A Pécsi Tudományegyetem
Informatikai Üzemeltetési Szabályzata

Pécs 2008.

Preambulum

A Pécsi Tudományegyetem (továbbiakban: Egyetem) Szenátusa az Egyetem alap és kutatási – fejlesztési feladatainak támogatása, a tanulás, információszerzés elősegítése, a kapcsolatteremtés és tartás új lehetőségeinek, valamint az információ szabad áramlásának informatikai eszközökkel történő biztosítása érdekében az alábbi szabályzatot alkotja.

I. fejezet

Általános rendelkezések

A szabályzat alapelvei

1. § (1) A szabályzat a világszerte elfogadott ITIL (IT Infrastructure Library) de facto IT szolgáltatásirányítási szabvány szerkezetét követi. Ennek célja, hogy az Egyetem az IT szolgáltatásaival kapcsolatos szolgáltatói szemléletmódot mind felhasználói, mind szolgáltatói oldalon erősítse.

(2) Az Egyetem informatikai szolgáltatásainak kialakítása, üzemeltetése és igénybevétele a hatályos jogszabályi környezet, különösen a szerzői és szerzői joghoz kapcsolódó jogok és a személyes adatok védelméhez való jog figyelembe vételével történik.

A szabályzat hatálya

2. § (1) A szabályzat az Egyetem informatikai szolgáltatásainak kialakítását, üzemeltetését, igénybevételét és ellenőrzési lehetőségeit szabályozza. A szabályzat meghatározza az eszközök használatának módját és feltételeit.

(2) Jelen szabályzat mindenkire nézve kötelező, aki az Egyetem informatikai szolgáltatásait, illetve informatikai infrastruktúráját, annak berendezéseit üzemelteti vagy használja (felhasználók), így a személyi hatály kiterjed különösen az Egyetem hallgatóira és dolgozóira, akik oktatási, tudományos vagy az intézmény adminisztrációs feladataikhoz az Egyetem informatikai infrastruktúráját használják, valamint az infrastruktúra használatára jogosult harmadik személyekre.

Az Egyetem átfogó informatikai menedzsmentje

3. § Az Egyetem informatikai tevékenységének szabályozását és koordinálását a Klinikai Központ (továbbiakban: KK) részére az Egészségügyi Informatikai Osztály (továbbiakban: EIO), a többi egyetemi szervezeti egység részére a Műszaki Igazgatóság keretén belül működő Egyetemi Informatikai Szolgáltató Központ (továbbiakban: EISZK) látja el.

Feladat, felelősség és hatáskörök az informatikai biztonság területén

4. § (1) Valamennyi üzemeltetett rendszer esetében az informatikai szabályzatnak való megfelelés az adott rendszert üzemeltető szervezeti egység felelőssége.

(2) Az adott szolgáltatás üzemeltetési feladatainak ellátásáért felelős személyt (a továbbiakban szolgáltató), illetve az üzemeltetésért felelős szervezeti egységet (a továbbiakban szolgáltató egység) az adott szolgáltatás szolgáltatási szint megállapodásában kell megnevezni.

(3) Az informatikai szolgáltatások szakmai felügyeletét az OEKK tekintetében az EIK, minden más egyetemi szervezeti egység esetében az EISZK szolgáltatás menedzsere látja el.

(4) A szolgáltatás menedzser felelős a szolgáltató és a szolgáltatás igénybevevője között a szolgáltatás tartalmának és egyéb paramétereinek egyeztetéséért, a megállapodás betartásának ellenőrzéséért.

(5) A PTE adatvédelmi felelőse jogosult az egyes szolgáltatások jelen szabályzatnak való megfelelőségének ellenőrzésére.

Jogszabályi megfelelőség és a felelősség szabályozása

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

(2) A szolgáltatás üzemeltetője az egyetemi szabályzatokban meghatározott nyilvántartásokat köteles vezetni.

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

a) a szolgáltatás korlátozása,

b) szolgáltatás megtagadás (kizárás a szolgáltatásból),

c) az okozott anyagi kár megtérítése,

d) polgári peres eljárás kezdeményezése,

e) büntetőeljárás kezdeményezése.

(4) A szolgáltatások igénybe vevőinek szankcionálása csak akkor történhet meg, ha az üzemeltető dokumentálta a szankció elrendelését kiváltó eseményt, incidenst. Ennek felelőse a szolgáltatást nyújtó szervezeti egység vezetője.

