A Pécsi Tudományegyetem
Informatikai Biztonsági Szabályzata

Pécs 2008.

Preambulum

A Pécsi Tudományegyetem (továbbiakban: Egyetem) Szenátusa az Egyetem informatikai biztonságának biztosítása, illetve fenntartása érdekében az alábbi szabályzatot alkotja.

I. fejezet

Általános rendelkezések

A szabályzat alapelvei

1. § (1) A szabályzat az MSZ ISO/IEC 27001:2005 szabvány figyelembevételével készült. Ennek célja, hogy az Egyetem hatékony és nemzetközi szabványokon alapuló informatika biztonsági irányítási rendszert alapozzon meg.

(2) Az Egyetem informatikai biztonságának kialakítása, és fenntartása 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 tárgyi hatálya az egyetem informatikai szolgáltatásainak biztonsági kérdéseire terjed ki.

(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, gyógyító munkájukhoz vagy az intézmény adminisztrációs feladataihoz az Egyetem informatikai infrastruktúráját használják, valamint az infrastruktúra használatára jogosult harmadik személyekre.

Értelmező rendelkezések

3. § (1) 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.

(2) Informatikai szolgáltatás: minden olyan informatikai rendszerhez történő definiált és dokumentált hozzáférési, felhasználási lehetőség, amelyet a rendszer üzemeltetői a felhasználók számára elérhetővé tesznek.

(3) Intézményi adat: az Egyetem által kezelt, nem személyes adat.

Kapcsolódó szabályozások

4. § Jelen szabályzatban nem szabályozott kérdésekben az alábbi dokumentumok irányadók:

a) az Egyetem Szervezeti és Működési Szabályzata (továbbiakban PTE SZMSZ),
b) az Egyetem Informatikai Szabályzata,
c) a 20/2004. (VI.21.) IHM rendelet a Nemzeti Információs Infrastruktúra Fejlesztési Program Felhasználói Szabályzatának közzétételéről (HBONE AUP).

II. fejezet

Informatikai Biztonsági Politika

5. § (1) Az Informatikai Biztonsági Politika célja, hogy az Egyetem szervezeti egységei részére egységes és általános értelmezést adjon az informatikai rendszerekben kezelt adatok bizalmassága, hitelessége, sértetlensége, rendelkezésre állása és funkcionalitása biztosítása érdekében a követendő irányelvekre.

(2) A személyes adatok kezelésére vonatkozó előírásokat az Egyetem Adatvédelmi Szabályzata tartalmazza.

(3) Az irányelvek figyelembevételével meghatározható a különböző adatokat kezelő informatikai rendszerek biztonsági osztályba sorolása, kidolgozhatóak az adatot, mint a támadások célját körülvevő rendszerelemekre vonatkozó konkrét informatikai biztonsági szabályozások, amelyek az informatikai rendszer teljes életciklusában meghatározzák a szabványos biztonsági funkciók tervezéséhez, megvalósításához, üzemeltetéséhez és megszüntetéséhez szükséges alapelveket és követelményeket.

IT rendszerek biztonsági osztályai, besorolás

6. § Az Egyetemen kritikus, kiemelt, normál, illetve egyéb osztályú rendszerek működnek. A rendszerek besorolása, illetve átsorolása a szabályzat 6-9. §-ra tekintettel az üzemeltető feladata.

Kritikus rendszerek

7. § Az egyetem működése szempontjából kritikus az a rendszer, amely az Egyetem egészére kiterjed, vagy a PTE SZMSZ 85-86. §-ban meghatározott szervezeti egységben üzemel, vagy személyes adatokat 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) iratkezelési rendszer,
e) Vezetői Információs Rendszer,
f) központi levelező kiszolgáló,
g) központi tárhely kiszolgálók,
h) egyetemi authentikációs rendszerek,
i) EÜ információs rendszerek.

Kiemelt rendszerek

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

a) telekommunikációs hálózat,

b) technológiai rendszerek,

c) kommunikációs rendszerek.

Normál rendszerek

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

(2) Ezen rendszerek indítása/üzemeltetése a Klinikai Központ (továbbiakban KK) területén az Egészségügyi Informatikai Osztály (továbbiakban EIO), az egyetem más szervezeti egységeinél az Egyetemi Informatikai Szolgáltató Központ (továbbiakban EISZK) jóváhagyásával történik. Ebbe a kategóriába tartoznak különösen a következő rendszerek:

a) interaktív kiszolgáló szerverek,

b) kutatói rendszerek

c) oktatási célú rendszerek.

Egyéb rendszerek

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

Informatikai biztonsági alapelvek

11. § (1) Az Egyetem szervezeti egységei által kezelt informatikai infrastruktúra védelmét úgy kell megvalósítani, hogy az informatikai rendszereknek és környezetének védelme teljes körű, zárt, kockázatokkal arányos és folytonos legyen, valamint megvalósuljon a zárt szabályozási ciklus az alábbiak szerint.

(2) A teljes körűségre vonatkozó alapelvet a fizikai, a logikai, az adminisztratív és a humán védelem területén kell érvényesíteni úgymint:

a) az összes információbiztonsági rendszerelem csoportra,
b) az informatikai rendszer infrastrukturális környezetére,
c) a hardver rendszerre,
d) az alap és felhasználói szoftver rendszerre,
e) a kommunikációs és hálózati rendszerre,
f) az adathordozókra,
g) a dokumentumokra és feljegyzésekre,
h) a belső személyzetre és a külső partnerekre,
i) az MSZ OSI 7498-1 szabványban meghatározott nyílt rendszerek architektúrája minden rétegére, azaz mind a számítástechnikai infrastruktúra, mind az informatikai alkalmazások szintjén.

(3) A védelem zártsága akkor biztosított, ha az összes valószínűsíthető fenyegetés elleni védelmi intézkedések megvalósulnak.

(4) A védelem akkor kockázatarányos, ha az informatikai rendszerek által kezelt adatok védelmének erőssége és költségei a felmért kockázatokkal arányban állnak. Célkitűzés a minimális védelmi költséggel elért maximális védelmi képesség. Ehhez az informatikai projektek elején, a biztonsági rendszer tesztelésekor és az üzemeltetés során évente egyszer el kell végezni a kockázatelemzést

(5) A védelem folytonossága úgy biztosítható, hogy az informatikai rendszerek megvalósítása és fejlesztése során kialakított védelmi képességeket a rendszerből történő kivonásig, a rendszeres ellenőrzéssel és az ezt követő védelmi intézkedésekkel folyamatosan biztosítani kell.

(6) Zárt szabályozási ciklus úgy érvényesíthető, hogy az adminisztratív védelemmel biztosítani kell a szabályozás, érvényesítés, ellenőrzés és a védelmi intézkedések/szankcionálás zárt folyamatát.

Az informatikai biztonság szervezeti kérdései

Az informatikai biztonság belső szervezete

12. § Az informatikai biztonsággal kapcsolatos felelősség megoszlik az EIO, az EISZK, az informatikai infrastruktúrát működtető szervezetek és a felhasználók között.

