A Pécsi Tudományegyetem

Információbiztonsági politikája

Pécs 2009.

1. Dokumentum adatlap

Azonosítás	
Dokumentum címe	Információbiztonsági politika
Állomány neve	Informaciobiztonsagi politika.docx
Dokumentum verzió	1.0
Kiadás időpontja	2009.12.01.
Hatályba lépés időpontja	2010.01.01.
Az Információbiztonsági politika felülvizsgálatának az ideje	2010.12.31.
Készítette	Ripli Péter
Ellenőrizte	Sári Csaba
Jóváhagyta (IIG)	Sári Csaba

2. Tartalomjegyzék

3. Tevékenység

Az eljárás a Pécsi Tudományegyetem (későbbiekben PTE vagy Egyetem) Információbiztonsági Politikájának (IBP) kialakítására, elfogadtatására és ellenőrzésére vonatkozik.

4. Cél

Az információbiztonsági politika célja, hogy a PTE teljes egészére egységes szemlélettel megfogalmazza azt a vezetői szándékot, amely az IT rendszerek által kezelt adatok

- bizalmasságának,
- hitelességének,
- sértetlenségének
- rendelkezésre állásának megőrzésére irányulnak.

Az informatikai-biztonsági helyzet elemzése során a biztonsággal kapcsolatos legjelentősebb hiányosságok az emberi tényezőkre, a szabályzatok és az ellenőrzés hiányára vezethetők vissza.

A központilag kialakított, bevezetett és követett Információbiztonsági Politika (továbbiakban IBP) megfogalmazása elengedhetetlenül szükséges az egységes PTE szintű (Pécsi Tudományegyetem és az egyetemhez tartozó telephelyekre szervezeti egységekre vonatkozó) biztonsági szabályozások kialakításához, és ezáltal az egyenszilárdságú védelem elvének gyakorlati megvalósításához.

Célja továbbá, olyan nem-funkcionális követelmények definiálása, amelyek biztosítják az informatikai stratégiaiában megfogalmazott projektek megvalósítása során – pl. az informatikai infrastruktúra beszerzése vagy az alkalmazások újrafejlesztése – az informatikai biztonsági követelményeknek történő megfelelőséget. Az Információbiztonsági Politikában megfogalmazott irányelvek a PTE minden szintjén érvényesítendő követelményeket határoznak meg.

Az Információbiztonsági Politika előfeltétele a szervezet egységes biztonsági szemléletének kialakítása, és alapját képezi az informatikai biztonsággal kapcsolatos további tevékenységeknek, az információ biztonság területén készülő jövőbeni szabályzatok kidolgozásának.

A biztonsági politikának tartalmaznia kell:

- a PTE vezetőinek elkötelezettségét az informatikai biztonság irányában,
- az informatikai biztonsági és etikai irányelveket,
- az megvalósítandó informatikai biztonsági feladatokat.
- felelősségi és végrehajtói szerepköröket
- időbeliségre vonatkozó becsült vezetői elvárásokat

5. Felelősség

5.1. Elkészítés

Az **információbiztonsági politika meghatározása** az informatikai adatbiztonság felelős feladata.

Dokumentumának összeállítása az informatikai adatbiztonság felelős feladata az informatikai osztályvezetőkből álló munkacsoport segítségével. A dokumentum összeállításához az informatikai szervezet valamennyi felelős munkatársának feladata információt szolgáltatni.

5.2. Jóváhagyás

Az elkészült információbiztonsági politika tervezetet az Informatikai igazgató feladata **ellenőrizni és jóváhagyásra előterjeszteni** a vezetése elé.

A **PTE Gazdasági Főigazgató** értelmezi az információbiztonsági politika tervezetet és elemzi a benne összefoglalt célkitűzések megvalósíthatóságát, realitását.

5.3. Aktualizálás

Amennyiben **pontosítás**ra szorul a tervezet az adatbiztonság felelős feladata azokat végrehajtani.

5.4. Ellenőrzés

Az információbiztonsági politikának megfelelő működést az **informatikai igazgató, az Intézményvezetők és az Adatbiztonság Felelős ellenőrzi, értékeli**, és a szükséges **javító intézkedéseket kezdeményezi**.

Az eljárásban hivatkozott dokumentumok jóváhagyott példányainak az informatikai adatbiztonság felelősnél elérhetőnek kell lenniük.

6. Kontroll pontok

Az információbiztonsági politika **dokumentum**ának **megléte**.
Az információbiztonsági politikában vállalt **felelősség megnyilvánulása**.

Az információbiztonsági politika **felülvizsgálat**a az informatikai adatbiztonság felelős feladata az informatikai biztonság aktuális állapotának tekintetében.

