.....	- 7 -
9.2	A szolgáltatási megállapodások (SLA) tartalma.....	- 7 -
9.2.1	Megfigyelés, jelentés és áttekintés (felülvizsgálat)	- 9 -
9.3	Ügyfélszolgálat/Incidenskezelés.....	- 9 -
9.3.1	Incidens naplózás és kezelés	- 9 -
9.3.2	Ügyfélszolgálat (Service Desk) opciók és eljárások	- 9 -
9.3.3	Incidens osztályozás és prioritás hozzárendelés	- 9 -
9.4	Problémakezelés	- 10 -
9.4.1	Incidens, probléma és az ismert hiba kezelése	- 10 -
9.4.2	Trend-azonosítás	- 10 -
9.4.3	Probléma megelőzés.....	- 10 -
9.5	Konfigurációkezelés	- 10 -
9.5.1	Alapelvek és terminológia.....	- 10 -
9.5.2	A konfigurációkezelés adatbázisa	- 11 -
9.6	Változáskezelés.....	- 11 -
9.6.1	Központosított változás-felügyelet	- 11 -
9.7	Kiadáskezelés (új szolgáltatás indítása).....	- 11 -
9.7.1	Terítés és implementáció.....	- 12 -
9.7.2	A hiteles szoftver tár	- 12 -
9.7.3	Licencek kezelése.....	- 12 -
9.8	IT szolgáltatásfolytonosság biztosítása.....	- 12 -
9.8.1	Kockázatkezelés	- 12 -
9.8.2	Üzleti (működési) hatáselemzés.....	- 12 -
9.8.3	Vészhelyzeti opciók és az IT szolgáltatásfolytonossági terv.....	- 13 -
9.9	Rendelésre-állás biztosítása.....	- 13 -
9.9.1	Rendelésre-állás, megbízhatóság, szervizelhetőség szintjei	- 13 -
9.9.2	Karbantarthatóság, biztonság szintjei	- 13 -
9.9.3	A magas szintű rendelkezésre-állás tervezése	- 13 -
9.10	Pénzügyi irányítás.....	- 13 -
9.10.1	Költségvetés	- 13 -
9.10.2	Informatikai számvitel.....	- 14 -
9.10.3	Költségterhelési opciók.....	- 14 -
9.11	Kapacitáskezelés	- 14 -
9.11.1	Kapacitástervezés	- 14 -
9.11.2	A kapacitásterv.....	- 14 -
9.11.3	A kapacitáskezelés eleme	- 15 -
10	Fogalmak, rövidítések.....	- 15 -
11	Mellékletek	- 19 -
11.1	Egyszerűsített Szolgáltatási Katalógus	- 19 -
11.2	IT-SZ változáskezelési lap.....	- 20 -

11.3	IIG fórumainak elérhetősége.....	- 21 -
11.4	Felhasználói nyilatkozat.....	- 22 -
11.5	ÜZEMELTETÉSI DOKUMENTÁCIÓ.....	- 23 -

1 Az Informatikai Szabályzat (IT-Sz) kiadásának célja, hatálya, szerkezete

Az informatikai szabályzat célja az egyetemen folyó oktató-, kutató- fejlesztőmunka támogatása, a tanulás, információ szerzés elősegítése, a kapcsolatteremtés- és tartás új lehetőségeinek valamint az információ szabad áramlásának informatikai eszközökkel történő biztosítása.

A szabályzat „informatikai szolgáltatásnak” határoz meg minden olyan, informatikai rendszerhez történő, definiált és dokumentált hozzáférési, felhasználási lehetőséget, amelyet a rendszer üzemeltetői a felhasználók számára elérhetővé tesznek.

Az informatikai szabályzat az intézmény informatikai szolgáltatásainak kialakítását, üzemeltetését, igénybevételét és ellenőrzési lehetőségeit szabályozza. A szabályzat meghatározza az eszközök használatának módját, feltételeit, kitér a jogi és etikai kérdésekre is. Jelen szabályzat mindenkire nézve kötelező, aki használja az ELTE informatikai szolgáltatásait illetőleg infrastruktúráját, számítógép-hálózatát, annak berendezéseit (későbbiekben felhasználók). Az előbbieknek megfelelően a szabályzat személyi hatálya kiterjed az ELTE összes hallgatójára és dolgozójára, aki oktatási, kutatási, tudományos vagy az intézmény adminisztrációs feladataihoz az ELTE számítógép-hálózatát és eszközeit használja. Ha az intézmény harmadik félnek is lehetőséget biztosít hálózatának használatára, akkor harmadik félre nézve is kötelező a szabályzatban foglaltakat betartani.

A szabályzat alapszerkezete követi az ITIL (IT Infrastructure Library) de facto IT szolgáltatásirányítási szabvány szerkezetét. Ennek célja, hogy az ELTE IIG IT szolgáltatásaival kapcsolatos szolgáltatói szemléletmódot mind felhasználói mind szolgáltatói oldalon erősítse.

A mindenkori szabályzat felhasználók számára készült kivonata az Informatikai Házirend.

2 A kiadás dátuma, érvényessége

Jelen szabályzat az ELTE Szenátusa által történő jóváhagyás pillanatában lép hatályba. A szabályzat jelen változata mindaddig érvényesnek tekintendő, amíg annak egy új változatát az Egyetemi Szenátus jóvá nem hagyja.

3 A kötelező felülvizsgálat (revízió) időpontja

A szabályzat felülvizsgálatára az alábbiak szerint kerül sor:

- évente egy alkalommal (az esedékes következő felülvizsgálati időpontot a dokumentum lezárásakor kell kijelölni.)
- minden olyan esetben, amikor a szabályzatban leírtakban jelentős változás(ok) történnek.

