A Pécsi Tudományegyetem
Informatikai Biztonsági Szabályzata

Pécs
Hatályos: 2022. július 1. napjától

Tartalom

Preambulum

A Pécsi Tudományegyetem (továbbiakban: Egyetem) Szenátusa az Egyetem oktatási, egészségügyi, kutatási, fejlesztési, adminisztratív feladatainak támogatása, valamint az információ szabad áramlásának, az adatok, az információk és a tudás megragadásának és hasznosításának informatikai eszközökkel történő védelmének biztosítása érdekében, a nemzeti felsőoktatásról szóló 2011. évi CCIV. (továbbiakban: Nftv.) törvényben foglaltakat figyelembe véve; továbbá az Egyetem létfontosságú rendszerelem üzemeltetőként az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben (továbbiakban Ibtv.) előírtak megvalósítása és a az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendelet szerint a kijelölt rendszerelemek biztonsági osztályba, és az Egyetem, valamint egyes szervezeti egységek biztonsági szintbe sorolása érdekében az Egyetem Informatikai Biztonsági Szabályzatát (továbbiakban: Szabályzat) az alábbiak szerint határozza meg:

1. fejezet Általános rész

A szabályzat célja

1.§ (1) A Szabályzat alapvető célja, hogy az Egyetem működése során

a) biztosítsa az Egyetem által kezelt, feldolgozott, továbbított, valamint tárolt adatok és információk kockázattal arányos védelmét (bizalmasság, sértetlenség és rendelkezésre állás) a felmerülő veszélyforrások ellen az 2013. évi L. törvény szerint;
b) azonosítsa és meghatározza az információbiztonság szereplőit és feladataikat;
c) előírja az Egyetemhez kapcsolódó bármely tevékenységek során betartandó információbiztonsági szabályokat, irányelveket és felelősségi köröket.

(2) A Szabályzat célja előmozdítani az informatikai és kommunikációs eszközök előírásoknak megfelelő és biztonságos használatát, továbbá az Egyetem egyes szervezeti egységei, illetve a felhasználók között az információáramlás biztosítása, valamint egyéb informatikai és kommunikációs szolgáltatások nyújtása a felhasználók számára.

(3) A Szabályzat a fentiek megvalósítása érdekében keretjelleggel – a hatályos jogszabályokkal és az Egyetem belső szabályzataival, így különösen a Pécsi Tudományegyetem Informatikai Szabályzatával összhangban – meghatározza a rendszerekre és a rendszerekkel kapcsolatos tevékenységekre vonatkozó adminisztratív, fizikai és logikai követelmények elérésével és fenntartásával összefüggő garanciális folyamatokat, feladatokat és felelősségeket. A vonatkozó részletszabályokat jelen Szabályzat felhatalmazása alapján kancellári utasításban szükséges meghatározni.

(4) A Szabályzat aktualizálása az informatikai és innovációs igazgató (továbbiakban: i3 igazgató) felelőssége.

A szabályzat hatálya

2.§ (1)A Szabályzat személyi hatálya kiterjed:

a) PTE SZMSZ 77-78. §-okban meghatározott karokra, önálló szervezetekre, valamint az Egyetem által fenntartott köznevelési és szakképző intézményekre,
b) az Egyetemmel bármilyen, munkavégzésre irányuló jogviszonyban álló személyekre (továbbiakban: foglalkoztatott),
c) az Egyetemmel hallgatói, vagy egyéb képzési jogviszonyban álló személyekre (továbbiakban: hallgató),
d) az Egyetemmel szerződéses vagy egyéb jogviszonyban álló természetes és jogi személyekre, amennyiben azok hozzáférést kapnak az Egyetem informatikai erőforrásaihoz, rendszereihez,
e) az Egyetemmel szerződéses jogviszonyban nem álló bármely természetes és jogi személyre, amennyiben az Egyetem által nyújtott informatikai szolgáltatásokat igénybe veszik

(továbbiakban együttesen: felhasználókra).

(2) A szabályzat területi hatálya kiterjed:
a) az Egyetem teljes területére,
b) az Egyetem tulajdonában vagy használatában lévő informatikai eszközöknek az Egyetem területén kívül történő igénybevétele esetén az igénybevétel helyére (pl. hordozható eszköz otthoni munkavégzéshez),
c) az Egyetem területén kívül, idegen eszközön történő igénybevétel esetén az igénybevétel helyére (pl. saját tulajdonú eszközről távoli eléréssel).

(3) A Szabályzat tárgyi hatálya kiterjed
a) az Egyetem teljes hálózati infrastruktúrájára,
b) Egyetem minden információkezeléssel és feldolgozással kapcsolatos folyamatában résztvevő informatikai eszközre, nyilvántartást strukturáltan megvalósító rendszerre, mely az Egyetem területén található, illetve ezen eszközök elhelyezésére szolgáló létesítményekre,
c) az Egyetem tulajdonában vagy használatában lévő informatikai eszközökre és az informatikai eszközök által kezelt, tárolt, továbbított adatokra, információkra, a szoftverek teljes körére,
d) az Egyetem informatikai hálózatára csatlakozó, de nem az Egyetem tulajdonában lévő eszközökre, függetlenül azok földrajzi elhelyezkedésére.

(4) A Szabályzat felülvizsgálatát el kell végezni az alábbi esetekben:
a) két éves rendszerességgel, valamint;
b) szervezeti, infrastrukturális, informatikai erőforrásokban bekövetkező változások, tevékenységi körben, folyamatokban történő jelentős változások, jelentős személyi változások, magasabb szintű belső szabályzatokban történt módosítások, jogszabályi változások esetén eseti jelleggel, valamint;
c) amennyiben egy súlyos incidenst követően az Informatikai Bizottság erre javaslatot tesz;
d) bármikor, a Kancellár vagy az Információbiztonsági Felelős vagy az i3 igazgató kezdeményezésére.

3. § (1)A Szabályzatban alkalmazott meghatározásokat az 1. számú melléklet (Fogalomtár) tartalmazza.

(2) A vonatkozó jogszabályok, további belső szabályzatok a 2. számú mellékletben (Kapcsolódó jogszabályok, szabályozások listája) találhatóak.

2. fejezet Az információbiztonsági rendszer

Alapelvek

4. § (1) Az Ibtv. 5. §-a alapján az elektronikus információs rendszerek teljes életciklusában meg kell valósítani és biztosítani kell
a) az elektronikus információs rendszerben kezelt adatok és információk bizalmasságát, sértetlenségét és rendelkezésre állását, valamint
b) az elektronikus információs rendszer és elemeinek sértetlensége és rendelkezésre állása zárt, teljes körű, folytonos és kockázatokkal arányos védelmét.

(2) Kockázatarányos, differenciált, többszintű informatikai védelmi rendszert kell kialakítani és működtetni az Egyetemen.

Vezetői elkötelezettség

5.§ (1) Minden szervezeti egység vezetője közreműködik az információbiztonság kultúrájának kialakításában és fenntartásában.

(2) A vezetők elkötelezettségüket személyes példamutatással, személyes felelősségvállalással, a szabályok teljeskörű betartásával és betartatásával demonstrálják.

(3) Az információbiztonsági intézkedések megvalósításához szükséges erőforrások biztosítása az Egyetem vezetőinek a felelőssége a Pécsi Tudományegyetem Szervezeti és Működési Szabályzatában (továbbiakban: SZMSZ) meghatározottak szerint.

(4) A vezetők megkövetelik és elősegítik az információbiztonsági követelmények megismertetését és betartatását a szervezeti egységükhöz tartozó munkavállalókkal.

Az információbiztonsági rendszer kialakítása és működtetése

6.§ (1) A jelen Szabályzat egységes rendszerbe foglalja az Egyetem információbiztonsági feladatait, így felkészítve az Egyetemet az információbiztonságot fenyegető veszélyekkel szemben történő szervezett védekezésre.