II. fejezet

IT rendszerek biztonsági osztályai, besorolás

Kritikus rendszerek

6. § Az Egyetem működése szempontjából kritikus az a rendszer, amely az Egyetem egészére kiterjed, vagy a PTE SZMSZ 85-86. §-aiban meghatározott szervezeti egységekben üzemel, vagy személyes adatot tartalmaz. Ezek a rendszerek adatvédelmi szempontból kiemelt védelmet igényelnek. Ebbe a kategóriába tartoznak különösen a következő rendszerek.

a) bér- és munkaügyi rendszer,

b) gazdasági, ügyviteli rendszer,

c) tanulmányi rendszer,

d) Vezetői Információs Rendszer,

e) iratkezelési rendszer,

f) központi levelező kiszolgálók,

g) központi tárhely kiszolgálók,

h) intézményi authentikációs rendszerek,

i) EÜ információs rendszerek,

Kiemelt rendszerek

7. § Az Egyetem működése szempontjából kiemelt rendszerek, melyek elsősorban technikai jellegűek, a rajtuk tárolt adatok nem személyes jellegűek. Ebbe a kategóriába tartoznak a következő rendszerek:

a) telekommunikációs hálózat,

b) technológiai rendszerek,

c) kommunikációs rendszerek.

Normál rendszerek

8. § (1) A normál rendszerek a kritikus rendszerek vagy a kiemelt rendszerek közé nem sorolt, a teljes intézmény napi működése szempontjából kritikus, illetőleg az Egyetemnek csak egyes részeire kiterjedő olyan rendszerek, amelyek használatához személyes authentikáció szükséges és legalább egy féléven át üzemelnek, valamint amelyekhez teljes körű dokumentáció készül.

(2) Ezen rendszerek indítása, üzemeltetése a KK területén az EIO, az Egyetem más szervezeti egységeinél az EISZK jóváhagyásával történik. Ebbe a kategóriába tartoznak különösen az alábbi rendszerek

a) interaktív kiszolgáló szerverek,
b) kutatói rendszerek
c) oktatási célú rendszerek.

Egyéb rendszerek

9. § Az előző három kategóriába nem sorolt rendszerek az egyéb rendszerek kategóriába tartoznak.

Az informatikai biztonsági követelmények az IT rendszerek szállítási szerződéseiben (beszállítók)

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

a) hatályos jogszabályoknak megfelelés,

b) átadás / átvételi jegyzőkönyv vagy teljesítési igazolás (mint a szerződés melléklete),

c) kapcsolattartó neve, elérhetősége,

d) technikai feltételek,

e) támogatási garanciális feltételek,

f) a beszállítás (projekt) menedzsmentje,

g) jogi nyilatkozat (tulajdonjog, szoftver használati jog, stb.),

h) biztonsági kérdések,

i) felelősségi körök elhatárolása.

Az IT rendszerek biztonsági ellenőrzése

11. § Az IT rendszerek biztonsági ellenőrzésének részletes szabályait az Egyetem Informatikai Biztonsági Szabályzata tartalmazza.

III. fejezet

Szolgáltatásszint menedzsment

Szolgáltatásszint menedzsment folyamata

12. § (1) A kritikus rendszer és a kiemelt rendszer az OEKK területén az EIK, az Egyetem más szervezeti egységeinél az EISZK által, vagy engedélyével üzemeltethető.

(2) A szolgáltatás tartalmára a szolgáltatási szint megállapodásban az üzemeltető szervezeti egység vezetője tesz javaslatot, a szolgáltatás indíthatóságáról a megállapodási javaslat alapján a Műszaki Igazgatóság vezetője dönt.

(3) Elutasító döntés esetén a javaslattevő 15 napon belül panasszal élhet az Informatikai Bizottság elnökénél. A panaszt az Informatikai Bizottság véleménye alapján a rektor bírálja el.

(4) A kritikus rendszer és a kiemelt rendszer kategóriába nem tartozó rendszerek esetében a rendszert üzemeltető szervezeti egység vezetője kérheti a szolgáltatás előző módon történő jóváhagyását. Az így jóváhagyott rendszerek normál rendszer kategóriájúnak minősülnek.

(5) A központilag jóváhagyott szolgáltatásokat az EIK és az EISZK honlapján közzéteszi. Ezek a szolgáltatások az egyetem hivatalosan authentikált szolgáltatásainak tekintendők.

A szolgáltatási szint megállapodások (SLA) tartalma

13. § Az Egyetem által nyújtott szolgáltatásokra szolgáltatási szint megállapodások készülnek (Service Level Agreement, SLA). A szolgáltatások nyújtása a megállapodások alapján történik. A szolgáltatási szint megállapodásoknak tartalmaznia kell az 1. számú mellékletbe foglaltakat.