Jelen szabályzat hivatkozott mellékletei IIG Igazgatói utasítás alapján módosíthatóak.

4 Kapcsolódó szabályozások (hivatkozások)

- ELTE Szervezeti és Működési Szabályzata (továbbiakban ELTE SZMSZ)
- Munkaköri leírások
- Hallgatók jogállását leíró dokumentumok

5 Általános rendelkezések

5.1 Az Intézmény átfogó informatikai menedzsmentje

Az Intézmény informatikai tevékenységének szabályozását és koordinálását a Gazdasági és Műszaki Főigazgatóság Informatikai Igazgatósága (továbbiakban IIG) látja el.

5.2 Feladat-, felelősség- és hatáskörök az informatikai biztonság területén

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 (a továbbiakban szolgáltató), illetve az üzemeltetésért felelős szervezeti egységet (a továbbiakban szolgáltató egység) az adott szolgáltatás SLA-jában kell megnevezni.

Az informatikai szolgáltatások szakmai felügyeletét az IIG igazgatója mellett működő szolgáltatásmenedzser látja el.

A szolgáltatásmenedzser felelős a szolgáltató és a szolgáltatás igénybevevője között a szolgáltatás tartalmának és egyéb paramétereinek egyeztetéséért, a megállapodás betartásának ellenőrzéséért.

Az IIG igazgatója jogosult az egyes szolgáltatások IT-SZ megfeleléségének ellenőrzésére.

5.3 Jogszabályi, törvényességi megfeleléség

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

A szolgáltatás üzemeltetője a jogszabályokban meghatározott nyilvántartásokat vezetni köteles.

Törvényes megkeresés alapján, a vonatkozó jogszabályi kereteknek megfelelően az ELTE minden, a bűncselekmény elkövetésének gyanúja alá eső felhasználó adatait, valamint naplózott adatokat a nyomozóhatóságnak kiszolgáltatja.

A szolgáltatások igénybevevőit a szabályzatban leírtak megsértése esetén az alábbi szankciók sújthatják:

- szolgáltatás megtagadás (kizárás a szolgáltatásból)
- a szolgáltatás korlátozása
- az okozott anyagi kár megtérítése
- polgári vagy büntető feljelentés megtétele

A szolgáltatásokat igénybe vevők bármilyen szankcionálása csak akkor történhet meg, ha az üzemeltető dokumentálta a szankció elrendelését kiváltó eseményt, incidenst. Ennek felelőse a szolgáltatást nyújtó szervezeti egység vezetője.

5.4 IT rendszerek biztonsági osztályai, besorolás

5.4.1 Kritikus rendszerek (A)

Az intézmény működése szempontjából kritikus, az intézmény egészére kiterjedő rendszerek, amelyek szenzitív, illetve személyes adatokat tartalmaznak. Adatvédelmi szempontból kiemelt védelmet igényelnek.

- Bér- és Munkaügyi rendszer
- Gazdasági, ügyviteli rendszer
- Dokumentumkezelési rendszer

- Tanulmányi rendszer
- Központi levelező kiszolgálók
- Központi tárhely-kiszolgálók
- Intézményi autentikációs rendszerek

5.4.2 Kiemelt rendszerek (B)

Az intézmény működése szempontjából kritikus rendszerek, amelyek elsősorban technikai jellegűek, a rajtuk tárolt adatok nem személyes jellegűek.

- Telekommunikációs hálózat
- Technológiai (environment, middleware) rendszerek
- Kommunikációs rendszerek

5.4.3 Normál rendszerek (C)

A vagy B kategóriába nem sorolt, a teljes intézmény napi működése szempontjából nem kritikus, illetőleg az intézménynek csak egyes részeire kiterjedő olyan rendszerek, amelyek indítása/üzemeltetése során központi felülvizsgálat történik, illetőleg teljes körű dokumentáció készül.

- Interaktív kiszolgáló szerverek
- Kutatói rendszerek
- HPC

5.4.4 Egyéb rendszerek (D)

Az előző három kategóriába nem sorolt rendszerek.

5.5 Az IT-SZ hozzáféréseinek általános szabályai

Az IT-SZ Főigazgatói előterjesztésben, Egyetemi Szenátusi határozatként lép életbe és ennek megfelelően teszik közzé, valamint az IIG web portálján elérhető, illetve letölthető.

6 Az IT-SZ Változásmenedzsmentje

Az IT-SZ-el kapcsolatos észrevételeket, változtatási javaslatokat az IIG igazgatójának címzett, a 2. mellékletben található változáskezelési lapon lehet benyújtani. A változtatási javaslatot az ELTE Informatikai Bizottságának véleményezése alapján a Szenátus hagyja jóvá. Az IIG igazgatója a szenátusi határozatot követő 8 napon belül írásban köteles tájékoztatni az indítványozót a javaslat vagy beadvány sorsáról. A szabályzat mellékleteinek módosítását az IIG igazgatója saját hatáskörben végzi konzultálva az érintett szervezeti egységek vezetőivel. A mellékletek IIG Igazgatói utasítások formájában készülnek és módosulnak.

7 Informatikai biztonsági követelmények az IT rendszerek szállítási szerződéseiben (beszállítók)

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

- Hatályos jogszabályoknak megfelelés
- Átadás / átvételi jegyzőkönyv vagy teljesítési igazolás (mint a szerződés melléklete)

- Kapcsolattartó neve és elérhetősége
- Technikai feltételek
- Támogatási / garanciális feltételek
- A beszállítás (projekt) menedzsmentje
- Jogi nyilatkozat (tulajdonjog, szoftver használati jog, stb.)
- Biztonsági kérdések
- Felelősségi körök elhatárolása

8 Az IT-rendszerek biztonsági ellenőrzése

Az IIG igazgatója felelős azért, hogy az A besorolású IT-rendszerek teljes körű belső biztonsági felülvizsgálata dokumentált módon (belső felülvizsgálati jelentés) legalább évente megtörténjen, és érdemi változás esetén kerüljön sor külső, harmadik fél általi felülvizsgálatra. A felülvizsgálatok eredményei alapján az IIG igazgatója rendel el javító, helyesbítő és megelőző intézkedéseket, melyeket mindig a soron következő belső vagy külső, harmadik fél általi felülvizsgálat során kell dokumentált módon visszaellenőrizni.