(2) Az Egyetem szervezeti egységei által használt informatikai infrastruktúra védelmét az adatgazdáknak úgy kell megvalósítaniuk, hogy az informatikai szolgáltatásoknak és környezetüknek védelme teljes körű, zárt, kockázatokkal arányos és folytonos legyen, valamint, hogy megvalósuljon a zárt szabályozási ciklus az alábbiak szerint.

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

a) az összes információbiztonsági rendszerelem csoportra,
b) az informatikai szolgáltatás 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) az egyetemi polgárokra és a külső partnerekre,
i) a nemzetközi és magyar szabványban meghatározott nyílt rendszerek architektúrájának minden rétegére, azaz mind a számítástechnikai infrastruktúra, mind az informatikai alkalmazások szintjén.

(4) A szabályzatokat közzététel útján megismerhetővé kell tenni, az új belépőket oktatásban kell részesíteni, szükség esetén további képzéseket kell szervezni.

Az információbiztonsági szabályozás rendszere

7.§ (1) Az informatikai biztonsági rendszer kiépítése során az Egyetem elkötelezi magát a folyamatszemléletű működés mellett. Az informatikai rendszer kialakítása és működtetése a PDCA (Plan-Do-Check-Act) modellnek megfelelően valósul meg. Ezt támogatja és erősíti a kockázatalapú gondolkodásmód, mely elősegíti a követelményeknek való megfelelés mellett az átgondolt folyamatok kialakítását, nyomon követését és szükség szerinti korrigálását is.

(2) Jelen Szabályzat az informatikai biztonság alapdokumentuma, mely magas szinten, keretjelleggel szabályozza az információbiztonsági szempontból releváns területeket a 2. számú mellékletben felsorolt jogszabályi előírásoknak megfelelően.

(3) A folyamatleírásokat, a dokumentációs mintákat, valamint a dokumentációkkal szemben támasztott informatikai szakmai követelményeket, elvárásokat az Informatikai és Innovációs Igazgatóság (a továbbiakban: i3) a saját elektronikus felületén, továbbá amennyiben az adattartalom felhasználói jogosultsághoz kötött, nem nyilvános dokumentumtárában tárolja és teszi elérhetővé az i3 munkatársai és az érintettek adatgazdák számára.

(4) Az egyes elektronikus információs rendszerekre vonatkozó különleges szabályozásokat a rendszerspecifikus előírások és dokumentációk tartalmazzák a jelen Szabályzat által definiált alapelvek figyelembevétele mellett.

(5) A rendszerspecifikus előírások és dokumentációk kiadása és módosítása előtt az i3 igazgatója, mint elektronikus információs rendszerért felelős szervezet vezetője köteles az Információbiztonsági Felelősnek, személyes adatok érintettsége esetén az adatvédelmi tisztviselőnek, valamint egészségügyi adatok érintettsége esetén az egészségügyi adatvédelmi tisztviselőnek a véleményét kikérni.

Információbiztonsági Politika

8. § (1) Az Egyetem az Információbiztonsági Politikában határozta meg az információbiztonsági működés kereteit, alapvető működésének elvét. Az Információbiztonsági Politika jelen Szabályzat 3. számú mellékletét képezi.

(2) Az Egyetem szervezeti egységei által kezelt informatikai infrastruktúra védelmét az adatgazdáknak úgy kell megvalósítaniuk, hogy az informatikai szolgáltatásoknak és környezetüknek védelme teljes körű, zárt, kockázatokkal arányos és folytonos legyen, valamint, hogy megvalósuljon a zárt szabályozási ciklus az Információbiztonsági Politikában leírtaknak, valamint a jelen Szabályzatban foglaltaknak megfelelően.

Információbiztonsági kockázatmenedzsment

9. § (1) A kockázatelemzés végrehajtásához az Egyetem Belső Kontroll Kézikönyvében meghatározottak alapján szükséges eljárni.

(2) Az információbiztonsági kockázatok felmérését az integrált kockázatfelmérés keretében kell elvégezni, felelőse az Információbiztonsági Felelős.

Megelőző intézkedések rendszere

10. § (1) A megelőző intézkedések célja a nemkívánatos események megelőzése.

(2) A nemkívánatos események megelőzése érdekében az Egyetem a következő intézkedéseket alkalmazza:
a) informatikai technológiai védelmi intézkedéseket foganatosít annak érdekében, hogy a nagy gyakorisággal bekövetkező fenyegetésekből eredő kockázatok bekövetkezésének valószínűségét vagy bekövetkezésük esetén azok hatását csökkentse;
b) szabályozott folyamatokat vezet be, eljárásrendekben, munkautasításokban rögzíti a biztonsági kontrollok működtetését, illetve az esetleges incidensek feltárását és kezelését;
c) rendszeres biztonságtudatossági oktatásokat végez a humánkockázatok csökkentésére.

Biztonsági események kezelése

11.§ A biztonsági esemény kezelésének célja az információbiztonságot, a szervezet erőforrásainak, folyamatainak, információbiztonsági kontrolljainak működését veszélyeztető, illetve a rendeltetésszerűtől eltérő események figyelése, biztonsági események azonosítása, kezelése, valamint annak lezárását követően tanulságok levonása és védelmi intézkedések meghatározása a biztonsági esemény okának megszüntetésére a további bekövetkezési gyakoriság, illetve hatás csökkentése céljából.

Biztonsági esemény jelentése

12. § (1) A biztonsági eseményt az észlelőnek haladéktalanul jelenteni kell az észleléskor az i3 által a honlapján közzétett elektronikus címen (biztonsági esemény bejelentő csatorna)., illetve a biztonsági esemény bejelentése tehető közvetlenül az Információbiztonsági Felelősnek és az i3 igazgatónak is. Amennyiben a biztonsági esemény személyes adatokat is érint és adatvédelmi incidens is megvalósul egyidejűleg az Adatvédelmi Tisztviselőt, illetve egészségügyi adatok érintettsége esetén az Egészségügyi Adatvédelmi Tisztviselőt is értesíteni szükséges az Egyetem adatvédelmi szabályzataiban foglaltaknak megfelelően.

(2) Biztonsági eseményre utalhat, melyet a felhasználóknak azonnal jelenteniük kell, ha
a) szolgáltatás, a berendezés vagy az eszközök elvesztése történik,
b) rendszer rendellenes működését észlelik,
c) a szabályzatoknak vagy irányelveknek való nem-megfelelés válik nyilvánvalóvá,
d) észlelhető a fizikai biztonsági rendelkezések megsértése,
e) nem ellenőrzött rendszerbeli változásokat tapasztalnak,
f) a szoftver vagy hardver hibás működése lép fel,
g) jogosulatlan hozzáférést tapasztalnak.

(3) Biztonsági eseménynek számít minden, nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat, amely az elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, és amelynek hatására az elektronikus információs rendszer által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül;
Információbiztonsági incidens kezelése során törekedni kell arra, hogy bizonyítékok összegyűjtésre kerüljenek.

(4) Az értesítés rendet külön kancellári utasítás keretében – a biztonsági esemény kezelési rendben – szükséges részletesen meghatározni.

(5) Amennyiben szükséges, a biztonsági eseményt a hatályos jogszabályok szerint jelenteni kell az illetékes hatóságok felé is, a vonatkozó jogszabályokban megkövetelt határidőn belül.

(6) A biztonsági esemény jelentésének elmulasztása az eseményjellegétől és mértékétől függően szankcionálható.

(7) Az i3 arra kijelölt felelőseinek naponta ellenőriznie kell a naplóállományok bejegyzései alapján generált riasztásokat. A naplózásra vonatkozó eljárásrendje tartalmazza a jelentési folyamat leírását.