Vezetői elkötelezettség

13. § (1) Minden szervezeti egység vezetője személyesen felel az informatikai biztonság kultúrájának kialakításáért és fenntartásáért.

(2) A vezetők elkötelezettségüket személyes példamutatással (szabályozások betartása) és személyes felelősségvállalással demonstrálják.

(3) A belső és külső szolgáltatói megállapodások (SLA-k) figyelése, figyelembe vétele és a bennük megfogalmazott paraméterek mérése a vezetői elkötelezettség kinyilvánítása. Az informatikai biztonsági intézkedések megvalósításához szükséges erőforrások biztosítása szintén a vezetői elkötelezettséggel összhangban zajlik.

(4) Az egyetemi szintű informatikai rendszerek szabályzatnak való megfelelősége az EISZK vezetőjének a hatásköre.

Informatikai biztonsági koordináció (érintett felekkel egyeztetés)

14. § (1) Az informatikai rendszerek szabályzatnak való megfelelőségi vizsgálatát, illetőleg az ezzel kapcsolatos tanácsadást a KK területén az EIO, az egyetem más szervezeti egységei vonatkozásában az EISZK Biztonsági Megbízottja végzi.

(2) A szabályzatnak való megfelelőségi vizsgálatot az üzemeltetési és szolgáltatási területtől függően az EIO vagy az EISZK vezetője, vagy a rendszert üzemeltető szervezeti egység vezetője kezdeményezheti.

(3) Az Egyetem informatikai biztonsági vezetője a főtitkár.

Az informatikai biztonsági felelősségek allokációja

15. § (1) Azon informatikai rendszerek esetében, amiknek nem volt sikeres a szabályzatnak való megfelelőségi vizsgálata, minden negatív biztonsági esemény felelőssége az üzemeltető szervezeti egység vezetőjét terheli.

(2) Azon rendszerek esetében, ahol a szabályzatnak való megfelelőségi vizsgálat sikeres volt (illetőleg a vizsgálat során készült és elfogadott hiánylistát az üzemeltető pótolta) a negatív biztonsági események felelőssége egyedi vizsgálat alapján állapítható meg. A szabályzat betartása esetén az üzemeltető jóhiszeműségét vélelmezni kell.

(3) Az EIO és az EISZK Biztonsági Megbízottjának a feladata az informatikai biztonsági események, incidensek tanulságainak és a pozitív példák megjelenítése az Egyetem szokásos információs csatornáin.

Új információs-feldolgozó rendszerek elfogadási eljárása

16. § (1) Új informatikai szolgáltatás indítási kérelméhez csatolni kell a rendszer vázlatos leírását és a tervezett SLA-t (szolgáltatási szint megállapodás). Ezen anyagok alapján az EIO vagy az EISZK vezetője a szolgáltatás engedélyezése előtt javaslatot kérhet a szervezeti egysége Biztonsági Megbízottjától a szabályzat mellékleteinek aktualizálására, az új szolgáltatás szabályzatba foglalt paramétereinek megállapítására.

(2) A szolgáltatás indítási kérelem automatikusan a szabályzat elfogadási szándéknyilatkozatának tekintendő.

Titoktartási nyilatkozat

17. § (1) Az informatikai biztonsági szabályok betartásával és betartatásával kapcsolatban az 1. számú mellékletben részletezett titoktartási nyilatkozatot írnak alá a kritikus és a kiemelt osztályú rendszerek üzemeltetői, illetve abban az esetben a felhasználók is, ha erről az adott rendszer SLA-ja külön rendelkezik. Ugyan ezt teszik az Egyetem üzleti partnerei is.

(2) A kritikus, illetve kiemelt rendszer üzemeltetőjének a feladata az (1) bekezdésben meghatározott titoktartási nyilatkozattal kapcsolatos adminisztrációs teendők ellátása.

(3) A rendszer üzemeltetői munkaköri feladataik ellátása során különféle személyes, illetőleg bizalmas adatokhoz férhetnek hozzá. Ezen adatok védelméről az Adatvédelmi Szabályzatban foglaltak szerint gondoskodni kell.

(4) A munkavégzés során a munkavégzők részére átadott, illetve tudomásukra jutott információkat védeni kell.

(5) Minden bizalmassági kérdésben érintett szereplővel ***titoktartási*** nyilatkozatot kell kitöltetni, melynek aláírásával felvállalja, hogy a birtokában lévő információval nem él vissza.

Kapcsolattartás hatóságokkal

18. § A különböző törvényekben és rendeletekben előírt informatikai biztonsági adatszolgáltatási kötelezettség teljesítése a KK vonatkozásában az EIO az Egyetem egyéb szervezeti egységeit illetően az EISZK vezetőjének felelőssége. Az egyének hatósággal folytatott jogvitáiban az Egyetem, illetve az EIO és az EISZK jogi képviseletet nem lát el.

Kapcsolattartás szakmai érdekközösségekkel

19. § (1) Az EISZK vezetője felelős az egyetemi szintű kapcsolattartásért a szakmai érdekközösségekkel, mint pl. a magyar non-profit internet használók közössége, a Hungarnet Egyesület. Minden hivatalos tagsági és kapcsolattartási kérdésben az Egyetem érdekeinek figyelembe vételével az EISZK vezetője dönt.

(2) A felhasználók egyéni tagsága az adott személy felelőssége. Egyéni tagként is köteles a kapcsolattartás során a szabályzat vonatkoztatható előírásait betartani.

Az informatikai biztonság felülvizsgálata

20. § Mivel az Egyetem Belső Ellenőrzési Osztálya informatikai biztonsági vizsgálatot nem végez, ezt a funkciót a KK szervezeti egységeinek vonatkozásában az EIO, más egyetemi szervezeti egységek esetében az EISZK Biztonsági Megbízottja látja el. A kritikus rendszerek esetében az audit évente végrehajtásra kerül. Más rendszerek esetében az audit szükségességéről és módjáról esetileg – az üzemeltető szervezeti egység hovatartozásától függően – az EIO, vagy az EISZK vezetője dönt.

A külső felekhez, partnerekhez kapcsolódó kockázatok azonosítása

21. § A külső felekkel, partnerekkel történő kapcsolattartás szabályai:

a) Személyes vagy intézményi adatok kiadása, csak a hatályos jogszabályoknak megfelelően történhet.
b) Az átadott adatok védelméért a szerződő fél tartozik felelősséggel
c) A kapcsolattartó információbiztonsági kérdésekben az EIO, vagy az EISZK Biztonsági Megbízottjától, a személyes adatok védelmével kapcsolatos kérdésekben az Egyetem adatvédelmi felelősétől kérhet tanácsot.

Ügyfelekkel kapcsolatos informatikai biztonsági feladatok (jogosultság kiadás felhasználóknak)

22. § Kritikus, kiemelt, normál rendszerek esetében az installálási időszakon kívüli partner hozzáférést az üzemeltetők eseti kérelme alapján az üzemeltető szervezeti egység vezetője, vagy az általa megbízott felelős engedélyezheti. A kérelemnek tartalmaznia kell az ügyfél adatait, a hozzáférés indokát, módját, paramétereit és tervezett időtartamát. Engedély nélküli hozzáférés biztosítása esetén az adott informatikai rendszer nem minősül szabályzat megfelelőnek.