9 Szolgáltatásszint menedzsment

9.1 A szolgáltatásszint menedzsment folyamata

„A” és „B” kategóriájú rendszer csak az IIG által vagy engedélyével üzemeltethető. A szolgáltatás tartalmára a szolgáltatási megállapodásban az üzemeltető szervezeti egység vezetője tesz javaslatot, a szolgáltatás indíthatóságáról a megállapodási javaslat alapján az IIG igazgatója dönt. Elutasító döntés esetén a javaslattevő 15 napon belül felszólamlással élhet az Informatikai Bizottság elnökénél. Ilyen esetekben az Informatikai Bizottság véleménye alapján a végleges döntést az egyetem rektora hozza meg.

„A” és „B” kategóriába nem tartozó rendszer esetében a rendszert üzemeltető szervezeti egység vezetője kérheti a szolgáltatás előző módon történő jóváhagyását. Az így jóváhagyott rendszerek „C” kategóriájúnak minősülnek.

A központilag jóváhagyott szolgáltatásokat az IIG honlapján közzéteszi. Ezek a szolgáltatások („A”, „B” és „C” kategória) az egyetem hivatalosan auditált szolgáltatásainak tekintendők.

9.2 A szolgáltatási megállapodások (SLA) tartalma

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

- Szolgáltatás Neve (egyedi megnevezés)
- SLA Verziószám
- Lezárás dátuma (Az SLA lezárásának dátuma)
- Igénybe vevő és szolgáltató, jóváhagyó (A szolgáltatás Igénybevevője, vagy ezek képviselője, illetve a szolgáltató, illetve képviselője mellett az IIG részéről a jóváhagyó megnevezése)
- Rövid szolgáltatás leírás / összegzés (Pár mondatban, röviden összefoglalva a szolgáltatás célját, tartalmát.)
- Érvényesség / megszűnés
 - o (általában évente felülvizsgálendő, automatikusan meghosszabbításra kerül)
- Aláírások
 - o név pozíció dátum

- Szolgáltatás leírása (részletes, technikai leírás)
 - kulcs funkciók
 - kiterjedés, hatókör
 - elhelyezés (fizikai elhelyezés, helyiség, eszközök, szerver, stb.)
 - kik vehetik igénybe
 - prioritás (A-D) (IT-SZ 5.4 pontja alapján.)
- Szolgáltatási időszak
 - (pl.: 7x24; 8-16 munkanapokon, stb.)
- 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.)
- A szolgáltatással kapcsolatos tájékoztatás módja
- Karbantartási időszakok (éves szinten megadva, pl.: minden hónap első hétfő 21-23h.)
- Rendelkezésre állás (%)
 - Milyen mérőszámokkal mérhető
 - Hogyan történik a mérése
- Megbízhatóság
 - MTBF
 - Milyen mérőszámokkal mérhető
 - Hogyan történik a mérése
- Támogatás
 - Hogyan érhető el (Mi a teendő hiba észlelése esetén?)
 - Milyen támogatást nyújt
 - Mi a teendő támogatási időszakon kívül (pl.: hétvégén, éjjel, stb.)
- Incidens-kezelés
 - 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
- Teljesítmény / minőség
 - Optimális teljesítményadatok (pl.: elérési idő, válaszidő, ami értelmezhető az adott szolgáltatás esetében, stb.)
- funkcionalitás (ha értelmezhető)
 - hány és milyen jellegű hiba tolerálható a szolgáltatáson belül
- Változáskezelési eljárások
 - Normál esetben hivatkozás a szervezet változáskezelési eljárására. Itt csak a sajátosságokat / kivételeket kell említeni.
- IT üzletmenet folytonosság
 - A DRP/BCP –re hivatkozás. Itt csak a sajátosságokat / kivételeket kell említeni.
- Biztonság
 - A ITBSZ –re hivatkozás. Itt csak a sajátosságokat / kivételeket kell említeni. (Pl.: egyedi/kiemelt biztonsági kockázat, illetve ennek kezelése.)
- Felülvizsgálat ideje / időszak (Az SLA felülvizsgálatára, módosítására minden a szolgáltatásban, illetve a szolgáltatás nyújtásának feltételeiben bekövetkezett érdemi változás esetében szükség van.)

- Szójegyzék (Azok a technikai, speciális kifejezések, amelyek szerepelnek az SLA-ban és magyarázatra szorulnak.)

9.2.1 Megfigyelés, jelentés és áttekintés (felülvizsgálat)

Az előre ütemezett (tervezett) szolgáltatás-kieséseket illetve a meghibásodás miatti kieséseket az SLA-ban meghatározott módon publikálni kell, ennek felelőse az adott szolgáltatást nyújtó szervezeti egység vezetője.

Az SLA-kban megadott szolgáltatási kulcsparaméterek monitorozásért az adott szolgáltatást nyújtó szervezeti egység vezetője a felelős.

Az SLA-k tartalmazzák az adott szolgáltatás monitorozási feltételeit. Az SLA-kban rögzített méréseket és jelentéseket az IIG igazgatója illetőleg a szolgáltatás üzemeltetője áttekinti, és a fejlesztési tennivalók (ötletek) közé felveszi a teljesítési problémákat mutató területeket. Lásd költségvetés tervezési fejezetet (9.10.1)!