(8) Az informatikai biztonsági szabályok megsértését jelenteni kell az Egyetem IT Ügyfélszolgálatának és az i3 Infrastruktúra Szolgáltatási Főosztály és Alkalmazás Szolgáltatási Főosztály főosztályvezetőjének. Az i3 igazgató a szabálysértés súlyának ismeretében dönt a következményekről:
a) gondatlanságból elkövetett vagy szándékos, de enyhe szabálysértések esetén figyelmezteti a szabálysértőt és értesíti annak közvetlen felettesét a szabálysértésről;
b) ha a szabálysértés az Egyetem informatikai rendszerének működését sérti, vagy veszélyezteti, jelzi azt az Egyetemi IT Ügyfélszolgálatának, aki vagy
   - minősíti a szabálysértést a körülmények ismeretében, vagy
   - értesíti az Információbiztonsági Felelőst, aki az i3 igazgató, az érintettek bevonásával kivizsgálja a biztonsági eseményt.

(9) A biztonsági esemény kivizsgálásának eredményéről a vizsgálatban résztvevő személyek tájékoztatást adnak a Kancellárnak, aki dönt a további eljárásról.

(10) A biztonsági eseményekből levont tapasztalatokat folyamatosan értékelni kell, és azokat figyelembe kell venni a védelmi rendszer tervezése, szervezése, működtetése során.

(11) Az informatikai rendszerekkel összefüggő biztonsági események és gyengeségek kommunikálása olyan módon történjen, ami időben lehetővé teszi a szükséges helyesbítő intézkedések megtételét.

(12) A felhasználók tudatossági oktatásában ki kell térni arra, hogy hogyan kell válaszolniuk egy-egy felmerült biztonsági eseményre és milyen módon kell elősegíteniük a bizonyítékok gyűjtését.

(13) A részletszabályokat az információbiztonsági incidensek bejelentése, kezelése eljárásrendben kell tartalmazza.

Nem megfelelőség és helyesbítő tevékenység

13. § (1) Helyesbítő tevékenységet kell folytatni biztonsági esemény bekövetkezése során. A megelőző vagy helyesbítő tevékenység révén biztosítható, hogy az információk védelmével kapcsolatos problémák gyorsan és eredményesen kiküszöbölhetők legyenek, a hasonló események bekövetkezési valószínűsége a jövőben csökkenjen. A megelőző és helyesbítő tevékenységek szisztematikus alkalmazásával az információk biztonságának folyamatos javulását érhetjük el.

(2) A megelőző és helyesbítő tevékenységeket általában az alábbi esetekben folytat az Egyetem:
a) felhasználók, vagy külső érdekelt felek (megbízó, tanácsadó, auditor, szakértő stb.) által jelzett információbiztonsággal kapcsolatos észrevételek esetén;
b) egyedi és ismétlődő problémák esetén;
c) a rendszerrel kapcsolatos nem-megfelelőségek esetén (auditjelentés).

(3) A megelőző és helyesbítő tevékenységek során azonosítani kell a problémát, fel kell tárni a hibák okait, a megszüntetésükre és ismételt előfordulásuk megakadályozására intézkedéseket kell kialakítani és bevezetni. A megelőző és helyesbítő intézkedések megvalósítását dokumentálni szükséges és eredményességét meghatározott időközönként mérni kell.

(4) Az Egyetem információbiztonsági rendszerében meghatározott szabályoktól való eltérést az i3 igazgató – az Információbiztonságért Felelős egyetértésével – kizárólag írásban, indokolással engedélyezhet. Az engedélyeket tartalmazó nyilvántartást az i3 vezeti.

Védelmi intézkedések módosítása

14. § A védelmi intézkedések módosítását szükségessé teheti:
a) amennyiben a korábbi védelmi intézkedés szintje nem érte el a kívánt biztonsági szintet;
b) amennyiben egy védelmi intézkedés az indokoltnál jobban korlátozza az egyetemi polgárok munkavégzését;
c) amennyiben az informatikai rendszer változása miatt a korábbi biztonsági kontrollok érvényüket vesztik;
d) amennyiben az adott kontroll elavul és/vagy jobb, újabb technológiák bevezetése válik indokolttá.

Biztonsági események lezárása

15. § (1) A biztonsági esemény kezelése abban az esetben tekinthető lezártnak, amennyiben a biztonsági eseményre való reagálás, elhárítás megtörtént, további károk okozása elhanyagolható, valamint a bizonyítékok gyűjtése és vizsgálata lezárult, az esemény teljes kivizsgálása megtörtént, a szükséges megállapításokat a szakértők megtették és a következtetéseket levonták.

(2) A biztonsági esemény vagy incidens elhárításának lépéseit, illetve kivizsgálásának eredményeit dokumentált módon rögzíteni kell. A dokumentáció lehet jegyzőkönyv, vagy valamely erre a célra alkalmazható informatikai rendszer is.

(3) A biztonsági esemény vagy incidens elhárításáról írásban (elektronikus levél, belső portálon tájékoztatás, felugró ablak) tájékoztatni kell az elhárításban, illetve kivizsgálásban résztvevőket, valamint az érintett munkatársakat. A tájékoztató csak a szükséges és elégséges mértékben kell, hogy tartalmazza az információkat, az események, illetve vizsgálati eredmények részletes megosztása tilos.

Tanulás a biztonsági eseményekből

16. § (1) Az Információbiztonsági Felelős feladata az i3 igazgatója által meghatározott munkatársak bevonásával a biztonsági események során keletkező kár mértékének meghatározása, valamint a biztonsági események során nyert tapasztalatok felhasználásával a meglévő információbiztonsági rendszer tökéletesítése.

(2) A biztonsági esemény ismételt előfordulásának megakadályozása érdekében az Információbiztonsági Felelősnek a szükséges szakértők bevonásával intézkedési tervet kell kidolgoznia. Az intézkedési tervet az Informatikai Bizottság véleményezi, az i3 igazgató hagyja jóvá.

(3) Az intézkedési tervek végrehajtásáról szóló jelentésekben az Információbiztonsági Felelős beszámol a Kancellárnak a biztonsági eseményekről, incidensekről, a kidolgozott és végrehajtott akciótervekről.

A szervezet biztonsági szintbe és az elektronikus információs rendszerek biztonsági osztályba sorolása

17. § (1) A rendszerhez rendelt védelmi intézkedések tervezése és teljesítése az elektronikus információs rendszerek 2. számú mellékletben felsorolt jogszabályi előírásoknak, követelményeknek megfelelően és a hatályos jogszabályban előírtak alapján történik.

(2) Az Ibtv. alapján a szervezet biztonsági szintjét és az elektronikus információs rendszerek biztonsági osztályba sorolását az információbiztonsági felelős javaslatára a Kancellár határozza meg. Az elektronikus információs rendszerek besorolását az 4. számú melléklet, az Egyetem aktuális biztonsági szintjét a 5. számú melléklet tartalmazza.

(3) Amennyiben egy, az Ibtv. hatálya alá tartozó információs rendszernél az elvárt biztonsági szint nem teljesül, a szervezetnek két évente szükséges legalább egy fokozattal magasabb biztonsági szintet elérnie mindaddig, amíg az elvárt szint nem teljesül. A magasabb szint elérése érdekében két évre vonatkozóan cselekvési tervek kidolgozása szükséges, melyek megvalósítása az Információbiztonsági Felelős jóváhagyását követően kezdhető meg.

(4) Az Információbiztonsági Felelős gondoskodik a rendszerek osztályba sorolásának háromévenkénti vagy szükség esetén soron kívüli felülvizsgálatáról. Új rendszer bevezetésekor annak biztonsági osztályba sorolása is megtörténik és meghatározásra kerülnek az osztály követelményeinek teljesítéséhez szükséges intézkedések.

3. fejezet Az információbiztonság szervezete

Információbiztonsági szerepkörök

18. § (1) Az informatikai és az információbiztonsági feladatokat ellátó és az információbiztonság koordinálásában szerepet játszó szervezeti egységeket szervezeti szinten el kell különíteni a Pécsi Tudományegyetem Szervezeti és Működési Szabályzatában, valamint a kapcsolódó mellékleteiben.