Megfelelés: A felülvizsgálat eredményeként meg kell állapítani mennyire követi az informatikai biztonság működése/működtetése az információbiztonsági politikában megfogalmazott irányelveket. Amennyiben jelentős - indokolatlan - eltérés tapasztalható, ki kell vizsgálni az okát, amely az informatikai adatbiztonság felelős feladata, és intézkedéseket kell megfogalmazni a politikát követő működés érdekében.

Az IBP aktualitásának megtartása érdekében a **dokumentum rendszeres karbantartás**t igényel.
Az IBP felülvizsgálatát, annak belső auditálását követően kell elvégezni, a legutolsó belső audit óta bekövetkezett jogszabályi, funkcionális, biztonsági, technológiai, működési illetve egyéb változások tükrében. Az IBP belső auditálását legalább **évente egyszer** el kell végezni.

A dokumentum **rendkívüli felülvizsgálat**át kell végrehajtani amennyiben:

- a PTE céljai megváltoznak;
- informatikai szolgáltatások jelennek, illetve szűnnek meg;
- új informatikai technológiák kerülnek bevezetése, illetve egyes technológiák alkalmazása szűnik meg;
- a külső és belső körülmények változásával összefüggő kockázatelemzés következtében új, lényeges változtatások válnak szükségszerűvé;
- ha bármilyen más okból az Információbiztonsági Politika nem tölti be elvárt szerepét;
- Egyéb tényezők (pl. jogi környezet változása) ezt szükségessé teszi.

A szükséges módosításokat, kiegészítéseket a megváltozott körülmények, célok felismerésekor, lehetőleg az új tevékenység, technológia, szolgáltatás megkezdése, bevezetése előtt kell kezdeményezni és megvalósítani.

Amennyiben változtatásra szorul a korábbi dokumentum, annak végrehajtása az informatikai adatbiztonság felelős feladata.

A **biztonság tudatos felhasználói magatartás**t, önkontrolok bevezetését erősíteni kell,

-oktatással,

-ösztönzéssel,

-publikálással.

Külső auditot kell elrendelni például szakterületet érintő tanúsítvány megszerzése vagy megtartása esetén.

7. Kapcsolódó jogszabályok

7.1. Jogszabályok

1959. évi IV. törvény: A Polgári Törvénykönyvről,

1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról

2005. évi CXXXIX. törvény a felsőoktatásról

7.2. Szabványok

7.3. Ajánlások, irányelvek

COBIT, ISACA

8. Az Információbiztonsági Politika hatálya

8.1. Szervezeti hatály

Az IBP hatálya kiterjed a PTE minden szervezetei egységére.

8.2. Személyi hatály

Az Információbiztonsági Politika személyi hatálya kötelező érvénnyel kiterjed a PTE minden közalkalmazottjára hallgatójára. Az IBP elveit érvényesíteni kell a PTE-vel szerződéses kapcsolatban álló cégek és személyek körére is (különös tekintettel a szállítókra, tanácsadókra, stb.). Az Információbiztonsági Politika érvényesülését a partner szerződések tartalmának megfelelő kialakításával kell biztosítani.

8.3. Tárgyi hatály

Az IBP tárgyi hatálya kiterjed a PTE által használt valamennyi informatikai rendszerre, amely felhasználja, feldolgozza, tárolja és továbbítja illetve felügyeli, ellenőrzi a PTE-nél keletkező, illetve felhasznált adatokat, információkat.

Az információbiztonsági politika közzététele napján lép érvénybe, és visszavonásáig marad hatályban.

9. Az információbiztonság alapelvei

Az információ hitelességét, bizalmasságát, sértetlenségét és rendelkezésre állását elősegítő megelőző intézkedések a folyamatos üzletmenet biztosításának elengedhetetlen feltételei.

- Hitelesség: az információ megbízhatóságának és a közlő egyértelmű azonosításának biztosítása.
- Bizalmasság: az információ jogosulatlan felhasználóktól való védelme.
- Sértetlenség: az információ pontosságának és teljességének megtartása.
- Rendelkezésre állás: annak biztosítása, hogy az információ hozzáférhető legyen az arra jogosult felhasználók számára, amikor azt igénylik.

10. Az informatikai biztonság irányelvei

A PTE a megelőző (preventív) informatikai biztonsági intézkedéseket helyezi előtérbe, ezért a napi operatív intézkedéseken túl, az alább részletezett irányelveket kívánja érvényesíteni közép- és hosszú távú informatikai biztonsági terveiben.