9.3 Ügyfélszolgálat/Incidenskezelés

9.3.1 Incidens naplózás és kezelés

Támogatás (support): Az adott szolgáltatás SLA-ja alapján, az abban leírtaknak megfelelően nyújtja a szolgáltató.

Incidens-kezelés, naplózás: Az adott szolgáltatás SLA-ja alapján, az abban leírtaknak megfelelően végzi a szolgáltató.

9.3.2 Ügyfélszolgálat (Service Desk) opciók és eljárások

Központi ügyfélszolgálaton az A és B kategóriájú rendszerekre vonatkozó incidens bejelentése csak írásban történhet (papír, e-mail vagy web űrlap útján) az incidens típustól függő kötelező és opcionális adatok megadásával. A bejelentés aktuális módját és a megadandó adatokat a szolgáltatás SLA-ja tartalmazza, a szolgáltató és az IIG igazgatója jóváhagyásával az IIG weblapján hozzáférhető.

Az ügyfélszolgálatnak minden bejelentést regisztrálnia kell és ennek tényéről (egy, az esetre egyedi hivatkozást lehetővé tevő azonosítóval ellátva) értesítenie kell a bejelentőt. Az ügy lezárása esetén annak tényéről és az ezzel kapcsolatos eredményekről a bejelentőt értesíteni kell.

A központi ügyfélszolgálat csak hatáskörébe tartozó rendszerekkel összefüggő műszaki problémákat old meg. Nem vesz részt harmadik féllel felmerült vitás kérdések rendezésében, nem lát el jogi képviseletet sem felperesi, sem alperesi oldalon.

9.3.3 Incidens osztályozás és prioritás hozzárendelés

A bejelentett incidensek kezelésére a rendszer besorolásától (A-D) függően prioritizálva kerül sor. A prioritizálás az ügyfélszolgálat feladata és felelőssége. Több incidens fellépésekor a magasabb prioritású incidens megoldása elsőbbséget élvez.

9.4 Problémakezelés

9.4.1 Incidens, probléma és az ismert hiba kezelése

Az ezzel a tevékenységgel az IIG igazgatója által megbízott szervezeti egység vagy munkacsoport automatikus incidens és/vagy probléma felderítő rendszereket üzemeltethet az SLA-k alapján, és ennek megfelelő szankciókkal élhet az 5.3 pont szerint.

A szolgáltatás incidenseket és problémákat az üzemeltető személyzet, a felhasználók jelezhetik, illetve ahol erre lehetőség van és kiépített felderítő rendszer üzemel, ott automatikus jelzés is történhet.

A visszatérő, több incidens kiváltó okaként megjelenő problémáknak a probléma adatbázisba felvétele manuális, amit az üzemeltető személyzet vagy az ügyfélszolgálat végez.

Az ismert hibák kiszűrése a hibafelvétel során történik.

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

9.4.2 Trend-azonosítás

Az SLA-kban előírt teljesítmény-mutatók figyelése során a szolgáltatónál statisztikai értelemben vett idősorok jönnek létre, melyek elemzése az adott szolgáltatást nyújtó szervezeti egység vezetőjének a feladata. Az ilyen módon képződött adatokat a szolgáltató illetőleg a szolgáltató egység vezetője felhasználja a fejlesztési irányok és projektek kijelölésekor.

9.4.3 Probléma megelőzés

Az egyes szolgáltatások üzemeltetőinek nem csak reaktív, hanem preventív intézkedéseket is kell fogantatosítaniuk a szolgáltatás zavartalan működtetésének érdekében.

Ezek lehetnek általános és az adott szolgáltatásra speciálisan jellemző feladatok, például

- Igény szerinti újraindítás, reset
- A javítócsomagok, patchek, fixek telepítése
- A jelszavak és hozzáférési kódok rendszeres cseréje
- A naplóállományok rendszeres kiértékelése

Az IIG biztosíthatja a probléma-megelőzés alap infrastruktúráját, de az ELTE egyes szervezeti egységei jogosultak további megelőző intézkedéseket végrehajtani, azonban az intézkedéstervet kötelesek előzőleg bejelenteni az IIG igazgatójának, akinek a jóváhagyása után az intézkedések fogantatosíthatóak.

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

A probléma megelőzés érdekében az IIG évente konzultációt szervez a nem IIG-s szervezeti egységek üzemeltető személyzete részére.

9.5 Konfigurációkezelés

9.5.1 Alapelvek és terminológia

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

Az üzemeltetői dokumentáció vázlata, ami tartalmazza a kötelező elemeket is, a mellékletben megtalálható.

9.5.2 A konfigurációkezelés adatbázisa

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 változó komponensek egyértelmű azonosítását lehetővé tevő adatok
- a változás szükségességének indokai
- a tesztelésre vonatkozó adatok
- az aktuális visszaállási teendőket tartalmazó hivatkozást is tartalmaznia kell a konfigurációs bejegyzésnek.

9.6 Változáskezelés

9.6.1 Központosított változás-felügyelet

Az A B és C besorolású informatikai rendszerek esetében az IIG központi változás-felügyeletet gyakorol.

9.6.1.1 Változáskezelési folyamatok

A központi változás-felügyelet menete:

- „A”, „B” és „C” kategóriájú rendszer esetén a szolgáltatás üzemeltetője a változtatás megkezdése előtt engedélyeztetni a megvalósítandó hardver és szoftver konfigurációt az adott terület illetékes szakértőjével.
- A területi szakértőket (területenként) az IIG igazgatója jelöli ki. A területi szakértő személye esetileg egybeeshet a szolgáltatás üzemeltetőjével.
- Az engedélyezett változtatásokat (Hw, Sw, adatbázis, stb.) a szolgáltatás üzemeltetője az üzemeltetési leírásban foglaltak alapján végrehajthatja, sikeres végrehajtás esetén a rendszer leírásában azt dokumentálja.