(2) Az Egyetem információbiztonsági rendszerének működtetése a Kancellár feladata, tevékenységét az Információbiztonsági Felelős útján gyakorolja. E Szabályzatban meghatározott intézkedési jogköröket a Kancellár által más személyek, szervezeti egységek részére átruházott hatáskörként kell értelmezni.

(3) Az összeférhetetlenség elkerülésének biztosítása érdekében az információbiztonsági és informatikai szervezeti egységeket szervezeti szinten el kell különíteni. Az informatikai szerepkörök és feladatok szervezeti egységre és személyre telepítését úgy kell végrehajtani, hogy a fejlesztési, üzemeltetési, ellenőrzési feladatok ellátásának egymástól való függetlensége biztosított legyen.

(4) Az informatikai és az informatikai biztonsági szerepkörök és feladatok személyre telepítésekor a közvetlen vezető köteles gondoskodni a helyettesítésről.

Adatgazdai szabályozás

19. § (1) Az Adatgazdák feladata az Egyetem adatvagyona tekintetében, hogy a törvényileg és az egyetemi szabályzók által megfogalmazott biztonsági követelményeket érvényesítsék. Az adatok kezelésének szabályaival kapcsolatos felelősségek az adatokat ténylegesen felhasználó szervezeti egységekre hárulnak.

(2) Az Adatgazda kijelölése a Belső kontroll kézikönyvben foglaltakkal összhangban történik.

(3) Minden adatgazdának el kell végeznie és legalább kétévente felül kell vizsgálnia az adatok besorolását. Az adatgazdáknak a hozzájuk tartozó adatkörök nyilvántartásba vételekor, illetve módosulásakor az Adatosztályozó lapot (6. számú melléklet – Adatosztályozó lap), illetve annak tartalmával megegyező nyilvántartást kell küldenie az Információbiztonság Felelősnek.

Külső ügyfelek és partnerek

Általános szabályok

20. § (1) Az információbiztonsági szabályozás szempontjából külső közreműködőnek, (a továbbiakban: harmadik félnek) tekintendő minden olyan külső szervezet, hatóság, szerződéses partner (jogi vagy természetes személy), akinek tevékenysége indokolttá teszi az Egyetem belső használatú és annál magasabb minősítésű adataihoz vagy bármely informatikai rendszeréhez történő hozzáférést.

(2) Kiemelt figyelmet kell fordítani a harmadik fél tevékenységében rejlő kockázatok azonosítására és kezelésére.

Harmadik féllel kötött titoktartási megállapodások

21.§ (1) Az Egyetem informatikai rendszereit, szolgáltatásait használó harmadik fél vonatkozó szerződésében szerepelnie kell titoktartási záradéknak vagy titokvédelmi megállapodásnak, melyben a harmadik fél kötelezettséget vállal arra, hogy a tudomására jutott, a nem publikus egyetemi információkat sem a munkavégzés során, sem annak vége után nem hozza harmadik fél tudomására; továbbá olyan záradékra, amely vagy tartalmazza, vagy utal minden olyan információbiztonsági követelményre, amely biztosítja az Szabályzatnak és az Egyetemen bevezetett szabályoknak való megfelelést. A szerződésben egyértelműen jelölni szükséges, hogy a harmadik fél tevékenységét ki felügyeli.

(2) Minden harmadik féllel kötött megállapodás esetében a megállapodásban rögzíteni kell az adatvédelmi és informatikai biztonsági kérdéseket. Személyes adatokhoz való hozzáférés vagy személyes adatok átadása kizárólag erre vonatkozó írásos szerződés (adatfeldolgozói megállapodás, közös adatkezelői megállapodás vagy az adattovábbítást szabályozó rendelkezések) alapján lehetséges. Az adatfeldolgozói megállapodásra az Egyetem Adatvédelmi Szabályzatának 4. §-a alkalmazandó.

(3) A jogszabályi előíráson alapuló, rendszeres vagy eseti adatszolgáltatások esetén, minden esetben meg kell győződni az adatközlés jogalapjáról, kétség esetén az adatvédelmi tisztviselő vagy egészségügyi adatok esetén az egészségügyi adatvédelmi tisztviselő közreműködését kell kérni. Adatot továbbítani csak abban az esetben lehet, ha annak jogalapja egyértelmű, célja, és az adattovábbítás címzettjének személye pontosan meghatározott.

(4) Az informatikai beszerzések vonatkozásában a Pécsi Tudományegyetem hatályos szabályzatai és vezetői utasításai alapján kell eljárni az információbiztonsági előírások betartása mellett.

A külső partnerekkel történő kapcsolattartás szabályai

22. § (1) Külső partnerek egyetemi informatikai szolgáltatásokhoz történő hozzáférését a vonatkozó 7/2017. számú kancellári utasítás a Pécsi Tudományegyetem informatikai rendszereihez a külső partnerek részére biztosított hozzáférések rendjéről című dokumentum szabályozza.

(2) A kapcsolattartó információbiztonsági kérdésekben elsősorban az Információbiztonsági Felelőstől, továbbá az i3 igazgatótól, valamint a személyes adatok védelmével kapcsolatos kérdésekben az egyetemi adatvédelmi tisztviselőtől, egészségügyi adatok esetén az egészségügyi adatvédelmi tisztviselőtől tájékoztatást vagy állásfoglalást kérhet.

(3) A személyes adatok vonatkozásában a Pécsi Tudományegyetem Adatvédelmi Szabályzata, míg az egészségügyi adatok kapcsán a Pécsi Tudományegyetem Egészségügyi Adatvédelmi Szabályzata az irányadó.

Ellenőrzések, monitorozás

23. § (1) A jelen fejezetben rögzített, harmadik félre vonatkozó információbiztonsági előírásokat az Információbiztonsági Felelős a jelen Szabályzatban rögzítettek szerint köteles ellenőrizni.

(2) A harmadik féllel kötött szerződésben biztosítani kell az ellenőrzés Informatikai Biztonsági Felelős által történő elvégzésének lehetőségét.

(3) A harmadik fél által nyújtott szolgáltatások színvonalát monitorozni kell és vizsgálat keretében ellenőrizni szükséges, hogy a szerződésben előírt biztonsági előírások és egyéb szabályok betartásra kerülnek.

A harmadik fél által nyújtott szolgáltatások változásainak kezelése

24. § A harmadik féllel kötött szerződésben megkövetelt és bevezetett biztonsági intézkedések – beleértve a szabályzatokat, eljárásokat is – változásainak kezelésére olyan eljárásokat kell kidolgozni, melyek figyelembe veszik a folyamatok és rendszerek kritikusságát, az információbiztonsági előírások betartását, valamint biztosítják a kockázatok újraértékelését.

A harmadik féllel kötött megállapodások információbiztonsági követelményei

25. § A jelen Szabályzat hatálya alá tartozó szerződéseknek lehetőség szerint ki kell térnie az alábbi információbiztonsági követelmények és elvárások meghatározására:

a) az információk bizalmasságának, sértetlenségének és rendelkezésre állásának megőrzési követelményeit, a külső szereplőkre vonatkozó általános információbiztonsági előírásokat,
b) az elektronikus levelezés, fájlok titkosításának szabályait,
c) a papír alapú dokumentumok kezelésének információbiztonsági szabályait,
d) amennyiben értelmezhető:
   - a látogatókra vonatkozó fizikai biztonsági szabályokat,
   - a hozzáférés módját az egyetemi IT- és információs rendszerekhez, a hozzáférés szabályait és a felhasználó felelősségeit,
   - a dokumentumok és adathordozók átadásának, cseréjének és kezelésének információbiztonsági követelményeit és az ezzel kapcsolatos felhasználói felelősségeket;
e) a szerződésben foglalt információbiztonsági követelmények megszegéséből származó szankciókat,
f) a harmadik félnél történő személyi változások kezelését,
g) a szerződés megszűnésekor vagy lejártakor az információk és átadott információhordozók visszaadásának, valamint a szerződéses partner adathordozóján lévő információk megsemmisítésének

követelményeit.