10.1. A négy szem elv

Az „üzleti kockázatok" figyelembevétele mellett, az adatkezelés folyamatába (adatbevitel, adatmódosítás, adatfeldolgozás, stb.) beillesztett ellenőrzés, felülvizsgálat. Ezen üzletileg kockázatos tevékenységek csak két személy által, egymást ellenőrizve végezhetőek.

10.2. A szükséges és elégséges hozzáférés elve

Tekintettel az Egyetem oktatási, gyógyító, kutató tevékenységére, az adatokhoz való hozzáférési jogosultságokat és jogosultsági szinteket úgy kell meghatározni, hogy a felhasználó számára minden információ elérhető legyen, ami feladatának, munkakörének, ellátásához feltétlenül szükséges, fontos, hogy minden esetben csak a szükséges jogosultságokkal rendelkezzen egy felhasználó.

10.3. Kockázatarányos védelem elve

Az elektronikusan tárolt információ és az informatikai infrastruktúra, jelentős szerepet játszik az „üzleti folyamatok" támogatásában. Ezzel összefüggésben a szabályozási környezet egyre szigorúbb előírásokat fogalmaz meg az információk kezelésére, védelmére vonatkozóan. Az informatikai biztonságot érintő mindennapi kihívások szükségessé teszik, hogy az informatikához kapcsolódó kockázatok kezelése kulcsfontosságú részévé váljon az irányítási és ellenőrzési folyamatoknak. Ezért a PTE az informatikai biztonsági rendszerét

- az Európai Unio és a Magyar Köztársaság hatályos jogszabályaival
- a PTE belső rendelkezéseivel
- a felügyeleti szervek elvárásaival
- szerződéses kötelezettségeivel
- az Egyetem „üzleti" igényeivel
- a biztonsági kockázatokkal

összhangban alakítja ki.

A fenyegetettség elemzés során az informatikai rendszer minden elemcsoportjára (tárgyi, logikai, szabályozási és humán) kiterjedő felmérést kell végezni. Meg kell határozni a fenyegetettségek teljes körét, valamint a kockázatok mértékét a biztonsági esemény valószínűségének és következményének függvényében.

A fenyegetettség elemzés végrehajtása után - a feltárt kockázat mérséklése érdekében - elemcsoportonként meg kell tervezni a reális és kockázatarányos biztonsági intézkedéseket, a szükséges fejlesztéseket, valamint dokumentálni kell a megmaradó kockázatokat.

Az PTE tudatosan, a szervezet minden szintjén elemezze és kezelje az informatikai kockázatokat, veszélyforrásokat. Amennyiben a kockázatelemzés során feltárt veszélyforrások között vannak olyanok, amelyek kezelése nem történik meg (nem célszerű, nem gazdaságos, stb.) az ily módon létrejövő maradványkockázatok felvállalását dokumentálni kell.

Az informatikai biztonság a kockázatkezelés által épül be minden, informatikai eszközzel támogatott „üzleti folyamatba".

10.3.1. **Automatizmusok beépítése a működésbe és kontrollfolyamatokba**

Az informatikai folyamatok végrehajtását lehetőség szerint az emberi erőforrás kizárásával, ezáltal a hiba lehetőség csökkentésével célszerű megvalósítani, amelyben automatizmusokat célszerű beépíteni kontrol céllal.

10.4. Biztonsági szintek

Az informatikai erőforrásokat és adatokat fenyegető kockázatokkal arányos védelem megvalósításához meg kell határozni az informatikai rendszerekre, az adatokra és információkra vonatkozó biztonsági szinteket (osztályokat), és biztosítani kell a biztonsági szintek által meghatározott követelmények teljesülését.

10.5. Biztonságot érintő események és védelmi intézkedések

Biztosítani kell a PTE informatikai rendszereivel kapcsolatos biztonságot érintő események feltárását, jelentését, kezelését, értékelését és naplózását. Intézkedéseket kell kidolgozni a normálistól eltérő informatikai működés esetére a PTE minden szintjén.

10.6. Az informatikai biztonsággal kapcsolatos szabályzatok

Az Információbiztonsági Politikával összhangban ki kell dolgozni a PTE informatikai biztonsággal kapcsolatos szabályzatait, biztosítani kell ezek bevezetését, felülvizsgálatát és karbantartását, valamint betartásuk ellenőrizhetőségét.

10.7. A teljes körű védelem elve

Az Egyetem az információt és az informatikai rendszereket veszélyeztető minden kockázati tényezőre megfelelő választ és kezelést biztosít, valamint az informatikai biztonságot az informatikai életciklus (fejlesztés, bevezetés, üzemeltetés, kivezetés) minden pontján érvényre juttatja.