9.6.1.2 Szerepkörök és felelősségek

- A szolgáltatás üzemeltetője teljes felelősséggel tartozik minden olyan beavatkozásért, amit a felelős területi szakértő nem engedélyezett, illetve amelyek esetében a rendszer-üzemeltetési leírása nem lett betartva.
- A területi szakértő felelősséggel tartozik a hardver vagy szoftver konfigurációk engedélyezéséért, abban az esetben is, ha ezek működőképességéről nem győződött meg.
- Az IIG igazgatója tartozik felelősséggel azon területekért, amelyekre területi szakértőt nem jelölt ki.

9.7 Kiadáskezelés (új szolgáltatás indítása)

Az auditált rendszerek megvalósítását és dokumentálását, valamint a szolgáltatás tesztelését az IIG szolgáltatás-menedzsere ellenőrzi. A sikeres tesztüzem után a szolgáltatás üzembe állítását az IIG igazgatója engedélyezi.

Az A B és C kategóriás rendszerek esetében a szolgáltatás elindításának feltétele, hogy az IIG igazgatója jóváhagyja az SLA-t, az üzemeltetési dokumentációt, a rendszerkonfigurációt és a változáskezelési folyamatot. Vitás esetekben a 9.1 pontban foglaltaknak megfelelően kell eljárni.

9.7.1 Terítés és implementáció

Minden általa működtetett szolgáltatás esetén az IIG web portálja tartalmazza azon hardver és szoftver elemek (kliensek) listáját és elérhetőségét, amik a szolgáltatás igénybevételéhez szükségesek.

Az IIG szoftver disztribúciós szolgáltatása közvetlen program és installációs leírás letöltést is lehetővé tesz. Lehetőség szerint törekedni kell ennek a szolgáltatásnak a használatára.

9.7.2 A hiteles szoftver tár

Az IIG szoftverdisztribúciós munkatársa központilag hozzáférhető módon létrehozza és karbantartja a központilag beszerzett szoftverek eredeti példányainak és az installációs csomagjainak tárá. Amennyiben a beszerzett szoftver korlátozott hozzáférésű, meg kell határozni a hozzáféréssel rendelkezők körét.

A szoftverdisztribúciós munkatárs felelőssége:

- legfrissebb verziók letöltése, a csomagok frissítése
- patchek, hotfixek letöltése, közzététele
- csomagok vírusellenőrzése
- hozzáférési jogosultságok kezelése

9.7.3 Licencek kezelése

Minden szolgáltató rendszer esetében a törvényes működés bizonyítását lehetővé tevő licencek tárolása az üzemeltető szervezeti egység vezetőjének kötelezettsége.

Azon programok esetében, amikre az egyetem campus licence-szel vagy egyetemi korlátozott licence-szel rendelkezik, az IIG software disztribúcióval foglalkozó munkacsoport vezetője végzi a licencek tárolását és a kiadás elbírálását.

Az elbírálás és technikai kiadás munkáját termékenként más munkatársakra is átruházhatja.

9.8 IT szolgáltatásfolytonosság biztosítása

9.8.1 Kockázatkezelés

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 tett hatásait tartalmazza. Külön kell kezelni a szolgáltatás elérhetetlenségéből, illetőleg az adatbázis sérüléséből származó hatásokat. A kockázatelemzési dokumentum előállítása és karbantartása a szolgáltatás üzemeltetőjének a feladata.

9.8.2 Üzleti (működési) hatáselemzés

Minden „A” illetve „B” kockázati besorolású szolgáltató rendszer esetében a kockázatelemzési dokumentum kitér arra, hogy milyen hatással jár az adott rendszer vagy szolgáltatás kiesése az ELTE működési folyamataira.

A dokumentum előállítása és karbantartása a szolgáltatás üzemeltetőjének a feladata.

9.8.3 Vészhelyzeti opciók és az IT szolgáltatásfolytonossági terv

A szolgáltató rendszerek üzemeltetési leírásának tartalmaznia kell az alábbi teendőket (a szolgáltatásfolytonossági tervet):

- milyen helyettesítési lehetőségek (műszaki, technológiai és szervezési megoldások) vannak az adott szolgáltatás kiesése esetén (vészhelyzet)
- milyen intézkedéseket kell megtenni a működés folytonosságának fenntartása érdekében.
- Kik az intézkedésre jogosultak
- Kiket kell értesíteni az intézkedésekről

A dokumentum előállítása és karbantartása a szolgáltatás üzemeltetőjének a feladata.

9.9 Rendelkezésre-állás biztosítása

9.9.1 Rendelkezésre-állás, megbízhatóság, szervizelhetőség szintjei

Az egyetem működése szempontjából kritikus szolgáltatások (A és B kategóriájú rendszerek) esetében az adott területért felelős felső szintű vezető jóváhagyásával az IIG igazgatója határozza meg azt a rendelkezésre állási intervallumot, amiben a szolgáltatásnak elérhetőnek kell lennie.

9.9.2 Karbantarthatóság, biztonság szintjei

Az adott szolgáltatás üzemeltetőinek a szolgáltatás aktuális üzemeltetői dokumentációjában fel kell tüntetni azon műszaki megoldásokat, amik a szolgáltatás meghatározott elérési paramétereit hivatottak biztosítani (pl. redundanciát, failover-t biztosító rendszerkomponensek). Az üzemeltetőknek a szolgáltatás következő éves fejlesztési tervében rögzíteniük kell az elavult, nem szervizelhető komponensek a cseréjére vonatkozó javaslatot.

9.9.3 A magas szintű rendelkezésre-állás tervezése

A és B kategóriájú rendszerek esetében a rendelkezésre állás biztosítását tervezni kell. A terv elkészítéséért a szolgáltató egység vezetője, a tervezés ellenőrzéséért az IIG igazgatója felelős.