4. fejezet Az információ védelme, részletes védelmi intézkedések meghatározása

Részletes védelmi intézkedések minimum követelményei

26. § Annak érdekében, hogy az információ védelme egységesen legyen kezelve az Egyetemen belül, és a szükséges és elégséges információbiztonsági követelmények, kontrollok meghatározhatóak legyenek, legalább az alábbiak végrehajtása szükséges:

a) adatvagyon felmérés;
b) üzleti hatáselemzés készítése;
c) kockázatelemzés készítése;
d) informatikai rendszerek biztonsági osztályba sorolása;
e) hozzáférés és jogosultság menedzsment folyamatok működtetése,
f) adatvagyon elemek személyes, illetve egészségügyi adatköri minősítése.

Emberi erőforrásokkal kapcsolatos biztonsági intézkedések

27. § (1) A részletszabályokat a foglalkoztatott munkavégzésre irányuló jogviszonyának létesítése, megszűnése, valamint munkakörváltozása esetén érvényes eljárásrendje tartalmazza.

(2) Minden foglalkoztatottnak belépéskor alá kell írni a Titoktartási nyilatkozatot.

(3) Az Egyetem foglalkoztatottjaival a munkáltatói joggyakorlónak meg kell ismertetnie az Informatikai Biztonsági Szabályzat beosztásuk alapján rájuk vonatkozó szabályait:

a) az alkalmazandó információbiztonsági szabályokat;
b) az informatikai rendszerek használatával kapcsolatosan elvárt és tiltott magatartásokat, azok megsértésének szankcióit;
c) az informatikai rendszer számára nagy kockázattal járó fenyegetések és veszélyforrások közérthető magyarázatát, a biztonságtudatosság fokozása érdekében.

Általános információbiztonsági előírások a munkavégzés során

28. § (1) Minden esetben törekedni kell az „Üres íróasztal, tiszta képernyő” politika betartására, a munkanap végén irat nem maradhat az asztalokon, illetve a munkakörnyezetben.

(2) A nyomtatókról azonnal el kell távolítani a kinyomtatott iratokat.

(3) Az aktuálisan nem használt számítógépet ki kell kapcsolni vagy jelszóvédetten kell zárolni.

Áthelyezés, munkavégzésre irányuló jogviszony megszűnése, Informatikai eszközök visszaszolgáltatása

29. § (1) A foglalkoztatott kiléptetésekor a Pécsi Tudományegyetem HR Kézikönyvében foglaltak az irányadóak.

(2) Valamennyi foglalkoztatottnak és minden, az Egyetem informatikai rendszereit, szolgáltatásait használó harmadik félnek vissza kell szolgáltatnia az Egyetem valamennyi, használatra átvett informatikai vagyontárgyát, amikor foglalkoztatása, szerződése, megállapodása lejár vagy megszűnik. A visszaszolgáltatás azon szervezeti egység részére történik, ahol a vagyontárgy nyilvántartásba vétele korábban megtörtént.

(3) Az i3 az eszköz leadásakor ellenőrzi az átvett és az Átadás-átvételi lapon rögzített hardver-, szoftver specifikáció meglétét és üzemképes állapotát. Ez alól kivételt képez a Klinikai Központ nyilvántartásába tartozó eszközök visszavétele, melyek esetében az Egészségügyi Gazdálkodási Igazgatóság végzi az ellenőrzést.

Információbiztonsági oktatás és képzés, az információbiztonsági tudatosság elérése

30. § (1) A biztonságtudatossági oktatás célja, hogy az Egyetemen foglalkoztatottak értesüljenek a rájuk vonatkozó, Egyetem által előírt szabályozásokról, biztonsági előírásokról, tisztában legyenek azok betartásának szükségességével, tudomást szerezzenek az őket fenyegető lehetséges veszélyekről, támadási technikákról és elhárításukról, észlelésükről és jelentési módjukról.

(2) Az Egyetem informatikai rendszerei felhasználóinak a munkakörükhöz igazodó informatikai és információbiztonsági oktatást kell biztosítani, lehetőleg az informatikai rendszer használata előtt, illetve az általuk használt informatikai infrastruktúra változásakor (pl. új hardver vagy szoftver használatba vétele előtt), valamint az információbiztonsági kockázatok jelentős változásakor, új kockázati elem megjelenésekor.

(3) Az oktatás előkészítése során az Információbiztonsági Felelős feladata az alábbiak meghatározása:

a) a szükséges tanfolyamok (struktúra és témakör) meghatározása;
b) javaslat a képzésben részesítendő munkakörök/szerepkörök meghatározására;

c) oktatásra javasoltak meghatározása;
d) az oktatók személyére vonatkozó javaslattétel (amennyiben a képzés nem külső szervezésű).

(4) Az információbiztonsági tudatossági oktatáson való részvétel kötelező rendszeresen évente egy alkalommal, továbbá eseti jelleggel a következő események bekövetkezése után:
a) jelen Szabályzat hatályba lépését vagy jelentős módosulását követően;
b) új foglalkoztatott belépésekor az új belépő részére;
c) biztonsági esemény bekövetkezését és kivizsgálását követően az érintettek részére, amennyiben az Információbiztonsági Felelős indokoltnak látja a képzést.

(5) Az oktatás megvalósítási módját tekintve lehet tantermi, e-learning oktatás vagy ezek kombinációja is. Az oktatásnak tartalmaznia kell a kialakított Szabályzat előírásait is. Az oktatásokat a Belső képzési központnak kell megszerveznie. Az oktatásokon való részvételt hitelt érdemlően kell dokumentálni.

(5) A képzéshez kapcsolódóan – igény esetén – az i3 támogatást nyújt.

Az informatikai biztonság megsértése, veszélyeztetése esetén alkalmazandó következmények

31. § (1) Az informatikai szolgáltatások igénybevétele során elkövetett szabálysértésekért, illetve jogsértésekért a szolgáltatást igénybe vevő munkajogi, polgári jogi és büntetőjogi felelősséggel felelhet, amennyiben nem a szabályzatokban foglaltak szerint járt el és ennek következményeként jogsértés következett be.

(2) A Szabályzat, a vonatkozó jogszabályok, belső szabályzatok be nem tartása, valamint az informatikai biztonság veszélyeztetése, megsértése esetén a felhasználóval szemben fegyelmi, kártérítési, szabálysértési, illetve büntetőjogi felelősségre vonásnak lehet helye a vonatkozó jogszabályok, szabályzatok, illetve a Kollektív Szerződésben meghatározottak szerint.

(3) Az Információbiztonsági szabályok megsértésének gyanúja, illetve ilyen szabálysértéssel kapcsolatos tisztázatlan körülmények felmerülése esetén, az előbbieket észlelő személynek, értesítenie és tájékoztatnia kell az Információbiztonsági Felelőst, aki indokoltság esetén javaslatot tehet az i3 igazgató felé, vizsgálati eljárás lefolytatására. A javaslat alapján, az i3 igazgató utasítást ad az eset kivizsgálására.

Informatikai vagyonleltár

32. § Az Egyetem birtokában lévő informatikai vagyontárgyak egyértelmű azonosítása, nyilvántartása kötelező. Az ezekről felvett vagyonleltárt folyamatosan karban kell tartani. A kapcsolódó szabályokat a Pécsi Tudományegyetem Leltározási és Leltárkészítési szabályairól szóló kancellári utasítás tartalmazza.

Fizikai biztonság

Az Egyetem létesítményeibe való bejutás

33. § (1) Az Egyetem területén működő elektronikus beléptető rendszerrel ellátott helyiségek és területek elektronikus beléptető kártyáinak igénylését és a használat rendjét a Pécsi Tudományegyetem Biztonsági Szabályzata tartalmazza.