14. § Külső szervezettel történő megállapodás esetén– amennyiben a megállapodás alapján személyes adatok feldolgozására sor kerül – az SLA megállapodás tartalmazza az adatfeldolgozónak a személyes adatok feldolgozásával kapcsolatos jogait és kötelezettségeit, így különösen:

a) a személyes adatok adatfeldolgozó felé történő továbbításának (hozzáférésének) módját,

b) az adatfeldolgozással érintett adatkezelési műveletek körét,

c) az IBSZ-ben kifejtett adatbiztonsági intézkedéseket,

d) azt a tényt, hogy az adatfeldolgozó az adatkezelő (PTE) rendelkezései szerint köteles eljárni, és hogy saját céljára adatfeldolgozást nem végezhet,

e) azt a tényt, hogy az adatfeldolgozó tevékenységi körén belül felelős a személyes adatok feldolgozásáért, megváltoztatásáért, törléséért, továbbításáért és nyilvánosságra hozataláért,

f) azt a tényt, hogy az adatfeldolgozó tevékenységének ellátása során más adatfeldolgozót – adatfeldolgozás tekintetében alvállalkozót - nem vehet igénybe.

Megfigyelés, jelentés és áttekintés (felülvizsgálat)

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

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

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

IV. fejezet

Ügyfélszolgálat / incidenskezelés

Ügyfélszolgálat (Service Desk) opciók és eljárások

16. § (1) Az EIK és az EISZK ügyfélszolgálatot működtet. A kritikus rendszer és a kiemelt rendszer kategóriájú rendszerekre vonatkozó incidens bejelentése a nevezett szervezeti egységek ügyfélszolgálatánál írásban történik, a kötelező és opcionális adatok megadásával. A bejelentés módját és a megadandó adatokat a szolgáltatás SLA-ja tartalmazza. Az ügyfélszolgálat minden bejelentést regisztrál, és ennek tényéről, valamint az ügy lezárásáról értesíti a bejelentőt.

(2) A normál rendszer kategóriájú rendszerek esetében a szolgáltató köteles megnevezni azt a munkatársat, aki a felhasználók felé az ügyfélszolgálatot ellátja. A bejelentés módját és a megadandó adatokat a szolgáltatás SLA-ja tartalmazza.

(3) Az ügyfélszolgálat kizárólag a hatáskörébe tartozó rendszerekkel összefüggő problémákat old meg. Nem vesz részt harmadik féllel felmerült vitás kérdések rendezésében és nem lát el jogi képviseletet.

Incidens osztályozás és prioritás hozzárendelés

17. § A bejelentett incidensek kezelésére a rendszer besorolásától függően priorizálva kerül sor. A priorizálás az ügyfélszolgálat feladata. Több incidens fellépésekor a magasabb prioritású incidens megoldása elsőbbséget élvez.

Incidenskezelés és naplózás

18. § Az incidenskezelésre és a naplózásra vonatkozó részletes szabályokat az adott szolgáltatás SLA-ja tartalmazza.

Problémakezelés

Incidens, probléma és az ismert hiba kezelése

19. § (1) Az üzemeltetést végző szervezeti egység vezetője által megbízott munkacsoport automatikus incidens, illetve probléma felderítő rendszereket üzemeltethet az SLA-k alapján, és ennek megfelelő szankciókkal élhet az 5. § (3) bekezdése szerint.

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

(3) A visszatérő, több incidens kiváltó okaként szereplő problémának a probléma adatbázisba történő felvitele manuális, amit az üzemeltető személyzet vagy az ügyfélszolgálat végez.

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

Probléma megelőzés

20. § (1) 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, reset,

b) javítócsomagok, patchek, fixek telepítése,

c) jelszavak és hozzáférési kódok rendszeres cseréje,

d) naplóállományok rendszeres kiértékelése.

(2) Mind az EIK, mind az EISZK biztosíthatja az általuk kiszolgált szervezeti egységek számára a probléma megelőzés alap infrastruktúráját, de az Egyetem egyes szervezeti egységei jogosultak további megelőző intézkedéseket végrehajtani. Az intézkedési tervet kötelesek előzőleg bejelenteni az EIK, illetve az EISZK vezetőjének. A tervezett intézkedések csak az EIK, illetve az EISZK vezetőjének jóváhagyása után foganatosíthatók.