9.10 Pénzügyi irányítás

Az IIG felelősségi körébe eső szolgáltatások esetében a pénzügyi tervezés és irányítás éves ciklusa:

- Technikai, műszaki tervezés: (a pénzügyi évet megelőző október-november, osztályvezetők)
- Belső költségvetés és éves projektterv összeállítása: (november-december, osztályvezetői kollégium)
- Egyetemi szintű költségvetési fordulók: (IIG igazgatója, tárgyévi januárjában)
- Költségvetés és projekttervek véglegesítése: (osztályvezetői kollégium, tárgyévi február-március)

9.10.1 Költségvetés

Az IIG adott szolgáltatását üzemeltető csoport év végén beterjeszti azon tételeket összegekkel ellátva, amelyek a szolgáltatás fenntartásához – a fejlesztési terv szolgáltatásra vonatkozó részét figyelembe véve – szükségesek.

A következő évben indítandó, új szolgáltatások esetén az eljárás megegyezik a fentiekkel. Ezek a tételek összegezve adják az IIG következő éves fejlesztési költségvetését. A fix üzemeltetési költségeket ehhez szolgáltatásarányosan (pl. karbantartási szerződések) hozzá kell adni, ez adja a teljes költségvetést.

9.10.2 Informatikai számvitel

Az egyes IIG fejlesztési projektek projekt alapú gazdálkodásért a megvalósítást végző szervezeti egységek vezetői a felelősek. Ők készítik a projekt költségvetést, az időszaki forrás-felhasználási jelentéseket, és zárják a projekteket műszaki és pénzügyi értelemben.

Az amortizáció elszámolási módját, mértékét a mindenkori gazdasági szabályzatok határozzák meg.

Az egyes beszerzések csoportosítása, hozzárendelése a rendszerekhez úgy történik, hogy az osztályvezetők ismerik el az egyes szállítói számlák és szállítólevelek jogosságát, és az IIG igazgatója hagyja ezeket jóvá.

9.10.3 Költségterhelési opciók

Az ELTE az informatikai és távközlési szolgáltatók felé egykapus ügyintézés alkalmaz, tehát minden ilyen szolgáltatást az IIG rendel meg az ELTE nevében.

Ugyanígy tesz minden, az IIG saját hatáskörében üzemeltetett szolgáltatásaihoz kapcsolódó beszerzés esetében.

Ha a harmadik féltől megrendelt szolgáltatás nem IIG által nyújtott szolgáltatáshoz szükséges, akkor annak költségét az IIG a kérelmező szervezeti egységre továbbterheli.

Ennek elfogadásáról a megrendelő szervezeti egységnek költségvállalási nyilatkozatot kell aláírnia.

9.11 Kapacitáskezelés

Az IIG Igazgatója a felelős azért, hogy a felhasználóktól beérkező igények, a szolgáltatói környezet változása, a technikai fejlődés figyelembe vételével tervezze, és az elfogadott egyetemi költségvetés szerint biztosítsa az ELTE működéséhez szükséges IT- kapacitásokat.

9.11.1 Kapacitástervezés

A szolgáltatást biztosító rendszer várható terhelését az üzemeltető szervezeti egység vagy munkacsoport az eddigi használati trendek alapján évente előrejelzi a következő egy éves időtartamra.

9.11.2 A kapacitásterv

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.

9.11.3 A kapacitáskezelés eleme

Az IIG által üzemeltetett szolgáltatások esetében az üzemeltető osztály vezetője az adott szolgáltatás kapacitásterve alapján fejlesztési tervet készít, melyeket a következő évi költségvetés tervezetével együtt benyújt az IIG vezetőjének.

A kapacitástervek és a fejlesztési tervek elfogadásáról az IIG vezetője szolgáltatásonként külön, nyilvános döntést hoz.

10 Fogalmak, rövidítések

ELTE: Eötvös Loránd Tudományegyetem

IIG: Gazdasági és Műszaki Főigazgatóság Informatikai Igazgatósága

Ethernet hálózati kártya fizikai címe: A hálózati kártyára vonatkozó, annak gyártásakor rögzített hexadecimális 6 bájtos egyedi azonosító.

Fizikai IP-cím: A tartomány regisztráláskor az intézménynek juttatott A, B vagy C osztályú címtartomány egy eleme.

Virtuális IP-cím: Belső hálózaton (intraneten) található számítógépek egyedi hálózati azonosítója

Szellemi tulajdon: Az 1999. évi LXXVI. a szerzői jogról szóló törvény szerint a számítógépi programalkotás és a hozzá tartozó dokumentáció (a továbbiakban: szoftver) akár forráskódban, akár tárgykódban vagy bármilyen más formában rögzített minden fajtája ideértve a felhasználói programot és az operációs rendszert is – szerzői jogi védelem alá tartozik, ezért az ilyen művek engedély nélküli másolása törvénybe ütköző cselekedet.

Szoftver licencszerződés: Egy adott szoftver esetében a licencszerződés határozza meg a szerzői jog tulajdonosa által megengedett szoftverhasználat feltételeit. A szoftverhez adott licencszerződésre külön utalás történik a szoftver dokumentációjában, és/vagy a program indításakor megjelenő képernyőn. A szoftver ára tartalmazza a szoftver licencét, és megfizetése kötelezi a vevőt, hogy a szoftvert kizárólag a licencszerződésben leírt feltételek szerint használja.

Jogosulatlan másolás: A szoftver licencszerződés, amennyiben eltérően nem rendelkezik, a vevőnek csak egyetlen biztonsági másolat készítését engedélyezi, arra az esetre, ha az eredeti szoftver adathordozója meghibásodna vagy megsemmisülne. Az eredeti szoftver bármely további másolása jogosulatlan másolásnak minősül, és megsérti a szoftvert védő és használatát szabályozó licencszerződést, valamint a szerzői jogi törvényt.