(2) Az informatikai helyiségekbe való belépés rendjét az i3 Infrastruktúra Szolgáltatási Főosztály alakítja ki, működteti és szabályozza a jelen Szabályzatban foglalt előírásokra tekintettel.

Az informatikai helyiségek nyilvántartása

34. § (1) A Pécsi Tudományegyetem Biztonsági Szabályzata rendelkezik az Egyetem épületei, értékei és polgárai védelmének megszervezéséről, a feladatkörökről, valamint a figyelembe veendő szempontrendszerekről.

(2) Informatikai helyiségek az Egyetem mindazon helyiségei, amelyekben az informatikai infrastruktúra központi elemei elhelyezésre kerülnek:

a) szerverek;
b) telefonközpontok;
c) hálózati elosztószekrények, központi hálózati eszközök;
d) alkalmazói és irodai szoftverek és informatikai rendszer- vagy eszköz dokumentációk törzspéldányai;
e) biztonsági mentések.

(3) Az informatikai helyiségek tételes nyilvántartásáról az i3 utasítása szerint az Egyetembiztonsági Osztály gondoskodik.

Informatikai helyiségek kialakításának alapvető szabályai

35. § (1) Az informatikai szolgáltatások fizikai komponensei (szerver, tároló alrendszer, router stb.) csak külön erre a célra kialakított, megfelelő biztonsági paraméterekkel rendelkező helyiségekben informatikai helyiségekben működtethetők. A helyiségeket biztonságos mechanikus zárakkal (biztonsági zár, vagy beléptető kártyával működtethető zár) és beléptető rendszerrel kell ellátni.

(2) Az informatikai helyiségeket vagyonvédelmi célból lehetőség szerint kamerás megfigyelőrendszerrel szükséges ellátni és a vonatkozó jogszabályok szerint kell azokat üzemeltetni.

(3) Az informatikai helyiségekben a hatályos szabályozás szerinti tűzvédelmi minősítést el kell végezni, és a minősítéshez igazodó, oltás esetén a lehető legkisebb kárt okozó oltóberendezéssel kell rendelkezniük.

(4) Az informatikai helyiségek villám- és túlfeszültségvédelmét, valamint szünetmentes áramellátását biztosítani kell.

(5) A beléptető rendszer szükséges alapkonfigurációi: belépő személy azonosítása kód vagy kártya alapján, belépési jogosultság megállapítása, belépési időpont regisztrálása, jogosulatlan belépési kísérlet jelzése a biztonsági személyzet felé.

(6) Mind az informatikai helyiségek, mind a telephelyi egyéb helyiségek esetében a bejárati ajtónak zárt állapotban kell lennie, nyitvatartásuk csak a közlekedés idejére, felügyelet mellett engedélyezett.

(7) Az egyéb helyiségekben is gondoskodni kell a megfelelő tűz-, villám-, és túlfeszültség védelemről.

(8) Az informatikai helyiségekbe való belépési jogosultságot az i3 igazgatója, vagy az informatikai üzemeltetésért felelős főosztályvezetője engedélyezheti, a helyiségek és a végezhető munka felsorolásával. A belépési jogosultsággal rendelkezők e jogosultságukat nem ruházhatják át másra.

(9) Amennyiben az informatikai helyiségekbe belépési jogosultsággal rendelkező egyetemi polgár jogosultságát átruházza vagy a jogosultságával egyéb módon visszaél, továbbá amennyiben az informatikai helyiségekbe belépési jogosultsággal nem rendelkező személy lép be, hallgató esetén fegyelmi, munkavállaló esetén munkáltatói felelősségre vonásnak van helye. Jogosulatlan személy beengedéséből fakadó eseményekért a felelősség a beengedő személyt terheli.

(10) 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. A

megfogalmazottakon túl az erősáramú és gépészeti berendezéseknek redundánsnak kell lenniük, azaz egy meghibásodása nem okozhatja a helyiségben üzemelő eszközök leállását.

(11) Az informatikai helyiségekben minden olyan munkavégzés, ami az informatikai szolgáltatásokat vagy azok működését veszélyezteti, csak előzetes egyeztetés alapján, az i3 munkatársfelügyelete mellett végezhető.

(12) Az egyeztetést, a munkálatokat végző szervezeti egység vagy cég, és az i3 üzemeltetésért felelős főosztályvezetője végzi.

(13) A helyiséget kiszolgáló gépészeti és erősáramú berendezések működését veszélyeztető munkák csak az i3 üzemeltetésért felelős főosztályvezetője előzetes engedélyével folytathatók.

(14) A gépészeti, vagy erősáramú berendezéseken történő munkavégzésből eredő károkért és szolgáltatás kiesésért a munkát végző felel. Külső vállalkozó által végzett munkavégzés esetén a munkáért a munkák egyetemi megrendelője felel, kivétel, ha a szerződésben a felek másként rendelkeznek.

(15) Az informatikai helyiségeket kiszolgáló gépészeti és erősáramú rendszerekre külön karbantartási tervet kell készíteni, amelyet az Üzemeltetési és Beszerzési Igazgatóság üzemeltetésért felelős vezetője állít össze és gondoskodik a végrehajtásáról. A tervet az i3 üzemeltetésért felelős vezetői véleményezik és hagyják jóvá.

(16) 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.

(17) Az egyéb munkaterületek (pl. irodák) használatának módja megegyezik az általános egyetemi területek használati módjával.

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

(19) Az informatikai célú helyiségekkel kapcsolatos kérdésekben, a ki- és átalakítás koordinációjáért, a szakmai biztonsági szempontok betartásáért az adott helyiséghez tartozó szervezeti egység vezetője és az i3 Infrastruktúra Szolgáltatási Főosztály vezetője a felelős.

(20) Az Egyetem területén kifejezetten informatikai szolgáltatások biztosítását lehetővé tévő, informatikai eszközöknek helyt adó informatikai helyiségekhez az i3 igazgató által hitelesített, fényképes igazolvánnyal rendelkező munkavállaló férhet hozzá fizikailag, a helyiségben található eszközök üzemeltetését kizárólag ezen személyek végezhetik. Egyéb személyek kizárólag ezen munkavállalók felügyelete mellett léphetnek és tartózkodhatnak ezekben a helyiségekben.

(21) Az informatikai helyiségekben üzembe állítandó új szolgáltatások, vagy nagyobb rendszerkonfiguráció módosítás esetén a telepítés előtt előzetesen konzultálni kell az erősáramú és hűtési igény biztosításáról a gépészeti és erősáramú rendszerek működéséért felelős vezetővel. A szükséges gépészeti és erősáramú módosításokat az új szolgáltatás üzembe állítása előtt el kell végezni.

(22) Az informatikai helyiségeken kívül húzódó kábeleket (telefon és gerinchálózati kábeleket) tartalmazó egyetemi, vagy szolgáltatói tulajdonú alépítmények, kábelaknák és védőcsövek kiemelten óvandó területnek minősülnek. Azokban munkát végezni, vagy a megközelíthetőségüket korlátozni, csak az i3 üzemeltetéséért felelős vezetőinek előzetes engedélyével lehet.