10.8. A biztonsági követelmények teljesülése

A biztonsági környezetnek (a biztonságot meghatározó technikai eszközök és eljárások) az informatikai rendszer életciklusának minden fázisában, a rendszer minden pontján biztosítania kell, hogy a védelmi intézkedések kikényszerítsék a biztonsági követelmények teljesítését.

10.9. Biztonsági ellenőrzés

Az informatikai biztonság állapotát az Egyetemen rendszeres átvilágítással és folyamatos megfigyeléssel (monitoringgal) kell ellenőrizni.

Az ellenőrzés az informatikai biztonságot szabályozás, eszköz, eljárás és humán erőforrás oldalról egyaránt kezeli.

Konkrét esetekben, ha azt a helyzet kezelése megkívánja:

- Kötelező szabadságot kell biztosítani a dolgozók részére, amely ideje alatt az esetleges rendellenességek vizsgálatra kerülhetnek, illetve önmaguktól felszínre jutnak.
- Ajánlott a munkatársak rotációja a hasonló munkakörökben a beépült hibás gyakorlat, illetve viszonyrendszer frissítése céljából.

A tevékenységek dokumentálása legyen feladat, ahol az ésszerűen alkalmazható.

Az ellenőrzésnek lehetőség szerint preventív, detektív és korrektív minőségben is meg kell jelenni az informatikai tevékenységben.

11. A védendő erőforrások kezelésével kapcsolatos elvek

11.1. Dokumentumok adattárak kezelése

Az Egyetem belső működésével és szolgáltatásaival kapcsolatos dokumentumokat, adattárakat minősíteni kell tartalmuk, azaz a tárolt és kezelt információk bizalmassága alapján. Biztosítani kell továbbá a dokumentumok, adattárak minősítésüknek megfelelő használatát, védelmét. Rendelkezni kell a dokumentumok, adattárak megfelelő tárolásáról, felhasználásáról, továbbításáról illetve megsemmisítéséről.

A munkahelyi vezető felelős a feladat ellátásához szükséges munkavállalói kompetencia meglétéért.

11.2. Nyilvános szolgáltatások

Biztosítani kell, hogy a nyilvános szolgáltatásokon keresztül csak olyan adatok legyenek hozzáférhetők, amelyek nyilvánosságához a munkaadók és munkavállalók hozzájárulásukat adták vagy amelyek nyilvánosságát jogszabály elő írja. (1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról).

11.3. Kommunikált adatok, információk védelme

A PTE ügyfelekkel, társszervezetekkel és egyéb külső szereplőkkel folytatott, illetve belső kommunikációjában megjelenő adatait, információit azok biztonsági minősítésének megfelelően védeni kell a jogosulatlan hozzáférésektől.

11.4. Adathozzáférés

Az Egyetemen működő rendszerekben tárolt adatok elérhetőségéért a PTE felel, így a rendszereknek biztosítania kell, hogy – a jogosultság függvényében - minden adat lekérdezhető legyen (képernyőre, listába) a felhasználói felületről a lekérdezések naplózása mellett.

A hozzáféréshez kapcsolódó felelősségeket minden esetben egyértelművé kell tenni és alkalmazni.

11.5. Adatkonzisztencia

Az alkalmazói rendszereknek a bevitt vagy számított adatok konzisztenciáját bevitelkor, valamint később rendszeres, vagy ad-hoc ellenőrzésekkel kell biztosítania. Biztosítani kell továbbá az adatok formai és tartalmi sérthetetlenségét.

Az adatok konzisztenciájának vizsgálatát a rendszerek közötti kommunikációban is célszerű automatizmusokkal támogatni.

11.6. Azonosítás és hitelesítés

Az azonosítás és hitelesítés minden felhasználóra egyenként, differenciáltan terjedjen ki.

A PTE szintjén ki kell alakítani a jelszópolitikát, amely kötelezővé teszi a jelszavak használatát és definiálja a jelszavak kialakításánál és használatánál kötelezően figyelembe veendő szempontokat. A jelszavakon alapuló azonosítási rendszer mellett más hozzáférés szabályozási módszer is megengedett, ennek biztonsági kockázata összhangban van a védendő adatok elvárt biztonsági szintjével.

Az azonosítás és hitelesítés kötelező a szervezeten belüli rendszerkapcsolatok (interfészek) esetén, az egyes rendszerek több telephelyen telepített rendszerelemei között, valamint azokban az esetekben, amikor a PTE bármely rendszere adatszolgáltatást végez olyan rendszer felé, mely nem a PTE-n üzemel vagy melyet nem a PTE üzemeltet.