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

(4) A probléma megelőzés érdekében mind az EIK, mind az EISZK évente konzultációt szervez a szolgáltatási körébe tartozó, más szervezeti egységek üzemeltető személyzete részére.

V. fejezet

Konfigurációkezelés

Alapelvek és terminológia

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

A konfigurációkezelés adatbázisa

22. § (1) Az adott rendszer üzemeltetője minden szolgáltatás és szolgáltató rendszer esetében időrendben vezeti a konfiguráció változását leíró adatbázist.

(2) Minden változás esetén az alábbiakat kell megadni az adatbázisban:

a) a változó komponensek egyértelmű azonosítását lehetővé tevő adatokat,

b) a változás szükségességének indokait,

c) a tesztelésre vonatkozó adatokat,

d) az aktuális visszaállítási teendőket tartalmazó hivatkozást.

Változáskezelés

Központosított változás-felügyelet

23. § (1) A változás-felügyelet célja, hogy a változások gyors és hatékony kezelésére szabványos módszerek és eljárások használatát biztosítsa annak érdekében, hogy a változással összefüggő incidenseknek a szolgáltatás minőségére gyakorolt hatását minimalizálja, és ezzel is javítsa a szervezet működését.

(2) A kritikus rendszer és a kiemelt rendszer besorolású informatikai rendszerek esetében az OEKK területén az EIK, az Egyetem többi szervezeti egységénél az EISZK központi változás-felügyeletet gyakorol.

(3) A normál és egyéb osztályú rendszerek esetében a változás felügyeletet az üzemeltető szervezeti egység gyakorolja.

Változáskezelési folyamatok

24. § A központi változás-felügyelet menete:

a) a kritikus rendszer, kiemelt rendszer és normál kategóriájú rendszer esetén a szolgáltatás üzemeltetője a változtatás megkezdése előtt engedélyezteti a megvalósítandó hardver és szoftver konfigurációt az adott terület illetékes szakértőjével,

b) a területi szakértőket a kritikus rendszer és a kiemelt rendszer kategóriájú rendszerek esetében értelemszerűen az EIK vagy az EISZK vezetője, normál kategóriájú rendszereknél az üzemeltető

szervezeti egység vezetője jelöli ki. A területi szakértő személye esetileg egybeeshet a szolgáltatás üzemeltetőjével,

c) az engedélyezett változtatásokat (hardver, szoftver, adatbázis, stb.) a szolgáltatás üzemeltetője az üzemeltetési leírásban foglaltak alapján végrehajthatja, sikeres végrehajtás esetén a rendszer leírásában dokumentálja.

Szerepkörök és felelősségek

25. § (1) A szolgáltatás üzemeltetője teljes felelősséggel tartozik minden olyan beavatkozásért, amit a felelős területi szakértő nem engedélyezett, illetve amelyek esetében a rendszer üzemeltetési leírása nem került betartásra.

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

(3) Az EIK, az EISZK illetve az üzemeltető szervezeti egység vezetője tartozik felelősséggel azon területekért, amelyekre területi szakértőt nem jelölt ki.

Kiadáskezelés (új szolgáltatás indítása)

26. § (1) Az auditált rendszerek megvalósítását és dokumentálását, valamint a szolgáltatás tesztelését a szolgáltatási területnek megfelelően az EIK vagy az EISZK szolgáltatás menedzsere ellenőrzi. A sikeres tesztüzem után a szolgáltatás üzembe állítását az EIK vagy az EISZK vezetője engedélyezi.

(2) A kritikus rendszer, kiemelt rendszer és normál kategóriás rendszerek esetében a szolgáltatás elindításának feltétele, hogy a szolgáltatási területnek megfelelően az EIK, az EISZK vagy a szolgáltató egység vezetője jóváhagyja az SLA-t, az üzemeltetési dokumentációt, a rendszerkonfigurációt és a változáskezelési folyamatot.

Hiteles szoftver tár

27. § (1) Az EISZK szoftver disztribúciós munkatársa központilag létrehozza és karbantartja a központilag beszerzett szoftverek eredeti példányainak és az installációs csomagjainak tárát. Amennyiben a beszerzett szoftver csak korlátozott példányszámban használható, meg kell határozni a hozzáféréssel rendelkezők körét. Ezt az egyetem Informatikai Bizottsága végzi.

(2) A szoftver disztribúciós munkatárs feladatai:

a) a legfrissebb verziók letöltése, a csomagok frissítése,

b) patchek, hotfixek letöltése, közzététele,

c) csomagok vírusellenőrzése,

d) hozzáférési jogosultságok kezelése.