Harmadik féllel kötött megállapodások biztonsági kérdései

23. § Minden harmadik féllel kötött megállapodás esetében a megállapodásban rögzítendők az adatvédelmi és informatikai biztonsági kérdések.

III. fejezet

Az információvagyon menedzsmentje

Felelősség az információvagyonért

Az információvagyon leltárja

24. § Az egyetem a kritikus, kiemelt, normál kategóriájú rendszereinek nyilvántartását és az általuk biztosított szolgáltatások nyilvántartását az üzemeltetési szervezet hovatartozásától függően az EIO, vagy az EISZK Biztonsági Megbízottja végzi. Az ehhez szükséges adatszolgáltatás a rendszerek üzemeltetőinek a kötelezettsége.

Az információs vagyon tulajdonjoga

25. § Az Egyetem valamennyi informatikai rendszerének intézmény-specifikus konfigurációs adatai és beállításai (minden olyan konfigurációs komponens, ami a vásárolt rendszerben található állapottól eltér) az Egyetem tulajdonát képezik. Ugyanezen rendszerekben tárolt minden intézményi adat (és annak minden felhasználási joga) is az Egyetem tulajdona.

Az információs vagyon használatának szabályai

26. § (1) Minden alkalmazott és üzleti partner a számára meghatározott jogosultsággal léphet be a különböző rendszerekbe. A jogosultság változását az alkalmazottak esetében a felettesnél, üzleti partner esetében a megbízó szervezeti egység vezetőjénél kell kezdeményezni.

(2) Az SLA-ban kell rögzíteni a különböző szolgáltatásokkal kapcsolatos információvagyon és jogosultságkezelési használati szabályokat. Mindenfajta változtatás az SLA-k változtatási rendjének megfelelően végezhető.

(3) Adatok kiadása a különböző biztonsági osztályba sorolt rendszerekből csak az üzemeltetést végző szervezeti egység vezetőjének engedélyével lehetséges. Kivételt képez azaz eset, amikor az adatcserét, adatátadást vállalkozói szerződés rögzíti. Ebben az esetben a szerződésnek tartalmaznia kell az adatkezelésre vonatkozó szabályokat is. Ha a kiadandó adat személyes adatnak minősül, akkor az csak az Egyetem adatvédelmi szabályzata szerint továbbítható.

Az információvagyon osztályozása

Az osztályozás elvei, vezérfonala

27. § Az információvédelem területén történő osztályozás az adatok minőségi szintjével növekvő mértékű, a bizalmasság, hitelesség és a sértetlenség sérüléséből vagy elvesztéséből származó kárszinteken alapul.

a) Információvédelmi alapbiztonsági osztály:

Oktatással összefüggő és oktatási adatok, valamint ügyviteli adatok biztonsági osztály.

b) Információvédelmi fokozott biztonsági osztály:

Személyes, minősített, pénzügyi adatok, valamint üzleti titkok biztonsági osztálya.

Az osztályba sorolt információs vagyonelemek jelölése és kezelése

28. § Az információs vagyonelemek besorolása, jelölése a szabályzat 5. §-ban leírtak szerint történik és végrehajtásáért az EIO, illetve az EISZK Biztonsági Megbízottja a felelős.

IV. fejezet

Emberi erőforrással kapcsolatos biztonsági kérdések

Informatikai biztonság a felvételnél

29. § (1) A kritikus és kiemelt osztályú rendszerek üzemeltetőinek felvételi eljárása során – törvényes keretek között – olyan vizsgálatokat kell lefolytatni, melyek egyértelmű képet adnak a jelentkező informatikai biztonság oldaláról tekintett alkalmasságáról. A munkavállalótól csak olyan nyilatkozat megtétele, vagy olyan adatlap kitöltése kérhető, illetve vele szemben csak olyan alkalmassági vizsgálat alkalmazható, amely a személyiségi jogait nem sérti, a munkaviszony szempontjából lényeges tájékoztatást nyújthat és ahhoz az érintett írásban hozzájárult.

(2) A foglalkoztatás alapvető biztonsági feltételei az általános és a munkakörre vonatkozó speciális biztonsági előírások megismerése, elfogadása, valamint a munkavállaló részéről a Titoktartási Nyilatkozat aláírása.

Alkalmazás alatti tennivalók

30. § (1) A kritikus, kiemelt, normál rendszerek esetében minden üzemeltető, fejlesztő, vagy felhasználó csak a munkaköri leírásában rögzített feladatok ellátásához szükséges jogosultságokat birtokolhatja. (Azon fejlesztői rendszerek, amik személyes, vagy intézményi adatokat nem tartalmaznak, nem minősülnek kategorizált rendszernek).

(2) A kritikus és a kiemelt osztályú rendszerek bizonyos szolgáltatásainak igénybevételéhez (pl. gazdasági rendszer) a rendszer által kiszolgált szervezeti egység vezetője tanfolyam és/vagy vizsga teljesítését írhatja elő. A kritériumok teljesítésének költsége az intézményt terheli.

(3) A szabályzat előírásainak szándékos és tudatos megsértése esetén az alkalmazott az Egyetem Informatikai Üzemeltetési Szabályzatának 5. §-ban leírtak szerint szankcionálható.

Elbocsátás vagy munkakörváltozás

31. § (1) A dolgozó elbocsátása esetén minden kritikus, kiemelt, normál rendszer esetében az üzemeltetői, fejlesztői és felhasználói jogosultságokat, ilyen tevékenységet lehetővé tevő belépési kódokat azonnal vissza kell vonni, amit az adott szolgáltatás vezetőjénél a dolgozó munkáltatójának kell kezdeményeznie.

(2) Amennyiben a volt dolgozó a fenti tevékenységet céges partnerként végzi a továbbiakban, akkor a szerződés megkötése után új, partneri hozzáférés biztosítható a számára az ott részletezett szabályok alapján.

(3) Az elbocsátott dolgozó a normál és egyéb kategóriájú rendszerekben a (kizárólag) személyes adatainak elérésére szolgáló belépési kódjait a munkáltatójának eseti engedélye alapján megtarthatja.

V. fejezet

Fizikai és környezeti biztonság

Biztonsági zónák, területek

Fizikai biztonsági határvédelem

32. § (1) A kritikus és a kiemelt kategóriájú szolgáltató rendszer kritikus fizikai komponensei (szerver, tároló alrendszer, router, stb.) csak külön erre a célra kialakított, megfelelő biztonsági paraméterekkel rendelkező helyiségekben működtethetők. A helyiségeknek biztonságos mechanikus zárakkal (biztonsági zár, vagy beléptető kártyával működtethető zár) és beléptető rendszerrel kell rendelkezniük.

(2) A beléptető rendszer szükséges alapkonfigurációi: belépő személy azonosítása kód vagy kártya alapján, belépési jogosultság megállapítása, belépési időpont regisztrálása, jogosulatlan belépés jelzése a biztonsági személyzet felé. A C kategóriájú rendszerek estében minimálisan biztonsági zárral ellátott helyiséget kell biztosítani, a kulcsokról és a belépésekről írásos helyiségnaplót kell vezetni.