11.7. Titkosítás

Kriptográfiai rendszereket és technikákat kell használni az információk védelmére azokban az esetekben, amikor kiemelkedően nagy a kockázat, vagy a hagyományos védelmi eljárások nem biztosítják megfelelően az adatok, információk védelmét.

11.8. Jogosultságok szabályozása

A felhasználók informatikai erőforrásokhoz való hozzáférési jogosultságait úgy kell meghatározni, hogy mindenki csak a munkaköre ellátásához feltétlenül szükséges adatokhoz férhessen hozzá. Továbbá biztosítani kell a jogosultsági rendszer megkerülhetetlenségét. A PTE informatikai rendszerét oly módon kell kialakítani, hogy abban a hozzáférési jogosultságok kiosztása ne egyetlen személytől függjön.

Minden esetben nevesíteni kell a jogosultságot kiosztó illetve visszavonó személyeket.

11.9. Nyomonkövethetőség

A PTE informatikai rendszere biztosítsa a felhasználók belépés előtti azonosítását a jogosulatlan hozzáférések kizárása, a jogosult hozzáférések, illetve hozzáférési próbálkozások nyomon követhetősége és visszakövethetősége érdekében. A nyomonkövetéshez a belépéseket naplózni szükséges. A megbízható működéssel kapcsolatos eseményekről (rendszer indítás/leállás, nagyobb üzemzavarok, alap- és felhasználói szoftverekkel kapcsolatos, a megbízható működést érintő események) gépi, illetve manuális biztonsági naplózásokat kell végezni. Meghatározandók azok tartalmi követelményei, a naplók kezelési, értékelési és tárolási módja.

A védelemi módszerekhez sorolható naplózás (audit) ugyan közvetlenül nem alkalmas a hozzáférés megakadályozására, de az utólagos ellenőrzések miatt elrettentő, s később bizonyító hatása van.

11.10. Fizikai és logikai rendelkezésre állás

Az informatikai erőforrások működőképességét, megfelelő helyen és időben történő elérhetőségét és a működéshez szükséges kapacitását biztosítani kell mind részleges, mind átfogó sérülések esetére, az erőforrás biztonsági minősítésével összhangban.

Minden kritikus alkalmazói rendszerrel kapcsolatban meg kell határozni annak az elvárt rendelkezésre állását (ami rendszerenként különböző mértékű lehet), sebezhetőségi ablakát, azaz azt az időtartamot, amíg az adott rendszer kiesése a szervezet számára még elviselhető a működés fenntarthatósága szempontjából. Ehhez szükséges biztosítani a technikai feltételeket. Az elvárt vagy elvárható rendelkezésre állások mértékét rendszerenként elkészített Szolgáltatási Szint Megállapodásokban (SLA) kell rögzíteni.

Meg kell határozni a rendszer helyreállításának szintjeit és kapcsolódó időtartamát, valamint az elviselhető adatvesztés mértékét-időtartamát.

11.11. Tartalék eszközök

A PTE létfontosságú szolgáltatásainak biztosításához rendelkezésre kell, hogy álljanak azok az alapvető tartalék technikai eszközök, amelyek a szervezet biztonságos és zavartalan működését lehetővé teszik üzemzavar esetén. A tartalékokat a velük való hatékony gazdálkodás érdekében a rendelkezésre állási elvárásoknak megfelelően allokálni kell és csoportokba kell sorolni (azonnal, egy órán belül, stb. üzembe állítható). Törekedni kell arra, hogy az átállások a lehetőségekhez mérten automatizáltan hajtódjanak végre.

11.12. Informatikai rendszerkörnyezet

Az informatikai rendszerek környezetének kialakításakor az adott rendszer, illetve az azon tárolt vagy közvetített adatok biztonsági osztályba történt sorolásával összhangban szükséges biztosítani az informatikai rendszerkörnyezet fizikai védelmét (elhelyezés, belépés, stb.).

11.13. Mobil eszközök

A mobil eszközökön telepített rendszerek, illetve ezeken az eszközön tárolt adatok számára fokozott védelmet kell biztosítani.

Lehetőség szerint korlátozni kell a nem PTE tulajdonú, adattárolásra alkalmas eszközök alkalmazását,

A nagy értékű/adatértékű mobil eszközök védelmét ajánlott fizikai megoldással (keylock) támogatni.

12. Rendszerfejlesztéssel és üzemeltetéssel kapcsolatos elvek

12.1. Üzemeltetés szabályozása

A PTE-nek rendelkeznie kell az üzemeltetés minden tevékenységét, körülményét szabályozó üzemeltetési szabályzatokkal.

Biztosítani kell a PTE informatikájától elvárt szolgáltatási szint folyamatos monitorozását, valamint az esetleges hibák, rendellenességek észlelését, kezelését.