Illegális szoftverhasználat: Az illegális szoftverhasználat azt jelenti, hogy valaki egy számítógépes programot jogosulatlanul másol le és használ, ezzel megsértve a szerzői jogi törvényt, valamint a szerzőnek a szoftver licenz-szerződésben leírt feltételeit. Aki szoftvert illegálisan használ, az a szerzői jogi törvény értelmében büntetőjogi törvénybe ütköző cselekedetet követ el.

Szoftvergazdálkodás: Szoftverlicenchez való hozzájárulás, szoftvernyilvántartás felfektetése és folyamatos vezetése

Felhasználó: az infrastruktúrát használó személy. Általában munkavállaló, de minden olyan személy, aki a cég által rendelkezésére bocsátott informatikai infrastruktúrát használja.

PC: gép: számítógép

Desktop PC: asztali számítógép

Notebook: mobil eszköz: hordozható számítógép.

Kiszolgáló/ Szerver: minden olyan számítógép vagy funkció, amely más számítógépeket szolgál ki.

Internet, net: a világméretű hálózat, amely sok számítógépet kapcsol össze.

Tűzfal, web-proxy, proxy: a számítógép(ek) felé kívülről kezdeményezett, illetve a számítógépről kifelé kezdeményezett kapcsolatokat szabályzó és megfigyelőeszközök.

Mail, email, e-mail, levél: az interneten vagy a belső hálózaton küldött elektronikuslevél.

Web: az internet egyik leggyakrabban használt szolgáltatása – az email mellett –, a http protokollon elérhető szolgáltatások halmaza.

Szoftver: a számítógépen használt programok és adatok.

Le- és feltöltés: valamely számítógépre vagy -ről történő adatátvitel. Általában az internet erőforrásai és egy felhasználói PC között zajlik.

Fájlcsere-lők, P2P, peer-to-peer: az interneten egyes felhasználók számítógépein megtalálható fájlok cseréjét lehetővé tevő szoftverek. Ezek általában nem ellenőrizhető tartalmak le- és feltöltését lehetővé tevő szoftverek. Nincs központi kiszolgáló, a gépek egymással cserélnek adatokat.

Instant messenger, IM, azonnali üzenetküldő, chat program: két külön PC-t akár a világ két távoli pontján lévő személy írásbeli kommunikációját lehetővé tevő szoftver. Egyes munkahelyeken használatuk a munka része, máshol csupán szórakozás, a barátokkal, ismerősökkel való kapcsolattartás módja. Léteznek központi kiszolgálóra csatlakozó IM kliensek (pl.: MSN), illetve helyi privát kiszolgálóra kapcsolható kliensek is.

Licensz: egy szoftver felhasználását szabályozó szerződés. Az illegálisan telepített szoftverek miatt valakinek felelősséget kell vállalnia. Ez alapesetben az adott eszköz gazdájára hárul, de tekintettel arra, hogy nem tudja minden pillanatban ellenőrizni, hogy ki mit telepít fel a gépére, e szabályzatban rögzítjük a személyes felelősséget is.

Sávszélesség: Az internet elérés egyik fő jellemzője az egy időegység alatt átvihető adatok mennyisége. Ez a jellemző arányos a sávszélesség nevű műszaki paraméterrel, ezért leegyszerűsítve így nevezzük az internet elérés gyorsaságát. Ez egy véges kapacitás, és adott pillanatban a felhasználók osztoznak rajta, ezért egyesek számára “lassú lehet az internet”, ha mások terhelik a vonalat.

BCP: Business Continuity Plan – Üzletmenet (működés) folytonossági terv az üzletmenet (működés) fenntartása érdekében teendő intézkedések összessége, ha az adott üzleti folyamat vagy alkalmazás végrehajtása, működtetése valamilyen természeti vagy ember által okozott katasztrófa miatt akadályokba ütközik.

DNS: Domain Name Service. Az internet neveket és címeket egymáshoz rendelő adatbázisa.

DRP: Disaster Recovery Plan – Katastrófa utáni helyreállítási terv magába foglalja az üzletmenet (működés) szempontjából kritikus adatok, hardver, és szoftver működésének újraindítását természeti vagy ember által okozott katasztrófák esetén.

intranet: az intézményen belüli hálózat, kívülről nem érhető el.

IP telefónia: olyan számítógép-hálózati alkalmazás, amely dedikált eszközök (készülék és központ) segítségével telefonszolgáltatást tesz lehetővé. Ez a hagyományos telefonközpontokat felváltó számítógépes rendszer.

HPC (High Performance Computing): Speciálisan nagy számítási igényű feladatokra tervezett számítógépes rendszer.

LDAP (Light Weight Directory Access Protocol): nyílt szabványú címtár struktúra leíró nyelv.

NAT (Network Address Translation): olyan IP címszolgáltatási mechanizmus, amely az Interneten nem címezhető logikai címek számára elérést biztosít. Ehhez program azonosító port felhasználása is megtörténik.

NIIF (Nemzeti Információs Infrastruktúra Fejlesztési Intézet országos hatáskörű szerv), amely a magyar felsőoktatás és a közintézmények számára komplex adathálózati, tartalmi és Internet szolgáltatást nyújt.

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

TCP (Transmission Control Protocol): Az IP csomagban szállított, kapcsolat orientált forgalom továbbítási mechanizmus.

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

UDP (User Datagram Protocol): Az IP csomagban szállított, kapcsolat nélküli forgalom továbbítási mechanizmus.