Fizikai belépés szabályozás

33. § (1) A kritikus, kiemelt, normál kategóriájú rendszerek komponenseit tartalmazó szolgáltató helyiségekbe (géptermek, kábelrendezők, stb.) való belépési jogosultságot az üzemeltetés felelős vezetője engedélyezi a dolgozónak vagy a partnernek, a helyiségek és a végezhető munka felsorolásával. A belépési lehetőséggel rendelkezők ezen jogosultságukat nem ruházhatják át másik dolgozóra, vagy partnerre.

(2) Jogosulatlan személy beengedéséből fakadó eseményekért a felelősség a beengedő személyt terheli. Az illegálisan szerzett belépési lehetőség használata betörésnek minősül és jogi következményeket von maga után.

Irodák, szobák és egyéb létesítmények fizikai biztonsága

34. § (1) Az informatikai rendszerek működtetéséhez szükséges egyéb munkaterületek használatának módja megegyezik az általános egyetemi területek használati módjával.

(2) Kitüntetett hozzáférést vagy védett adatokat tartalmazó kiegészítő rendszerkomponensek (mentési berendezés, fejlesztői rendszer, felügyelő terminál, stb.) csak beléptető rendszerrel védett munkaszobában, irodában helyezhető el.

(3) Az informatikai célú helyiségekkel kapcsolatos kérdésekben a laborvezető, vagy üzemeltetés vezető a felelős a ki- és átalakítás koordinációjáért, a szakmai biztonsági szempontok betartásáért.

Külső és környezeti károk elleni védelem

35. § (1) A kritikus, kiemelt, normál kategóriájú szolgáltató rendszer kritikus fizikai komponensei csak a hatályos szabályozásnak megfelelő tűz- és villámvédelmi rendszerrel felszerelt helyiségekben üzemeltethetők. Talajszinten, vagy az alatt elhelyezkedő helyiségek estében a vízkár védelméről intézkedni kell.

(2) A tűzvédelmi rendelkezéseknek megfelelően az erősáramú ellátó rendszernek tartalmaznia kell olyan központi feszültségmentesítő kapcsolót, ami tűzjelzés esetén a biztonságos oltás feltételeit megteremti. A megfelelőségről az adott berendezés üzemeltetéséért felelős vezető köteles gondoskodni.

(3) Minden fenti helyiség esetén biztosítani kell azt a gépészeti hűtési kapacitást, ami a teljes termelt hőmennyiség biztonságos elvezetését automatikusan meg tudja oldani. Hasonló módon biztosítani kell azt az erősáramú ellátó kapacitást, ami a berendezések villamos energia ellátását túlterhelésmentesen el tudja látni. Az erősáramú ellátó rendszernek áramkör – szelektív túlterhelés védelemmel kell rendelkezniük.

Munkavégzés biztonsági zónákban

36. § (1) A minősített rendszereket tartalmazó helyiségekben minden olyan munkavégzés, ami az informatikai rendszereket, vagy azok működését veszélyezteti, csak előzetes egyeztetés alapján, felügyelet mellett végezhető. Az egyeztetést, a munkálatokat végző szervezeti egység vagy cég és az üzemeltető szervezeti egység felelős vezetője végzi.

(2) A helyiség gépészeti berendezéseinek működését veszélyeztető munkák csak az informatikai erőforrások üzemeltetéséért felelős személy előzetes engedélyével folytathatók.

Nyilvános hozzáférés, szállítási területek

37. § Minősített rendszereket tartalmazó helyiségekben minden szállítási tevékenység csak belépésre jogosult munkatárs felügyelete mellett végezhető.

Eszközbiztonság

Eszközök elhelyezése, védelme

38. § Minden minősített rendszerkomponens fizikai elhelyezésénél be kell tartani a gépterem/labor/kábelrendező felépítési elveit (pl.: rackben történő elhelyezés, ventilláció iránya, stb.) Ezen irányelveket az üzemeltetés felelős vezetője írja elő.

Támogató közművek (szolgáltatások)

39. § A gépterem/labor/kábelrendező helyiségekben üzembe állítandó új rendszerek, vagy nagyobb rendszerkonfiguráció módosítás esetén az installálást végző szakembereknek előzetesen konzultálniuk kell az erősáramú és hűtési igény biztosításáról az üzemeltetés felelős vezetőjével. A szükséges gépészeti módosításokat az új rendszer üzembe állítása előtt el kell végezni.

Kábelbiztonság

40. § A kiemelt rendszerek védett helyiségen kívül húzódó, összekötő komponenseit (telefon és gerinchálózati kábeleket) tartalmazó egyetemi tulajdonú alépítmények, kábelaknák és védőcsövek, az EIO, vagy az EISZK által felügyelt területnek minősülnek. Azokban munkát végezni, vagy a megközelíthetőségüket korlátozni, csak a rendszerkomponens üzemeltetőjének előzetes engedélyével lehet.

Eszközkarbantartás

41. § (1) Minden szolgáltató rendszer üzemeltetője köteles a hardver komponensek karbantartási igényét felmérni és ezeket úgy ütemezni, hogy a rendszer élettartama ne rövidüljön a karbantartási hiányosságok miatt.

(2) A gépészet külön karbantartási tervvel rendelkezik, amit a létesítményfelelős az üzemeltetés vezetőjével egyeztetve állít össze és gondoskodik a végrehajtásáról.

(3) A karbantartás során a felmerült biztonsági sérülékenységeket megfelelően kell kezelni, illetve úgy kell a karbantartásokat elvégezni, hogy újabb biztonsági kockázatok ne merüljenek fel. Ennek felelőse a karbantartást végrehajtó személy, vagy szervezet.

Telephelyen kívül használt eszközök biztonsági szabályai

42. § A telephelyekről kivitt eszközök használata során bekövetkező károkért az a személy viseli a felelősséget, aki az eszközt kivitte. A telephelyen kívüli használat, munkavégzés során mindazon elvek és gyakorlat követendő, amelyeket a szabályzat egyes fejezetei leírnak.

Eszközök biztonságos megsemmisítése vagy újrahasznosítása

43. § (1) A használhatatlan, vagy elavult eszközök selejtezése az Egyetem hatályos szabályainak figyelembe vételével történik.

(2) Speciális eszközök selejtezése esetén az üzemeltető gondoskodik a szakszerű elhelyezésről, illetve átadás-átvételi jegyzőkönyv alapján ezt a tárolási feladatot átadhatja a Gazdasági Főigazgatóság selejtezési csoportjának.

(3) A kritikus, kiemelt, normál kategóriás eszközök selejtezésénél gondoskodni kell az azon tárolt adatok selejtezés előtti fizikai megsemmisítéséről.