(3) Minden szolgáltató rendszer esetében a jogszerű működés bizonyítását lehetővé tevő licencek tárolása az üzemeltető szervezeti egység vezetőjének kötelezettsége.

(4) Az Egyetem különböző szervezeti egységei által, a szakmai tevékenységük támogatására beszerzett szoftverek kezelését a fentiekben rögzített formában, a szervezeti egységvezető által megbízott munkatárs végzi.

(5) Azon programok esetében, melyekre az egyetem campus licence-szel, vagy egyetemi korlátozott licence-szel rendelkezik, a licencek tárolását és a kiadás elbírálását az EISZK szoftver disztribúcióval foglalkozó munkatársa végzi.

VI. fejezet

IT szolgáltatásfolytonosság biztosítása

Kockázatkezelés

28. § Minden kritikus rendszer és kiemelt rendszer besorolású szolgáltató rendszer esetében rendelkezni kell olyan kockázatelemzéssel, ami a rendszer által nyújtott szolgáltatások részleges vagy teljes kimaradásának az Egyetem működőképességére tett hatásait tartalmazza. Külön kell kezelni a szolgáltatás elérhetetlenségéből, illetőleg az adatbázis sérülésből származó hatásokat. A kockázatelemzési dokumentum előállítása és karbantartása a szolgáltatás üzemeltetőjének a feladata.

Vészhelyzet opciók és az IT szolgáltatásfolytonossági terv

29. § (1) A szolgáltató rendszerek üzemeltetési leírásának tartalmaznia kell a szolgáltatásfolytonossági tervet, amelynek tartalmaznia kell:

a) az adott szolgáltatás kiesése esetén (vészhelyzet) a helyettesítési lehetőségeket (műszaki, technológiai és szervezési megoldások),

b) a működés folyamatosságának fenntartása érdekében tett intézkedéseket,

c) az intézkedésre jogosultak körét,

d) az intézkedésről értesítendők körét.

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

Rendelkezésre állás, szervizelhetőség biztosítása

Rendelkezésre állás szintjei

30. § (1) Az egyetem működése szempontjából kritikus szolgáltatások (kritikus rendszer és a kiemelt rendszer kategóriájú rendszerek) esetében az adott területért felelős felső szintű vezető jóváhagyásával a szolgáltatási területtől függően az EIK, illetve az EISZK vezetője határozza meg azt a rendelkezésre állási intervallumot, amiben a szolgáltatásnak elérhetőnek kell lennie.

(2) A kritikus rendszer, kiemelt rendszer és a normál kategóriájú rendszerek esetében a rendelkezésre állást tervezni kell. A terv elkészítéséért a szolgáltató egység vezetője, a tervezés ellenőrzéséért az EIK, illetve az EISZK vezetője a felelős.

Karbantarthatóság

31. § (1) Az adott szolgáltatás üzemeltetőinek a szolgáltatás aktuális üzemeltetői dokumentációjában fel kell tüntetni azon műszaki megoldásokat, melyek a szolgáltatás meghatározott elérési paramétereit hívatottak biztosítani.

(2) Az üzemeltetőknek a szolgáltatás következő éves fejlesztési tervében rögzíteniük kell az elavult, nem szervizelhető komponensek cseréjére vonatkozó javaslatot.

VII. fejezet

Pénzügyi irányítás, költségvetés tervezés

32. § IT szolgáltatásokat végző szervezeti egységek a naptári évre vonatkozó pénzügyi tervezést az egyetem más szervezeti egységeivel azonos időszakban végzik. A pénzügyi tervezés ciklusai:

a) az adott szervezeti egység működésének és meglévő szolgáltatásának fenntartásához szükséges költségek meghatározása,

b) a következő évben indítandó, új szolgáltatások technikai, műszaki tervezése,

c) a megvalósításhoz szükséges projekttervek és azok költségvonzatának elkészítése,

d) a projekttervek és az összesített költségtervek elfogadtatása a felügyeletet ellátó szervezeti egység vezetésével,

e) egyetemi szintű költségvetési fordulók (egyeztetések a Gazdasági Bizottsággal, Dékáni-, illetve Rektori Tanáccsal),

f) projekttervek és költségvetés véglegesítése,

g) szenátusi jóváhagyás.

Pénzügy és számvitel

33. § A szolgáltatást nyújtó szervezeti egység részére jóváhagyott pénzügyi keret felhasználását a szervezeti egység vezetője engedélyezi. A felhasználás és annak bizonylatolása az erre vonatkozó általános szabályoknak megfelelően történik.