12.2. Üzembiztonság

Egy adott feladat ellátására beszerzett informatikai erőforrások kiválasztásánál alapvető döntési szempont a támogatandó feladat, folyamat fontossága, kritikussága – a kiválasztott eszközöknek arányosan meg kell felelniük a támogatandó folyamat üzembiztonsági követelményeinek.

12.3. Tűzfalas védelem

A tűzfalnak el kell rejtenie a külső szemlélő elől a belső hálózat struktúráját, valamint megfelelő ellenőrzési és behatolás detektáló, nyomkövetési, naplózási szolgáltatásokat kell biztosítania. Minden alkalmazással, illetve infrastruktúrával kapcsolatos tevékenységhez kötődő információáramlást minden irányban ellenőrizni kell. Minden bentről kifelé és kintről befelé haladó információnak át kell haladnia a tűzfalon. A PTE kiszolgáló gépeit (szervereit), amelyek a nyilvános hálózatból érkező szolgáltatási kérelmeket kezelik, ún. demilitarizált zónában (DMZ) kell elhelyezni.

12.4. Internet és elektronikus levelezés

Az Pécsi Tudományegyetemmel bármilyen jogviszonyban álló felhasználók az elektronikus levelezési és a levelezéshez kapcsolódó feladataikat, tevékenységeiket a „Az informatikai és hírközlési miniszter 20/2004. (VI.21.) IHM rendelete a Nemzeti Információs Infrastruktúra Fejlesztési Program Felhasználói Szabályzatának közzétételéről” alapján végezhetik.

6.§ „A NIIF hálózat a 4. és 5. §-ban meghatározott kereteken belül minden tevékenységre használható, amely nem ütközik a 7. §-ban foglalt rendelkezésekbe.”

7.§ „A NIIF hálózat nem használható az alábbi tevékenységekre, illetve ilyen tevékenységekre irányuló próbálkozásokra, kísérletekre:

a) a mindenkor hatályos magyar jogszabályokba ütköző cselekmények előkészítése vagy végrehajtása, így különösen mások személyiségi jogainak megsértése (pl. rágalmazás), tiltott haszonszerzésre irányuló tevékenység (pl. piramisjáték), szerzői jogok megsértése (pl. szoftver nem jogszerű terjesztése);
b) nem NIIF tagintézmények egymás közötti forgalmának bonyolítása, kivéve, ha azt az 5.§-ban meghatározott szerződéses munkakapcsolat indokolja;

c)…
.
.
.
m)”

Az Internet használat és levelezés létesítése és üzemeltetése vonatkozásában megfelelő tűzfalas védelmet kell kialakítani a külső támadások, illetve a belső erőforrásokhoz történő jogtalan hozzáférések megakadályozása érdekében.

Az Egyetem Informatikai Igazgatóságának betekintési, ellenőrzési joga lehet a PTE erőforrásain történő minden adatforgalomba a személyiségi jogok tiszteletben tartásával.

12.5. Rosszindulatú szoftverek elleni védekezés

Az alkalmazások és informatikai rendszerek sebezhetőek a rendszerbe bejutó rosszindulatú szoftverek (vírusok, „trójai falovak" stb.) által. A rosszindulatú szoftverek kártételeinek megelőzésére megfelelő megelőző, észlelési és korrekciós mechanizmusokat kell alkalmazni, ki kell dolgozni a válaszlépéseket és jelentési eljárásokat.

12.6. Költséghatékony, alacsony kockázatú rendszerek kialakítása

A PTE rendszereinek kialakításakor a célszerűségen túl elsődleges szempontként a költséghatékonyságot és a kockázatok minimalizálását kell szem előtt tartani.

12.7. A biztonság védelme külső kapcsolatokban

Külső féllel fenntartott, vagy létesítendő – szerződéses – kapcsolatokban biztosítani kell a biztonsági követelmények érvényesülését.

12.8. Hardverkarbantartás

A PTE hardvereszközeinek (szerverek, munkaállomások, hálózat) és a működést elősegítő kiszolgáló eszközöknek (szünetmentes táp, generátor, klíma, beléptető rendszer) zökkenőmentes és üzemszerű működéséhez biztosítani kell azok rendszeres megelőző karbantartását.

12.9. Hálózati és rendszerszoftverek

Biztosítani kell a hálózati és rendszerszoftverek telepítésének, használatba vételének, követésének, és egységes beállításának központi koordinációját és dokumentálását.

Priorizáltan kell kezelni a költséghatékony licence-gazdálkodást.