Eszközök kivitele telephelyről

44. § (1) Az eszközök épületből történő kiszállítását az egyetemen rendszeresített 3 példányos kiviteli engedéllyel kell kísérni, amelyből egy példány a kivitt eszköz leltárfelelősénél, egy példány a kiléptető portán a portaügyeletnél és egy példány a kiszállítást végzőnél marad. A kivitelt a felelős vezető az eszköz leltárfelelősével előzetesen egyeztetve a kiviteli engedélyen aláírásával engedélyezi.

(2) Az épületbe történő beszállítást szállítólevéllel kell kísérni. Mind a kiviteli engedélyen, mind a szállítólevélen az eszköz(ök) egyedi azonosítóját (ha értelmezhető) fel kell tüntetni.

VI. fejezet

Kommunikáció és üzemelés menedzsment

Működési folyamatok és felelősségek

45. § (1) Amennyiben egy szervezeti egység szolgáltatás-indítási kérelemmel fordul az EIO, vagy az EISZK vezetőjéhez, ezzel elismeri megfelelési szándékát az Egyetem Informatikai Üzemeltetési Szabályzat vagy jelen szabályzat kritériumainak.

(2) A szolgáltatás-indítási kérelem csak adathiány, vagy Informatikai Üzemeltetési Szabályzat és jelen szabályzat megsértése esetén utasítható el. Az elutasítást részletesen indokolnia kell az EIO, vagy az EISZK vezetőjének, nem kizárva az esetleges módosított kérelem újbóli beadását.

(3) Minősített rendszerek estében az Informatikai Üzemeltetési Szabályzatnak és jelen szabályzatnak való megfelelést az EIO, illetve az EISZK esetileg vizsgálhatja és esetleges hiánypótlásra az üzemeltetőt felszólíthatja.

(4) Minden informatikai rendszer esetében a használatra vonatkozó igény bejelentése (hozzáférés, vagy felhasználói azonosító igénylése) a szolgáltatási SLA elfogadásának szándéknyilatkozatát is jelenti. A hozzáférés megadásával az SLA a szolgáltató és igénybevevő között életbe lép.

46. § Az Informatikai Üzemeltetési Szabályzat szerinti kritikus és kiemelt osztályú rendszerek esetében az SLA-ban vállalt szolgáltatási és rendelkezésre állási paraméterek alulteljesítése miatt az intézményt anyagi és egyéb kár érheti. Ilyen esetben a felelősség és a szükséges lépések megtételére az EIO, vagy EISZK vezetője eseti bizottságot nevezhet ki. Ennek a bizottságnak a szolgáltató szervezeti egység hovatartozásától függően mindig tagja az EIO, vagy az EISZK Biztonsági Megbízottja.

Harmadik fél által nyújtott szolgáltatások menedzsmentje

47. § A harmadik fél által nyújtott informatikai szolgáltatások is SLA kötelezettek, a kritikus paramétereket a partnerrel kötött szolgáltatási szerződésben is rögzíteni kell. A szerződésnek ki kell terjedni az információbiztonsági kérdésekre is.

Rendszertervezés és elfogadás

48. § Az informatikai szolgáltató rendszerek esetében az Informatikai Üzemeltetési Szabályzatnak és jelen szabályzatnak való megfelelést már a tervezési szempontok között szerepeltetni kell. A kritikus, kiemelt, normál osztályú rendszerek esetében az Informatikai Üzemeltetési Szabályzatnak és jelen szabályzatnak megfelelés a szolgáltatás indításának szükséges feltétele. Az Egyetem információs rendszerei esetében a szolgáltatás megindítását a szolgáltatási területtől függően az EIO, vagy az EISZK vezetője engedélyezi a Biztonsági Megbízott javaslata alapján.

Védekezés vírusok és egyéb kártékony kódok ellen

49. § (1) Minden olyan rendszer esetében, ahol vírusfenyegetés fennáll és lehetséges installálni vírusvédelmi rendszert, valamint kémprogram jelző komponenst, akkor ott ezek megtörténte és folyamatos alkalmazása a szolgáltatás üzembe helyezésének és az üzemeltetésnek feltétele.

(2) Publikus levelező rendszerek esetében az intézményen kívüli kapcsolat létesítésének feltétele a levelek informatikailag veszélyes tartalmának folyamatos vizsgálata, illetőleg a feltétel nélküli továbbítás (open relay) lehetőségének kiküszöbölése.

(3) Felhasználói tulajdonú adathordozók, alkalmazások, és adatok használata esetén annak használata következtében okozott károkért az Egyetem rendszereiben, a felhasználóként belépett személy a felelős.

Biztonsági mentések

50. § (1) Minden kritikus, kiemelt osztályú szolgáltató rendszer leírásának tartalmaznia kell az alkalmazások és adatok mentési rendjét (a mentendő adatok körét, a mentés módját és gyakoriságát, a mentésért felelős személyt, a mentés tárolási rendjét).

(2) Kritikus osztályú rendszerek esetén telephelyen kívüli tárolású (offsite) mentésekkel is kell rendelkezni, kiemelt és normál osztályú rendszerek esetén telephelyen belüli tárolású (onsite) mentések is elfogadhatók.

(3) A mentési rendnek az alkalmazásra vonatkozó részét úgy kell megállapítani, hogy a rendszer működőképessége tetszőleges komponens meghibásodása vagy adatvesztése esetén is helyreállítható legyen. Ennek érdekében az alkalmazás futó kódját legalább minden release váltás előtt és után menteni kell, a mentést minimum 3 release-re vagy egy évre visszamenőleg meg kell őrizni.

(4) Az alkalmazások és rendszerek konfigurációs beállításait minden változás esetén, de leggyakrabban naponta kell menteni. A mentési eljárásnak lehetővé kell tennie egy adott állapot célirányos betöltését. A konfigurációs mentéseknek 10 előző állapotra, ill. minimum az előző 30 szolgáltatási napra ki kell terjedniük.

(5) A kritikus osztályú rendszerek esetében az alkalmazásokban tárolt intézményi adatokat minden munkanap végén menteni kell. A mentést heti gyakorisággal a teljes adattartalomra el kell végezni. A mentési módnak lehetővé kell tennie ezen adatok tesztrendszerbe történő betöltését.
A normál osztályú rendszerek esetében az adatok mentése is megengedett eljárás. Az alkalmazás üzemeltetője belátása szerint bármikor jogosult eseti mentés indítására, amennyiben az nem jár a szolgáltatás aránytalanul nagyfokú megzavarásával.

(6) Minden kritikus, kiemelt, normál osztályú rendszer esetében évente minimum egy alkalommal visszatöltési gyakorlatot (tesztelés) kell tartani, ami a mentések felhasználhatóságát ellenőrzi. A

visszatöltési gyakorlat a szolgáltató rendszerrel funkcionálisan egyező tesztrendszeren is teljesíthető. A mentések meglétét és a visszatöltési gyakorlatot az EIO, vagy az EISZK Biztonsági Megbízottja ellenőrizheti.

(7) Az archiválás kritériumai:
a) visszakereshető,
b) jogszabályi kötelezettségen alapul (az SLA-nak megfelelően),
c) kizárja az utólagos módosítás lehetőségét,
d) hiteles (azonosítható, letagadhatatlan, megváltoztathatatlan).