Kapacitáskezelés

34. § (1) Az EISZK vezetője felelős azért, hogy az Egyetem központi szolgáltatásainak biztosításához, működéséhez szükséges IT kapacitásokat a felhasználóktól beérkező igények, a szolgáltatói környezet változása, a technikai fejlődés figyelembe vételével tervezze, és a jóváhagyott egyetemi költségvetés szerint biztosítsa.

(2) Az OEKK működéséhez szükséges szakma specifikus igények kezelése az EIK vezetőjének feladata.

Kapacitástervezés

35. § (1) A szolgáltatást biztosító rendszer várható terhelését az üzemeltető szervezeti egység vezetője az eddigi használati trendek alapján évente előre jelzi a következő egy éves időtartamra (a költségvetés

tervezés időszakában) az üzemeltetők felé. A terhelés előrejelzés alapján az üzemeltetők kapacitástervet készítenek, aminek tartalmaznia kell az összes olyan rendszerkomponens listáját, amit a szolgáltatás zavartalan biztosítása érdekében módosítani, vagy bővíteni kell.

(2) Az elkészített kapacitástervek alapján, az üzemeltetés vezetője fejlesztési tervet készít, amit a következő évi költségvetés tervezetével együtt benyújt a szervezeti egység vezetőjének.

(3) A kapacitástervek és a fejlesztési tervek elfogadásáról a szervezeti egység vezetője szolgáltatásonként külön, nyilvános döntést hoz.

VIII. fejezet

Értelmező rendelkezések

36. § Értelmező rendelkezések:
Adat: Az információnak olyan új formában való ábrázolása, amely alkalmas közlésre, értelmezésre, vagy feldolgozásra. A számítástechnikában:

- a számítógépes állományok meghatározott része (minden, ami nem program)
- mindaz, amivel a számítógépek kommunikációjuk során foglalkoznak

Adatállomány, fájl: az informatikai rendszerben logikailag összetartozó, együtt kezelt adatok összessége.
Adatátvitel: Adatok informatikai rendszerek, rendszerelemek közti továbbítása
Akkreditálás: Olyan eljárás, amelynek során egy erre feljogosított testület vagy személy hivatalos elismerését adja annak, hogy egy szervezet vagy személy felkészült és alkalmas bizonyos, az akkreditációs okiratban, dokumentumban meghatározott tevékenységek elvégzésére.
Audit: Módszeres és független vizsgálat annak meghatározására, hogy a tevékenységek és a kapcsolódó eredmények az előirányzott tervezeteknek megfelelnek-e és a tervezetet hatékonyan és a célok elérésének megfelelően alkalmazzák-e.
Authentikáció: Az adatcsere során a kommunikációban résztvevő felek identitása megállapításának és ellenőrzésének folyamata.
Bizalmasság: Az adat tulajdonsága, amely arra vonatkozik, hogy az adatot csak az arra jogosultak ismerhessék meg, illetve rendelkezhessenek felhasználásáról.
BCP: (Business Continuity Plan) Üzletmenet folytonossági terv, az üzletmenet (működés) fenntartása érdekében teendő intézkedések összessége arra az esetre, ha az adott üzleti folyamat vagy alkalmazás végrehajtása, működtetése valamilyen természeti, vagy ember által okozott katasztrófa miatt, akadályokba ütközik.
Biztonság: A védeni kívánt rendszer olyan, a szervezet számára kielégítő mértékű állapota, amely zárt, teljes körű, folytonos és a kockázatokkal arányos védelmet valósít meg.
Biztonsági esemény: Az informatikai rendszer biztonságában beállt olyan kedvezőtlen változás, melynek hatására az informatikai rendszerben tárolt adatok bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása megsérült, vagy megsérülhet.
Biztonsági osztályba sorolás: Az adatnak az adatkezelés során a kezelés módjára, körülményeire, a védelem eszközeire vonatkozó védelmi szintet meghatározó besorolása, osztályozása.
DRP: (Disaster Recovery Plan) Katasztrófa utáni helyreállítási terv, amely magába foglalja az üzletmenet (működés) szempontjából kritikus hardver és szoftver elemek működésének újraindítását természeti, vagy ember által okozott katasztrófák esetén.
Hálózat: Informatikai eszközök közti adatátvitelt megvalósító logikai és fizikai eszközök összessége.
Hardver: az informatikai erőforrás fizikailag megfogható részeinek összessége.
Hitelesség: Az adat olyan tulajdonsága, amely arra vonatkozik, hogy az adatbizonyítottan vagy bizonyíthatóan az elvárt forrásból származik.
Incidens: A szolgáltatás standard működésétől eltérő esemény, amely fennakadást vagy minőségcsökkenést okoz, vagy okozhat a szolgáltatásban.