12.10. Biztonsági menések

A PTE adatbázisairól rendszeres biztonsági mentéseket kell készíteni. A mentéseket a kialakított infrastruktúrának megfelelően kell végrehajtani. Biztosítani kell a mentések megfelelően biztonságos tárolását, és időszakonként ellenőrizni kell, hogy a mentésekből a definiált mentés-visszaállítási folyamattal sikeresen visszaállítható-e a rendszer egy korábbi, konzisztens állapota.

12.11. Archiválás

A PTE informatikai rendszereinek támogatnia kell az adatok logikai állapota szerinti archiválást, valamint az archív adatokhoz való hozzáférést (archív rendszerrel, vagy a rendszerbe való visszatöltéssel).

Az archiválási rend kialakításánál különös tekintettel meg kell felelni mind a pénzügyi és egészségügyi jogi ellenőrzési elvárásoknak, előírásoknak.

12.12. Szoftverfejlesztés

Éles egyetemi felhasználásra készülő „ügyviteli”, egészségügyi, oktatási, stb. külső és belső fejlesztéseket egyaránt, az Informatikai Biztonsági Szabályzatban meghatározott műszaki, biztonsági elvárások betartásával szabad végezni. A rendszertervben szerepeltetni kell a jogszabályoknak és a biztonsági előírásoknak megfelelően a rendszerre vonatkozó biztonsági követelményeket és intézkedéseket. Minden külső fejlesztés esetén, a forráskód ellenőrzésével (vagy megfelelő alapossággal lefolytatott teszteléssel) kell az informatikai biztonság konzisztenciáját megőrizni. A fejlesztett rendszerelemeket bevezetésük előtt biztonsági tesztelésnek is alá kell vetni, amelynek eredményét dokumentálni kell.

A Egyetem és a szoftverfejlesztő közötti szerződésben rendelkezni kell az adatvédelmi, adatbiztonsági kérdésekről.

Fent leírtak nem vonatkoznak a kísérleti, kutatási, tesztelési céllal nem éles egyetemi üzemeltetésre szánt fejlesztésekre.

12.13. Tesztelés és fejlesztés támogatása

Csak megfelelően tesztelt rendszer telepíthető az éles környezetbe. Az alkalmazási rendszerek fejlesztésének és megfelelő tesztelésének biztosításához rendelkezésre kell állnia megfelelő, az éles rendszerhez paramétereiben és felépítésében hasonló, az éles rendszertől elkülönített tesztkörnyezeteknek.

12.14. Konfigurációkezelés

A rendszerek konfigurációkezelésének biztosítania kell, hogy adott rendszer aktuális állapota mindig ismert, és a rendszer bármikor reprodukálható legyen. A rendszer konfigurációja alatt az informatikai infrastruktúra egyes komponenseit értjük (hardver, szoftver, adatok, szolgáltatások, kapcsolódó dokumentáció), a konfigurációkezelés alatt pedig az egyes komponensek dokumentált beazonosítását és változásainak figyelemmel követését.

12.15. Dokumentációk rendelkezésre állása

Biztosítani kell az üzemeltetéshez, fejlesztéshez és az alapvető szervezeti folyamatokhoz kapcsolódó dokumentumok rendelkezésre állását, karbantartását és biztonságos tárolását.

A dokumentumok, kulcsfontosságú eszközök sürgős esetben szükséges pótlását kereszt-szerződésekkel, biztosítási megállapodásokkal kell támogatni.

13. A szervezettel és személyekkel kapcsolatos elvek

13.1. Felelősségi és hatáskörök

A szervezetben pontosan definiálni kell az informatikához tartozó munka- és felelősségi köröket, valamint folyamatosan biztosítani kell az ezek ellátásához szükséges hatásköröket. Az informatikai munkaköröket úgy kell kialakítani, hogy azok ne tartalmazzanak biztonsági szempontból egymást kizáró feladatokat (pl.: végrehajtási és ellenőrzési, illetve a fejlesztői és üzemeltetői felelősségek szétválasztása). A PTE-n érvényesülnie kell a hatáskör-szétválasztás általános biztonsági alapelvének. Ennek megfelelően a szervezetben egyértelműen különüljenek el a jóváhagyó, végrehajtó és ellenőrző funkciók valamint egy kézbe ne összpontosuljon túlzottan magas rendelkezési jog.

13.2. Biztonsági szervezet

Biztosítani kell a PTE informatikai biztonsági tevékenységeinek, az IT biztonság szabályozásának és ellenőrzésének központi koordinációját. Ki kell jelölni az informatikai biztonságért felelős vezetőt, valamint az egyes szervezeti egységeknél adatbiztonsági - adatvédelmi felelősöket. Meg kell határozni az informatikai biztonságért felelős személyek IT biztonsági feladatait és ellenőrzésük rendjét.