Hálózatbiztonság menedzsmentje

51. § Az Egyetem teljes területére kiterjedő gerinchálózati infrastruktúra (számítógépes és telefon) védelme egységes koncepció és megvalósítás mellett történik. Az irányelvek és módszerek meghatározását, valamint a szükséges operatív beavatkozásokat a hálózat üzemeltetésével megbízott EISZK – szükség esetén az EIO-val egyeztetve - szervezeti egység végzi. A kommunikációs hálózathoz történő csatlakozás feltétele a biztonsági előírások maradéktalan betartása. Ezen előírások a csatlakozásnak, mint szolgáltatásnak az igénybevételi feltételei között tekinthetők meg a vonatkozó SLA-kban.

Adathordozók kezelése

52. § (1) A különböző rendszerek adatállományainak mentései intézményi és személyes adatokat tartalmazhatnak, ezért ezen adathordozókra a rendszer osztálybasorolásának megfelelő biztonsági követelményeket kell alkalmazni.

(2) A biztonsági mentésre szolgáló adathordozókról nyilvántartást kell vezetni.

(3) A mentések adathordozóinak használatból történő kivonása és megsemmisítése a szolgáltatást biztosító üzemeltető feladata. A megsemmisítésről jegyzőkönyvet kell felvenni.

Információcsere

53. § (1) Az Egyetem kritikus, kiemelt, normál osztályú rendszerei esetében az automatikus adatcserét lehetővé tevő kapcsolatok létesítéséhez a szolgáltatás jellegétől függően az EIO, vagy az EISZK vezetőjének engedélye és az érintett adatgazda hozzájárulása szükséges. A kérelemben az alkalmazások üzemeltetőinek részletezni kell az elérendő adatkezelési célt és az alkalmazott informatikai megoldást, különös tekintettel a jogosulatlan adatcserét kizáró biztonsági megoldásokra.

(2) Az adatcsere környezetét, technológiai megvalósítását dokumentálnia kell az adatcserét kezdeményező alkalmazásüzemeltetőnek.

Monitorozás

54. § A kritikus és kiemelt osztályú rendszerek esetében az üzemeltetők felelőssége az automatikus szolgáltatás monitorozó komponensek bevezetési lehetőségének vizsgálata és a monitorozás megvalósítása.

Hozzáférés szabályozása

Működési követelmények a hozzáférés szabályozása érdekében (hozzáférési politika)

55. § (1) Minden olyan informatikai rendszer esetében, ami az Egyetem működéséhez szükséges, illetőleg bármilyen védett információt tartalmaz, meg kell határozni a hozzáférésre jogosultak körét és hozzáférési kísérlet esetén a jogosultságot ellenőrizni kell.

(2) Informatikai rendszerekhez, módosítást és védett adatok lekérdezését lehetővé tevő hozzáférésre, kizárólag másik rendszer vagy természetes személy lehet jogosult. Természetes személyek egy csoportja, közös használatú hozzáférési lehetőséget kizárólag publikus adatok lekérdezésére gyakorolhat.

(3) A jogosultság kezelést napra készen kell tartani és dokumentálni.

Felhasználói hozzáférés menedzsmentje

56. § (1) Az adott informatikai rendszerhez történő hozzáférés módját (igénybe vételre jogosultak köre, igénylés módja, igénylés elbírálása) a rendszeren működő szolgáltatások SLA-i tartalmazzák. Az igénylés során a természetes személynek azonosítania kell magát egyedi adatával, vagy adat párjával.

(2) Lehetőség szerint az informatikai rendszerek felhasználóinak azonosítása és jogosultság elbírálása központilag, erre a célra szolgáló rendszerrel történjen (ETR) és a felhasználói adatbázis kezelése egységesen és konzisztensen valósuljon meg. Kivételt azon már meglévő rendszerek képezik, amelyek nem képesek központi jogosultság kezelést megvalósítani.

(3) A szolgáltatási SLA megszegése esetén a felhasználó az adott szolgáltatásból kizárható. Kizárás esetén a felhasználót ennek tényéről, a kizárás időtartamáról, a problémát okozó tevékenységéről és a követendő magatartásról tájékoztatni kell. Ha a felhasználó által okozott kár csekély, akkor első alkalommal csak figyelmeztetésben kell részesíteni.

(4) A Kritikus és kiemelt rendszerek esetében az üzemeltető a hozzáférésre jogosultak esetében is előírhat engedélyezési eljárást a hozzáférés megadásához (pl.: a kérelmező munkáltatója által). Az engedélyt írásban, a kért jogosultságokat feltüntetve kell az üzemeltetőknek eljuttatni. Minden kritikus, kiemelt, normál rendszer esetében az üzemeltető feladata, hogy a kiadott hozzáférések adatait (név, alkalmazás, jogosultsági szint, kiadás dátuma, indoka) naprakészen nyilvántartsa.

Felhasználói felelősségek

57. § (1) A szolgáltatás felhasználója teljes felelősséggel tartozik az adott szolgáltatás SLA-jában általa vállalt kötelezettségek betartásáért, beleértve a korlátos erőforrások pazarlása miatt az üzemeltetőnél keletkező többletköltségeket is.

(2) A felhasználó a munkaköri leírásban meghatározottak alapján kezelheti az intézményi adatokat, azok bizalmas kezelése munkaköri kötelessége. Az intézményi rendszert köteles csak munkakörének megfelelően, erőforrás-kímélő módon, a kezelési utasításoknak megfelelően használni.

Hálózati hozzáférés

58. § (1) A számítógépes hálózatra történő fizikai csatlakozás csak az üzemeltető által elfogadott igénylés után, az abban megadott paraméterekkel lehetséges. A jogosulatlan csatlakozást az

üzemeltető a rendszer integritásának védelmében azonnal megszünteti. A csatlakozási lehetőségek és az igénylés módját a hálózati szolgáltatások SLA-i tartalmazzák.

(2) A hálózati szolgáltatások SLA-iban szereplő feltételrendszer az üzembiztonság, a nyomon követhetőség és központi kezelhetőség szempontjai szerint van kialakítva, ezért az SLA be nem tartása a rendszer egészét, a többi felhasználó szolgáltatási környezetét veszélyezteti. Emiatt az SLA-t megszegő felhasználó a hálózati szolgáltatásokból utólagos figyelmeztetés mellett is kizárható.

(3) Az Internet bármely komponenséhez történő hozzáférés esetén a felhasználó köteles az egyetem Internet-szolgáltatójának szabályzatát (HBONE AUP) betartani, valamint az Internet közösség etikai irányelveit, mások vallási, politikai és erkölcsi nézeteit tiszteletben tartani.

(4) Az Internet hozzáférési pontokat jellemző forgalmi adatokat (fizikai cím, IP cím, felhasználónév hozzárendeléseket) amennyiben az műszakilag lehetséges, naplózni kell. Ennek biztosítása a szolgáltató felelőssége. Az adatokat 6 hónapig meg kell őrizni, utána törölni kell.