Informatikai szolgáltatás: minden olyan informatikai rendszerhez történő definiált és dokumentált hozzáférési, felhasználási lehetőség, amelyet a rendszer üzemeltetői a felhasználók számára elérhetővé tesznek
ITIL: (Information Technology Infrastructure Library) Informatikai infrastruktúra könyvtár az emberi és technológiai folyamatok optimalizálásának, a költségek csökkentésének lehetőségeit mutatja be. Egy jól bevált módszertani ajánlás, amely csúcsminőségű IT szolgáltatások kialakítására és az üzleti hatékonyság növelésére összpontosít. Az ITIL áttekinti az informatikai tervezés módszereit, a modelleket és a folyamatokat, valamint meghatározza a végrehajtásukhoz szükséges szerepköröket és azok kapcsolatát. Az Egyesült Királyság kormányának felügyeleti keretrendszereként fejlesztették ki az 1980-as években, azóta az egész világon az IT szolgáltatásmenedzsment „de facto" szabványává vált.
Kockázatmenedzsment: Védelmi intézkedések kidolgozása, elemzése és meghozatala, amelyet követően a maradványkockázatok elviselhető szintűre változnak
Központi menedzsment: Több számítógép felügyeletének párhuzamos ellátása. Ha a számítógépek azonos vagy hasonló kiépítettségűek, és feladataik is azonosak, vagy hasonlóak, akkor a rendszergazda egy megfelelően kialakított hálózatos telepítés és később megfelelő házirend kialakításával egységes gépparkot alakíthat ki. Ez egyrészt csereszabatossá teszi a gépeket, másrészt meggátolja a napi üzemszerű működést sokszor károsan befolyásoló engedély nélküli szoftver telepítéseket és beállítás módosításokat és egyenszilárdságú védelem kialakítását teszi lehetővé.
Szolgáltatási szint megállapodás (Service Level Agremeent, SLA): olyan megállapodás, amely két fél között jön létre és meghatározza a két fél között nyújtandó szolgáltatás tartalmát és feltételeit.
Spam-szűrés: A kéretlen reklámlevelek közös gyűjtőneve a spam. Az egyre növekvő mennyiségben érkező spam kezelése, tárolása komoly erőforrás problémákat vet fel, tömeghatásával leterheli, lelassítja a rendszert és feleslegesen köt le nagy háttér tár kapacitást. Ennek kivédésére alkalmazzák a levelező kiszolgálón, vagy a tűzfalon telepített spam –szűrő megoldásokat.
Változásmenedzsment: Az informatikai termék, vagy rendszer fejlesztési, előállítási, vagy karbantartási folyamatai alatt megvalósuló változásokat kezelő rendszer.
WiFi: ld. WLAN
WLAN: a vezeték nélküli helyi hálózat angol elnevezésének rövidítése.

Záró és hatályba léptető rendelkezések

37. § (1) A szabályzat az új eszközök és szolgáltatások esetében a Szenátusa által történő elfogadás napján, a már működő eszközök és szolgáltatások esetében az elfogadást követő hatodik hónap első napján lép hatályba.

(2) Egy adott szolgáltatás üzemeltetési feladatainak ellátásáért felelős közalkalmazott munkaköri leírásában a munkáltatónak 2008. június 30. napjáig rögzítenie kell, hogy a közalkalmazott felelős az SLA betartásáért, folyamatos aktualizálásáért, valamint a szabályzatban meghatározott dokumentációk elkészítéséért.

(3)A szabályzat felülvizsgálatára szükség szerint, de legalább évente egy alkalommal sor kerül.

Pécs, 2008. április 24.

Dr. Gábriel Róbert
rektor

Záradék:

Jelen szabályzatot a Pécsi Tudományegyetem Szenátusa 2008. május 8-ai ülésen 164/2008. (05. 08.) számú határozatával elfogadta.