Informatikai helyiségek kialakításának további szabályai

36. § (1) Az egyetemi informatikai infrastruktúra elhelyezésének és az egyes központi és tartalék informatikai helyiségek kiválasztásának és kialakításának során az egyes informatikai helyiségekben elhelyezésre kerülő

informatikai eszközök üzemeltetési előírásaiban megfogalmazott környezeti paramétereknek megfelelő környezet kell biztosítani legalább az alábbi informatikai biztonsági szempontokat figyelembevételével:

a) A környezeti kockázatokat (füstérzékelő, vízbetörés érzékelő) folyamatosan figyelemmel kell kísérni. Az érzékelők karbantartását rendszeresen el kell végezni.
b) A hatályos tűzvédelmi előírások és szabályzatok szerint kell a tűzvédelmet biztosítani. Automatikus tűzoltó palackok elhelyezése kötelező.
c) Az informatikai helyiségekben használni tervezett erőforrások biztonságos működéséhez szükséges szinten kell tartani a hőmérsékletet, és annak szintjét figyelemmel kell kísérni.
d) Az informatikai helyiségeket úgy kell kialakítani, vagy az épület átépítése során csak úgy szabad a változtatásokat jóváhagyni, hogy a csővezetékek (pl. víz, csatorna, kondenzvíz, tűzi víz) rongálódásból származó károkkal szemben védve legyenek. Ahol az áthelyezésük nem megoldható, ott kiegészítő kontrollokat kell alkalmazni (pl. vízérzékelő, csepptálca).
e) Behatolás védelem.
f) Elhelyezés bejárattól, közösségi tértől távolabb, mindenképpen olyan helyen, ahová csak a portaszolgálaton, beléptető kapun át lehet eljutni, lehetőség szerint további fizikai védősávokkal (zárt folyosó, recepció) védve.
g) Elhelyezés oly módon, hogy maga az informatikai helyiség ne legyen feltűnő, frekventált helyen (pl. büfé, dohányzásra kijelölt folyosószakasz mellett).
h) Elhelyezés oly módon, hogy a helyiségek helye és jelentősége ne legyen bárki számára nyilvánvaló.
i) Áramellátás és áramvédelem:
   - szűrt és teljes túlfeszültség-védelemmel ellátott elektromos hálózat;
   - szünetmentes ideiglenes tartalék áramforrás (UPS), amely minimum 30 percig, de legalább az aggregátor elindításáig, illetve amennyiben nincs aggregátor, akkor legalább a rendszer rendeltetésszerű leállításáig biztosítsa az áramellátást;
   - tartós tartalék áramforrás (pl.: diesel generátor), amennyiben nincs lehetőség tartalék áramforrás használatára, kialakítására, úgy a szünetmentes tápegységet kell úgy méretezni, hogy az üzleti területek által meghatározott rendelkezésre állást az informatikai eszközökön biztosítani tudja.

(2) Informatikai helyiséget az i3 igazgató előzetes hozzájárulása és az Információbiztonsági Felelős tájékoztatása nélkül kialakítani és üzemeltetni tilos.

Informatikai eszközök védelme

Informatikai eszközök elhelyezése és védelme

37. § (1) Az informatikai eszközöket úgy kell elhelyezni, illetve védeni, hogy kockázati besorolásuknak megfelelő mértékű legyen a környezeti fenyegetésekből és veszélyekből eredő kockázat, valamint a jogosulatlan hozzáférés lehetősége szerint.

(2) A védelmi intézkedések biztosítják, hogy a különböző környezeti hatás miatt keletkező meghibásodások, adatvesztések csökkenjenek. A védelmi intézkedések érdekében:

a) a berendezéseket úgy kell elhelyezni, hogy a kapcsolódó munkaterületekre a szükségtelen belépéseket minimalizáljuk;
b) az érzékeny adatokat tároló és feldolgozó eszközök és munkahelyek monitorjait úgy kell elhelyezni (amennyiben lehetősége van rá, betekintésvédő fóliát alkalmazni), hogy azok használata közben illetéktelenek ne láthassák a képernyőn megjelenő adatokat;
c) intézkedéseket kell bevezetni a lopás, tűz, robbanóanyagok, füst, víz (vagy a vízellátás meghibásodása), köd, rázkódás, vegyi behatások, a villamos energiaellátás zavarai, elektromágneses sugárzás által okozott kockázatok minimalizálására;
d) az adatfeldolgozó eszközök közvetlen közelében folytatott étkezést, folyadékfogyasztást vagy dohányzást tiltani kell;
e) a környezeti feltételeket állandóan figyelni kell az olyan helyzetek felismerése érdekében, amelyek az adatfeldolgozó eszközök működésére negatív hatással lehetnek;
f) az adatfeldolgozó eszközöknek helyet adó épületeket villámvédelemmel, az elektromos tápellátást és a kommunikációs vonalakat pedig villámvédelmi szűrővel kell ellátni;

g) be kell tartani a tűzvédelmi és egyéb előírásokat a Pécsi Tudományegyetem Tűzvédelmi Szabályzatában foglaltaknak megfelelően.

(3) Az informatikai eszközöket folyamatos rendelkezésre állásuk és sértetlenségük biztosítása érdekében a gyártó útmutatása alapján, előírásoknak megfelelően karban kell tartani, amelyért az i3 Infrastruktúra Szolgáltatási Főosztály felelős.

A kábelezés biztonsága

38. § (1) Az adatátvitelt biztosító, az információszolgáltatásokat támogató elektromos, energiaátviteli és távközlési kábelhálózatot védeni kell az illetéktelen hozzáféréstől és a károsodástól.

(2) Fentiek megvalósításáért, ideértve a zárható szekrények és helyiségek kulcsainak tárolásáért, nyilvántartásáért az i3 igazgató és az Egyetembiztonsági Osztályvezető felel.

(3) Gondoskodni kell a berendezések megfelelő védelméről az áramszünet és egyéb elektromos rendellenesség esetén.

Tápáramellátás

39. § (1) Gondoskodni kell a berendezések megfelelő védelméről az áramszünet és egyéb elektromos rendellenesség esetében.

(2) A magas rendelkezésre állású kategóriába sorolt központi informatikai infrastruktúra folyamatos tápáramellátását

a) szünetmentes áramforrás;
b) több utas betáplálás;
c) tartalék-áramforrás

alkalmazásával kell biztosítani.

Az informatikai eszközök karbantartása

40. § (1) Az informatikai infrastruktúra, illetve eszközök karbantartását a gyártói útmutatás alapján, előírásszerűen kell elvégezni a folyamatos rendelkezésre állás érdekében. Ennek megvalósításáért az i3 Infrastruktúra Szolgáltatási Főosztály felelős.

(2) A Klinikai Központban, valamint azon szervezeti egységek esetében, melyek nem rendelkeznek a Kancellária által delegált területi informatikai referenssel, a karbantartási feladatok végrehajtásáért az adott szervezeti egység vezetője felelős.

Vagyontárgyak – telephelyről való eltávolítás, elszállítás

41. § (1) Az i3 igazgató előzetes engedélye nélkül nem vihetők ki az Egyetem területéről az informatikai eszközök, szoftverek, kivéve a személyes leltárban található eszközöket és az ezekre telepített szoftvereket.

(2) Az Egyetem területéről kivitt eszközök és adatok használata során bekövetkező károkért az a személy viseli a felelősséget, aki az eszközt az Egyetem területéről kivitte. Az Egyetem területénkívüli használat, munkavégzés során mindazon elvek és gyakorlat követendő, amelyek az Egyetem területénbelüli használat esetén is irányadók.

(3) Az adattároló médiumok, az információ és más értékek fokozott fenyegetettségnek vannak kitéve szállítás közben, ezért alábbi kontrollok megfelelő alkalmazásával kell gondoskodni biztonságukról:

a) az érzékeny, bizalmas információk, adathordozók szállítása esetén egyéb speciális kontrollokat is alkalmazni kell, mint:
   - a szállítandó eszközöket megfelelő csomagolással kell ellátni a fizikai károsodások (mágneses behatások) megelőzése érdekében;

- zárható tároló doboz, vagy hordtáska alkalmazása;
- olyan csomagolás alkalmazása, mely felbontás után nem zárható vissza az eredeti formában, így az esetleges illetéktelen hozzáférés felderíthető;
- kriptográfiai módszerrel történő titkosítás elektronikus adathordozó esetén;
- mobileszközök szállítása kizárólag zárolt állapotban hajtható végre.

b) javítás céljából az érzékeny információk, adathordozók elszállítására a következő kontrollokat kell alkalmazni:
- merevlemez (munkaállomás, nyomtató stb.) törlése, amennyiben ez lehetséges;
- amennyiben a vagyontárgyat (pl. szervizelésre kijelölt nyomtató) az Egyetem bármely területéről harmadik fél szállít el, a vagyontárgyat átadó személynek meg kell bizonyosodni arról, hogy a szállítást végző személy (pl. fényképes igazolvány, megbízólevél, céges bélyegző megléte stb. segítségével) valóban az adott szerződéses partnerhez tartozik, illetve a vagyontárgyat hiánytalanul átvette-e (pl.: felkerül a teherautóra) – az átvételről átadás-átvételi nyilatkozat kiállítása szükséges.