13.3. Munkatársi megbízhatóság

A munkatársak munkaviszonyának létesítésénél ellenőrizni kell a szóban forgó személy megbízhatóságát.
A munkaviszony alatt rendszeres időközönként ellenőrizni kell a személy megbízhatóságát.
A munkaviszony megszüntetésekor pedig védeni kell a bizalmasságot.

13.4. Tudatosság

A PTE minden közalkalmazottjában oktatás, tájékoztatás keretében tudatosítani kell az Információbiztonsági Politikában foglalt általános informatikai biztonsági irányelveket, valamint az informatikai biztonsághoz kapcsolódó szabályozások vonatkozó részeit.

13.5. Biztonsági események és incidensek kezelése

Biztonsági eseménynek nevezzük a PTE rendszereinek biztonsága szempontjából lényeges esetet. Ilyen lehet az az esemény vagy tett, amely megszegi vagy egyéb módon áthágja a biztonsági szabályzatot, vagy megsérti a biztonsági előírásokat. Biztonsági incidensnek nevezzük az informatikai rendszer biztonságát valamilyen szempontból fenyegető ártalmas eseményt, pl. az adatok titkosságának elvesztését, az adatok vagy a rendszer sértetlenségének megszűnését, vagy a rendelkezésre állás megtagadását, illetve megbomlását.

A PTE érdeke, hogy az egyetem informatikai biztonságáért felelős vezető(i) mielőbb értesüljenek a bekövetkezett biztonsági eseményekről és incidensekről. Minden alkalmazottnak, illetve az egyetemmel szerződéses viszonyban álló munkatársnak ismernie kell azt az eljárást, amelyben jelenthetik az általuk felismert biztonsági eseményeket és incidenseket.

Az eseményeket, incidenseket vagy felmerülésük megnövekedett kockázatát minden alkalmazott és hallgató köteles jelenteni.

13.6. Szankciók

A biztonsági előírások be nem tartásának eredményeként bekövetkező információs és vagyoni kárnak előre definiált – a Közalkalmazottak jogállásáról szóló 1992. évi XXXIII. Törvénynek megfelelő – szankciókat kell

maga után vonnia. Ezeknek a szankcióknak olyanoknak kell lenniük, hogy fenyegetésük visszatartó erejű legyen.

14. Az informatikai biztonság megvalósítása

A PTE az informatikai biztonsági céljainak megvalósítása során a BS 7799, ITIL-V3 és CobiT szabványok ajánlásait veszi alapul.

Az informatikai biztonság a folyamatosan növekvő fenyegetettségek mellett csak folyamatos fejlesztéssel érheti el célját. Ebből fakadóan az informatikai biztonsági rendszer auditálható, objektív mérések alapján folyamatosan fejlesztett folyamat, mely biztosítja a teljes körű és kockázatarányos védelmet, a naprakészséget és a környezet változásaira történő érzékeny reagálást.

14.1. Az informatikai biztonsági rendszer felépítése

- Információbiztonsági politika
- Informatikai biztonsági stratégia
- Gazdasági Főigazgatói utasítások
- Informatikai biztonsági és működési szabályzatok, munkautasítások

15. Az informatikai biztonság oktatása és képzése

15.1. Cél

Gondoskodni arról, hogy a **felhasználók tudatában legyenek** az informatikai biztonság fenyegetettségével és el legyenek látva minden olyan feltétellel, hogy a PTE Információbiztonsági politikában előírtakat, a szokásos napi munkájuk során betarthassák. A felhasználók legyenek oktatva a biztonsági eljárások és az informatikai eszközök helyes használatáról a lehetséges biztonsági kockázat minimalizálása érdekében.

15.2. Célcsoport

Az Információbiztonsági politika személyi hatályába tartozó személyek. Az oktatás belső tájékoztatást és belső, vagy külső képzést, illetve továbbképzést jelent.

16. Vezetői elkötelezettség

A Pécsi Tudományegyetem vezetősége az informatikai biztonságot alapvető, az „üzleti érdekek” megvalósítását támogató tényezőnek tekinti, amely elengedhetetlen a partnerek bizalmának elnyeréséhez és az eredményes működéshez.

Ezért a Pécsi Tudományegyetem vezetése – az adatok kezelésének jogszerűségén túl – elkötelezi magát a jelen dokumentumban megfogalmazott informatikai biztonsági alapelvek és koncepció alkalmazása mellett, támogatja az informatikai biztonság minél magasabb szintű megvalósítását.

17. Az Információbiztonsági Politika hatálya

Az Információbiztonsági Politika 2010. január 1. napján lép hatályba.