(5) A tartalmi adatok naplózása tilos. A naplózás során személyes adatok kizárólag a felsőoktatásról szóló 2005. évi CXXXIX. törvényben meghatározott célokból, így különösen a juttatások, kedvezmények, kötelezettségek megállapításával és teljesítésével, az intézmény rendeltetésszerű működésével és a képzés megszervezésével kapcsolatosan, a célnak megfelelő mértékben, célhoz kötötten kezelhetők.

Operációs rendszer hozzáférés

59. § Az SLA köteles szolgáltatások operációs rendszereiben a felhasználók kizárólag egyértelmű azonosítás után végezhetnek munkát. A hozzáférés tényét, időtartamát és forrását a rendszernek visszakereshető módon naplóznia kell az SLA-ban meghatározottak szerint, illetve minimum egy hónapig.

Alkalmazásokhoz és információkhoz történő hozzáférés szabályozása

60. § (1) Az intézményi adatokhoz történő hozzáférést lehetővé tevő alkalmazások jogosultsági köreit olyan módon kell kialakítani, hogy az alkalmazottak csak a munkakörükkel kapcsolatos adatokat láthassák, illetve kezelhessék.

(2) Az intézményi adatokhoz történő hozzáférést, ezen adatok módosítását alkalmazás szinten is – visszakereshető módon – naplózni kell. Az adatokat 6 hónapig meg kell őrizni, utána törölni kell.

(3) Az alkalmazásokban tárolt személyes adatokhoz való hozzáférés tekintetében az Adatvédelmi Szabályzat irányadó.

Hozzáférés forrásának szabályozása

61. § (1) A kritikus rendszerekhez történő tetszőleges, illetve a kiemelt osztályú rendszerekhez történő menedzsment hozzáférés kizárólag az intézményi belső hálózatból (intranet) lehetséges. A normál osztályú rendszerek menedzsment hozzáférése megfelelő titkosítással bíró adatkapcsolattal külső hálózatból is megengedett. Minden egyéb hozzáférési kísérlet incidensnek minősül és informatikai megoldásokkal is akadályozni kell az üzemeltetők részéről.

(2) Speciális hálózati szolgáltatásokkal (pl. VPN) az intranet az Egyetem fizikai hálózatán kívülről is hozzáférhető, ezáltal a munkahelyen kívüli munkavégzés lehetséges. Ezen megoldások felhasználó által történő önálló megvalósítása nem megengedett, kizárólag az intézmény ilyen jellegű szolgáltatásai vehetők igénybe. Az intranet védelmi megoldásainak megsértése a hálózati hozzáférés

nem megfelelő használatával (pl, saját átjáró, külső hálózati kapcsolat felhasználó általi létesítése) az SLA súlyos megsértésének minősül.

(3) A kritikus és kiemelt osztályú rendszerek tartalmazhatnak olyan felhasználói felületet szolgáltató komponenst, melynek célja az internetből való hozzáférés biztosítása (pl. ETR hallgatói WEB felület). Az SLA-ban a rendszer ilyen szolgáltatását külön meg kell határozni és a hozzáférés feltételeit külön szabályozni. Az ilyen felület nem nyújthat az alkalmazás adminisztrációjára vagy az adatok széles körű (nem a bejelentkező személyhez kapcsolódó) lekérdezésére vonatkozó szolgáltatásokat.

VII. fejezet

Információs rendszerek beszerzése, fejlesztése és karbantartása

Információs rendszerek biztonsági követelményei

62. § (1) Új rendszerek megvalósítása során a biztonsági követelményeket előzetesen meg kell határozni, és a szolgáltatásindítási kérelemhez mellékelni kell.

(2) A már működő rendszerek továbbfejlesztése, módosítása során a biztonsági követelmények nem változtathatóak olyan irányban, hogy a rendszer biztonsági szintje csökkenjen.

Alkalmazások helyes használata

63. § (1) A kritikus osztályú alkalmazásokhoz kizárólag azon felhasználók férhetnek hozzá, akiknek az intézményi szerepük ezt megkívánja és legfeljebb olyan jogosultsággal, amit a munkakörük maradéktalan ellátása indokol. Nevesítve:

a) rendszer üzemeltetői (üzemeltetői jogosultsággal),
b) rendszer felhasználói (felhasználói jogosultsággal).

(2) A rendszer fejlesztői a szolgáltató alkalmazáson nem rendelkezhetnek üzemeltetői jogosultságokkal, mivel ez az ő munkakörük ellátásához nem szükséges (éles üzemű rendszerben fejlesztés nem történhet).

Kriptográfiai szabályozások

64. § (1) A kritikus és kiemelt osztályú rendszerekbe történő, módosítási jogosultságot is lehetővé tevő bejelentkezés csak titkosított kommunikációval (pl. SSH, SSL, VPN) engedélyezett, kivéve azon bejelentkezési területeket, ahol a felhasználó munkahelye és a szolgáltató rendszer közötti hálózat külső fél általi lehallgatása technikailag nem lehetséges (pl. fizikai védelem miatt).

(2) A hozzáférési jogosultságok elbírálását végző komponensek bármely rendszer esetében a felhasználói jelszavakat csak titkosítva tárolhatják.

(3) Egyéb kriptográfiai szabályozások az adott szolgáltatás SLA-jában rögzítendők.

Rendszer fájlok biztonsága

65. § (1) A szolgáltató rendszer működését biztosító rendszer fájlokhoz a felhasználók csak olyan mértékben férhetnek hozzá, amit a szolgáltatás használata megkövetel. A szolgáltatás szempontjából kritikus rendszerfájlok felhasználók általi módosítása csak az üzembiztonságot ellenőrző köztes felületen lehetséges.

(2) A rendszer fájlok védelme az üzembiztos konfiguráció megőrzése és helyreállíthatóságának biztosítása az üzemeltető rendszergazdák munkaköri kötelessége.

Fejlesztési és támogatási folyamatok biztonsága

66. § (1) Minden alkalmazás fejlesztési tevékenységet a szolgáltató alkalmazás példányától és annak adatbázisától elkülönülten kell végezni. Amennyiben a fejlesztési tevékenységhez védett intézményi adatok is szükségesek, akkor a fejlesztői rendszer is az adatoknak megfelelő osztályú rendszernek minősül és a hozzáférési jogosultságok is ennek megfelelően adhatók ki.

(2) Egyetemi fejlesztésű vagy vásárolt szolgáltató rendszer csak funkcionális teszt után vonható szolgáltató üzembe. A funkcionális tesztnek az SLA-ban rögzített minden paraméterre és funkcióra, valamint tipikus felhasználási mintákra ki kell terjednie. A funkcionális tesztről írásos jegyzőkönyvnek kell készülnie, melynek az összes mért és ellenőrzött paramétert és funkciót tartalmaznia kell.

(3) Minden, a szolgáltatási felületben vagy a funkciókészletben különbséget tartalmazó alkalmazás verzió esetén a tesztelési eljárást újra el kell végezni. A tesztelési kötelezettség az operációs rendszerek, adatbázis kezelők és egyéb támogató alkalmazások (pl. web szerver) esetén is fennáll, de csak a használt funkciókra kell kiterjednie.