WiFi (Wireless Fidelity): olyan szabványos vezeték-nélküli adat-átviteli technika, amely az 1-54 Mbps-os tartományban működik. A szabad frekvenciatartományt használó rendszer átviteli sebessége nagymértékben függ a rádióhullámok terjedési környezetétől (akadályok, távolság). Legtöbb notebook, laptop, palmtop számítógép gyárilag rendelkezik ilyen kapcsolódási lehetőséggel

SLA: Service Level Agreement – Szolgáltatási szint megállapodás egy olyan írásos megállapodás, mely két fél között jön létre: a szolgáltató és a szolgáltatás igénybevevője

között. Ez az alapkoncepciója az IT szolgáltatások menedzselésének. Az SLA meghatározza a két fél között nyújtandó szolgáltatás tartalmát és feltételeit-

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 támogatja az informatika területén.

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

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

11 Mellékletek

11.1 Egyszerűsített Szolgáltatási Katalógus

Szolgáltatás	Mindenki	Egyetemi polgár	Vendégoktató	Hálózat felelős	Gazdasági Igazgatóság
ELTE nyilvános weblap	✓				
Saját weboldal		✓			
Központi tárhely		✓	✓		
Helpdesk				✓	✓
Központi elektronikus levélkezelő kiszolgáló (SMTP gateway)				✓	
Központi elektronikus levélkezelés (postafiók)		✓	✓		
Központi címtár szolgáltatás (LDAP)		✓			
DNS szolgáltatás		✓			
IP címek kiosztása és adminisztrációja				✓	
Hallgatói rendszer ETR		✓	✓		
Szuperszámítástechnika üzemeltetés, ütemezés		✓			
Gazdasági rendszerek					✓

Megjegyzések a szolgáltatás-katalógushoz:

- Az egyetemi polgárok csak meghirdetett szolgáltatást vehetnek igénybe (lásd Szolgáltatási Katalógus), annak feltételrendszerével (lásd az adott szolgáltatás SLA-ját)
- Saját személyes munkájukat szolgáló (és központi egyetemi szolgáltatáshoz nem tartozó) gépükön saját felelősségükre dolgozhatnak.

11.2 IT-SZ változáskezelési lap

Fejléc adatok:

Benyújtó neve:
Beosztása:
Elérhetősége:
e-mail:
telefon:
Benyújtás dátuma:
Aláírás:

A változtatni kívánt IT-SZ bekezdés száma, megnevezése:

A változtatás rövid indoklása:

A javasolt új szövegrész:

IIG tölti ki

Beérkezés időpontja:
Átvevő:

Az igény vizsgálatával kapcsolatos megjegyzések:

Az igény elbírálása: Bekerül a dokumentumba a változtatás

NEM kerül be a dokumentumba a változtatás

Indoklás:

Aláírás:

11.3 IIG fórumainak elérhetősége

IIG hivatalos web oldala:

<http://iig.elte.hu>

IIG hivatalos levelezési listái:

megnevezés	cím	funkció	kik iratkozhatnak fel rá
IIG hivatalos lista	Eltenet- l@listserv.elte.hu	értesítés	Egyetemi polgárok

11.4 Felhasználói nyilatkozat

Az egyetem által nyújtott szolgáltatás felhasználója kijelenti, hogy az egyetem Informatikai Házirendjét, valamint az adott szolgáltatásra vonatkozó SLA-t megismerte, és ennek megfelelően fogja használni az adott szolgáltatásokat.

Az informatikai rendszer üzemeltetése során keletkező naplóállományok személyes adatokat is tartalmazhatnak.

A nyilatkozatot nyomtatott betűkkel kell kitölteni!

Név:

Dátum:

Aláírás

A nyilatkozatot átvettem

Név:

Aláírás

11.5 ÜZEMELTETÉSI DOKUMENTÁCIÓ

1. Bevezetés

1.1 Verzió, lezárás dátuma

2. A rendszer (alkalmazás) alapfunkciói

3. A rendszer (alkalmazás) architektúrája

3.1 Az adatfolyam:

3.2 Külső és belső kapcsolatok

3.3 Elhelyezés, hardver és operációs rendszer környezet

4. Üzemeltetési feladatok

4.1 Rendszeres üzemeltetési feladatok

4.1.1 Rendszeres karbantartási feladatok

4.2 Eseti üzemeltetési feladatok

4.3 Jogosultságkezelés

4.4 Erőforrás igények:

4.4.1 A feldolgozások (futások) ideje

4.4.2 Helyszükséglet és az igényelt megőrzési idők

5. Az üzemmenet felügyelete, eseménykezelés

5.1 Szolgáltatási szint paraméterek és felügyeletük:

5.2 Az alkalmazás üzemképességi felügyeletének eszközei

5.2.1 Felügyeleti eszközök

5.2.1.1 Rendszer SMS-ek

5.2.1.2 Rendszer által küldött mailek

5.2.1.3 Az alkalmazás saját felügyeleti felülete

5.2.1.4 A rendszer által generált naplóállományok helye és elemzése, megőrzési ideje

5.2.2 Újrafuttatás

5.2.2.1 Egy teljes modul újrafuttatása

5.2.2.2 A teljes program újrafuttatása

5.2.2.3 Az egyes modulok összefüggései, logikai kapcsolatai

5.2.3 Incidenskezelés:

5.2.4 Back up (biztonsági mentések)

5.2.5 Katasztrófa elhárítási terv (DRP)

5.2.6 Üzletmenet (működés) folytonossági terv (BCP):

6. Az üzemeltetés személyi feltételei

6.1 Az alkalmazás üzemeltetéséhez szükséges ismeretek

6.2 Az alkalmazás használatához szükséges ismeretek:

6.3 Kiemelt felhasználók, szakmai adminisztrátorok, felelősségi körök

6.4 Támogató személyzet (és a támogatás szintjei)