1. számú melléklet

A szolgáltatási szint megállapodások minimális tartalma

1) szolgáltatás neve (egyedi megnevezés),
2) SLA verziószám,
3) az SLA lezárásának dátuma,
4) az SLA által érintett területek, határok,
5) igénybe vevő és szolgáltató, jóváhagyó (a szolgáltatás igénybevevője, vagy ezek képviselője, a szolgáltató, illetve képviselője mellett az EIK vagy az EISZK részéről a jóváhagyó megnevezése),
6) a szolgáltatás rövid leírása, amely összefoglalja a szolgáltatás célját, tartalmát,
7) érvényesség / megszűnés,
8) aláírások (név, beosztás, dátum),
9) szolgáltatás leírása (részletes, technikai leírás), szolgáltatás katalógus:
   a) kulcs funkciók,
   b) kiterjedés, hatókör,
   c) elhelyezés,
   d) kik vehetik igénybe,
   e) besorolás (A – D),
10) szolgáltatási időszak (pl.8 – 16 óra munkanapokon),
11) felhasználói csoportok meghatározása,
12) a szolgáltatás használata
   a) a kapcsolattartó neve, elérhetősége,
   b) a szolgáltatás igénylésének módja és helye,
   c) a szolgáltatás igénybevételének feltételei,
   d) az átfutási időtartama,
13) a szolgáltatás igénybevevőjének kötelezettségei,
14) szolgáltató és igénybevevő felelősségének meghatározása,
15) a szolgáltatással kapcsolatos tájékoztatás módja,
16) monitorozási feltételek,
17) karbantartási időszakok,
18) rendelkezésre állás (%)
   a) A rendelkezésre állás mérőszámai ,
   b) A mérés módja,
   c) Vállalt rendelkezésre állási mutatók,
19) támogatás
   a) A támogatás köre,
   b) A támogatás igénybevételének módja,
20) incidens kezelés
   a) Az incidenseket bejelentésének módja, helye,
   b) A bejelentés feldolgozásának időtartama,
   c) Visszajelzés menete az incidens lezárásakor,
21) teljesítmény / minőség
   a) Optimális teljesítmény adatok (pl. elérési idő, válaszidő stb. az adott szolgáltatás esetében),
   b) Minimális teljesítmény adatok,
22) a szabályzatban foglaltakhoz képest sajátos változáskezelési eljárások,
23) IT üzletmenet folytonosság
   a) A katasztrófa elhárítási tervre (DRP), illetve az üzletmenet folytonossági tervre (BCP) való hivatkozás (sajátosságokat ill. változásokat tartalmaz),
24) az IBSZ-hez képest sajátos biztonság szabályok,
25) az SLA felülvizsgálatának ideje,
26) szójegyzék.

2. számú melléklet

Felhasználói nyilatkozat

Alulírott, a PTE által nyújtott informatikai szolgáltatás felhasználója, kijelentem, hogy az egyetem Informatikai Üzemeltetési Szabályzatát, valamint az általam igénybevett szolgáltatás SLA-ját megismertem és az abban foglaltaknak megfelelően fogom az adott szolgáltatásokat használni.

Tudomásul veszem, hogy az informatikai rendszer üzemeltetése során keletkező naplóállományok személyes adatokat is tartalmazhatnak.

Név (nyomtatott betűkkel):

Dátum:

Aláírás:

A nyilatkozatot átvettem:

Név (nyomtatott betűkkel):

Aláírás:

Szervezeti egység:

Dátum:

3. számú melléklet

Üzemeltetési dokumentáció

1) Bevezetés
   a) Verzió, lezárás dátuma
2) A rendszer (alkalmazás) alapfunkciója
3) A rendszer (alkalmazás) architektúrája
   a) Az adatfolyam:
   b) Külső és belső kapcsolatok
   c) Elhelyezés, hardver és operációs rendszer környezet
4) Üzemeltetési feladatok
   a) Rendszeres üzemeltetési feladatok
      i) Rendszeres karbantartási feladatok
      ii) Eseti üzemeltetési feladatok
   b) Jogosultság kezelés
5) Üzemmenet felügyelet, eseménykezelés
   a) Szolgáltatási szint paraméterek és felügyeletük
   b) Az alkalmazás üzemképességi felügyeletének eszközei
      i) Rendszer SMS-ek
      ii) Rendszer által küldött mailek
      iii) Az alkalmazás saját felügyeleti felülete
      iv) A rendszer által generált naplóállományok helye és elemzése, megőrzési ideje
   c) Incidenskezelés
   d) Biztonsági mentések
   e) Katasztrófa elhárítási terv (DRP)
   f) Üzletmenet folytonossági terv (BCP)
6) Az üzemeltetés személyi feltételei
   a) Az alkalmazás üzemeltetéséhez szükséges ismeretek
   b) Az alkalmazás használatához szükséges ismeretek
   c) Kiemelt felhasználók, szakmai adminisztrátorok, felelősségi körök
   d) Támogató személyzet és a támogatás szintjei