(4) Szolgáltató üzemben működő alkalmazáson csak sikeres tesztelési jegyzőkönyv birtokában és az üzemeltető rendszergazda engedélyével végezhető változtatás (külső munkavégző cég esetében is). Ezen előírás alól csak a szolgáltatás helyreállítását célzó sürgős hibajavítás jelent kivételt, ami esetében a dokumentálást utólag kell elvégezni.

Műszaki sérülékenység menedzsment.

67. § Az adott alkalmazás üzemeltetőjének felelőssége a publikált technikai sérülékenységek elleni védekezés megvalósítása. A publikált sérülékenységek elleni védekező intézkedés az észlelést követő első munkanapon végrehajtandó.

VIII. fejezet

Információbiztonsági események menedzsmentje

Biztonsági események és gyengeségek jelentése

68. § (1) Minden szolgáltató rendszer esetében a szolgáltatás üzemeltetője köteles incidens bejelentési kötelezettséget biztosítani a felhasználóknak, és a bejelentés módját az SLA-ban közzétenni. A bejelentett incidenseket az üzemeltetők a szolgáltató rendszer integritásának és a kezelt adatoknak a védelmében kötelesek a rendszer osztályba sorolásától függően rövid reakcióidővel elbírálni és a szükséges lépéseket megtenni. Az üzemeltető köteles a bejelentőt tájékoztatni a biztonsági esemény következményeiről és a megtett intézkedésekről. Tömeges érintettség esetén lehetőség van az egyetem központi hírcsatornáinak használatára is.

(2) Biztonsági esemény, vagy gyengeség bejelentése esetén a bejelentő köteles csatolni mindazon adatokat, amik az esemény megítéléséhez legjobb tudása szerint szükségesek.

(3) A szolgáltatások felhasználása közben tapasztalt gyengeségek jelentése (a rendszer működőképességének fenntarthatósága érdekében) minden felhasználónak kötelessége. Ennek elmulasztása vagy a gyengeség kihasználása biztonsági eseménynek minősül.

Információbiztonsági események és fejlesztések menedzsmentje

69. § (1) Az informatikai szolgáltató rendszerek esetében egyenszilárdságú biztonsági megoldásokat kell kialakítani. Rendszerenként egységes tervezés és megvalósítás alapján kell a biztonsági megoldásokat kezelni. Amennyiben egy informatikai rendszer egy másik szolgáltatását igénybe veszi, akkor a szolgáltatási SLA biztonsági követelményei az igénybevevő rendszer egészére vonatkoznak.

(2) A megvalósítandó, vagy üzemben álló szolgáltató rendszer rendszertervének az alkalmazott és a felhasználók számára előírt biztonsági megoldásokat is tartalmaznia kell. Amennyiben ezek a változó körülmények miatt nem bizonyulnak elegendőnek, a rendszer fejlesztési tervében szerepeltetni kell az új biztonsági rendszer tervezett megoldásait.

Működés - folytonosság biztosítása

A működés folytonosság információbiztonsági vetülete

70. § Az Egyetem működése szempontjából kritikus, kritikus és kiemelt osztályú rendszerek működésfolytonosságának biztosítása az üzemeltető feladata. Ez kiterjed az SLA-k feltételrendszerének körültekintő meghatározására, a felelős incidenskezelésre, a szükséges funkcionális és biztonsági javítások telepítésére a szabályzat betartására, valamint a rendszer fejlesztési terveinek erőforrás-kalkuláción alapuló körültekintő elkészítésére.

IX. fejezet

Megfelelőség

Jogszabályi megfelelőség

71. § A nyújtott szolgáltatások vonatkozásában a mindenkori jogszabályi megfelelőség biztosítása a szolgáltatást végző szervezeti egység vezetőjének a felelőssége. Ezen szervezeti egység vezetője nem felel a felhasználók által elkövetett jogsértésekért és hatósági megkeresés esetén a jogszabályban előírt adatokat az adott felhasználóval kapcsolatban az Adatvédelmi Szabályzatban meghatározottak szerint ki kell adnia

Megfelelés a biztonsági politikának, szabványoknak és műszaki előírásoknak

72. § A szolgáltatást végző szervezeti egység vezetőjének a felelőssége a mindenkori biztonsági politikának, szabványoknak és műszaki előírásoknak való megfelelőség biztosítása a nyújtott szolgáltatások vonatkozásában.

Információs rendszerek felülvizsgálatával kapcsolatos megfontolások

73. § (1) Az Informatikai Üzemeltetési Szabályzattal összhangban az üzemeltető szervezeti egység vezetője felelős azért, hogy az IT rendszerek teljes körű belső biztonsági felülvizsgálata dokumentált módon (belső felülvizsgálati jelentés) legalább évente megtörténjen és legalább háromévente sor kerüljön külső, harmadik fél általi felülvizsgálatra a kritikus osztályú rendszerek esetében.

(2) Súlyos SLA sértés esetén a szolgáltatást végző szervezeti egység vezetője külön rendkívüli biztonsági ellenőrzést és felülvizsgálatot rendelhet el.

(3) A felülvizsgálatok eredményei alapján a szervezeti egység vezető rendelhet el javító, helyesbítő és megelőző intézkedéseket, melyeket mindig a soron következő belső vagy külső, harmadik fél általi

felülvizsgálat során kell dokumentált módon visszaellenőrizni. Erről a szolgáltatási területnek megfelelően az EIO, vagy az EISZK vezetőjét írásban tájékoztatni köteles.

X. fejezet

Hatályba léptető és záró rendelkezések

74. § (1) Jelen szabályzat az új eszközök és szolgáltatások esetében az Egyetem Szenátusa által történő elfogadás napján lép hatályba.

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

Pécs, 2008. június 12.

Dr. Gábriel Róbert
rektor

Záradék:

Jelen szabályzatot a Pécsi Tudományegyetem Szenátusa 2008. június 26-ai ülésén 193/2008. (06.26.) számú határozatával elfogadta.

1 sz. melléklet

TITOKTARTÁSI NYILATKOZAT

a Pécsi Tudományegyetemen titoktartási kötelezettséggel járó informatikai rendszert üzemeltető, felhasználó személyek részére

Titoktartásra kötelezett személy neve:

Munkaköre:

Szervezeti egység neve:

Alulírott kijelentem, hogy munkaköröm ellátásával kapcsolatban tudomásomra jutott, az Egyetem gazdasági helyzetéről, az Egyetem szerződéseiről, illetve az Egyetem által foglalkoztatott, vagy az Egyetemmel kapcsolatban álló személyekről szóló információt illetéktelen személyek tudomására nem hozok.

Tudomásul veszem, hogy a fenti információkat csak munkaköröm ellátásához szükséges mértékben használhatom és közölhetem olyan személyekkel, akik az információ megszerzésére való jogosultságukat hitelt érdemlően igazolták.

Tudomásul veszem, hogy a jelen nyilatkozatban foglalt kötelességem megszegése esetén, felelősséggel tartozom, beleértve az anyagi felelősséget is.

Dátum:

---

aláírás

Dolgozó aláírása