A mobil informatikai eszközök biztonságos használata

42. § (1) A mobil eszköz használatát a szervezeti egység vezetője hagyja jóvá. Az Egyetem tulajdonában lévő mobil eszközök munkavégzés céljából kerülnek átadásra.

(2) A mobil eszközök használatára vonatkozóan legalább az alábbi irányelvek betartása kötelező:
a) tilos felügyelet nélkül nyilvános helyen, gépkocsiban hagyni;
b) az Egyetem informatikai rendszeréhez kapcsolódni csak az Egyetem eszközével és az i3 által biztosított módon (pl. VPN) lehet;
c) gyártó előírásokat mindig be kell tartani az eszköz védelme érdekében;
d) amennyiben az Egyetem informatikai rendszeréhez idegen tulajdonú eszköz csatlakoztatása szükséges, arra csak írásbeli engedély alapján kerülhet sor;
e) mobil eszköz elhagyása, elvesztése vagy másnak tartós használatra való átadásakor, amennyiben az eszközön be van állítva valamilyen egyetemi informatikai szolgáltatás elérése, a felhasználó köteles bejelentést tenni az Egyetemi IT Ügyfélszolgálatának a szolgáltatás és az eszköz közti kapcsolat mielőbbi törlése érdekében.

Az informatikai eszközökön adatok biztonságos megsemmisítése, az eszközök újra felhasználása

43. § (1) A használatból kivont információ-feldolgozó eszközöket szükség esetén egy hónapig raktározni lehet az esetleges visszaállítás érdekében, feliratozva, illetéktelen hozzáféréstől védve, annak érdekében, hogy fontos információk ne semmisüljenek meg és ne szivárogjanak ki.

(2) Az adott szervezeti egység kezelésében lévő adathordozók tekintetében a megsemmisítését vagy újra felhasználását kizárólag az Adatgazda kezdeményezheti.

(3) Amennyiben a nagy mennyiségű adathordozók megsemmisítését harmadik fél végzi, a megsemmisítést kizárólag erre a feladatra megfelelő felkészültséggel rendelkező partner végezheti. Az adathordozók megsemmisítésére irányuló szerződésben kell külön rögzíteni a titoktartási feltételeket, illetve a szerződőnek garanciát kell vállalni az adatok visszaállíthatatlan megsemmisítésére, a teljes és időbeli korlátozás nélküli titoktartásra is.

(4) Az eszközökben található adathordozókról az adatokat újra felhasználás előtt visszaállíthatatlan módszerrel törölni (WIPE) kell, akkor is, ha az nem tartalmaz bizalmas adatokat.

(5) Az informatikai eszközök selejtezéséről A Pécsi Tudományegyetem felesleges vagyontárgyak selejtezéséről, belső hasznosításáról szóló szabályzata rendelkezik

5. fejezet Informatikai üzemeltetés, fejlesztés biztonsága, beszerzése

Általános rendelkezések

44. § (1) Az informatikai szolgáltatások beszerzésére, fejlesztésére vonatkozó igényt minden esetben az Egyetemi IT Ügyfélszolgálatán, e-mailen, vagy az önkiszolgáló ügyfélszolgálati rendszerben kell jelezni. A telefonon, illetve nem az ügyfélszolgálaton jelzett igény az írásos megkeresést megelőzően nem kezelhető.

(2) Új informatikai szolgáltatás bevezetését megelőzően az adott szolgáltatásért felelős szolgáltatásgazda vagy alkalmazásgazda kijelölése szükséges, a Rendszerkatalógusban való rögzítéssel egyidejűleg.

(3) Az informatikai üzemeltetésre, fejlesztésre és beszerzésre vonatkozóan a Pécsi Tudományegyetem Informatikai Szabályzatában foglaltak az irányadók.

Dokumentált üzemeltetési eljárások

45. § (1) A magas szintű szolgáltatásnyújtás elengedhetetlen feltétele az informatikai infrastruktúra esetében a megfelelően dokumentált, egységes elvek szerint történő üzemeltetés, amit az informatikai üzemeltetési eljárásrendben a foglaltaknak megfelelően szükséges kialakítani. A kapcsolódó szabályozókat, munkautasításokat, üzemeltetési kézikönyveket minden informatikai szereplő számára elérhetővé kell tenni.

(2) Az informatikai szolgáltatásokkal összefüggő minden változást nyomon követhető módon dokumentálni szükséges, így különösen

a) a hozzáférések engedélyezését, módosítását,
b) a rendszer konfigurációk módosítását,
c) a fizikai hozzáféréseket.

(3) Minden szolgáltatás esetében az adott szolgáltatásra szabottan szükséges a dokumentációs rendet kidolgozni.

Változáskezelés

46. § (1) Változás alatt kell érteni nem csak a rendszerfejlesztéseket, hanem a rendszerek komponenseinek, illetve biztonsági beállításainak lényeges és az elfogadott standardoktól, szabályoktól eltérő módosítását is. Az információ-feldolgozó eszközök és rendszerek változtatásait nyomon kell követni, a változásokat előzetesen meg kell tervezni (tesztelés, végrehajtás lépései, szükség esetén a visszaállítás lépései) és az i3 igazgatóval engedélyeztetni.

(2) Minden olyan információ feldolgozó eszközökben és rendszerekben (éles, fejlesztői és teszt környezetben egyaránt) bekövetkező változást, amely hatással van az információbiztonságra, felügyelet alatt kell tartani, illetve dokumentálni kell.

(3) Minden tervezett változtatásról, amely hatással lehet az információbiztonságra, tájékoztatást kell küldeni az Információbiztonsági Felelős részére is.

Informatikai beszerzések és fejlesztések

47. § (1) Az Egyetem által üzemeltetett (fejlesztési-, tesztelési- és éles) környezeteket fizikailag és logikailag egymástól külön kell választani. Ezeknél a felhasználók számára egyértelművé kell tenni az azonosítást.

(2) Az egyes rendszerekkel szemben támasztott követelményekről a Pécsi Tudományegyetem Informatikai Szabályzata rendelkezik.

(3) A külső fejlesztésű rendszerek szerződésének tartalmaznia kell a telepítési és használati feltételeket, valamint a fejlesztési lehetőségeket, verziókövetést. Ebben az esetben a fejlesztővel, szállítóval kötött szerződésben kell kitérni jelen Szabályzat 25. §-ában részletezett információbiztonsági követelményekre, melyet az Információbiztonsági Felelős ellenőrizhet.

Hibakezelés, konfigurációkezelés

48. § A rendszerspecifikus előírások tartalmazzák az egyes rendszerekre vonatkozó speciális feltételeket és előírásokat.

Tesztelés, a tesztadatok kezelése

49. § (1) Új rendszer fejlesztésének vagy meglévő módosításának megkezdésekor azonosítani kell a fejlesztéssel kapcsolatos kockázatokat, az Alkalmazás Szolgáltatási Főosztály vezetője vagy az általa kijelölt személy felelőssége, hogy az érintett területeket bevonja a kockázatelemzésbe. Amennyiben más (meglévő) rendszerhez is kapcsolódik, abban az esetben meg kell vizsgálni a kapcsolatot és az új sérülékenység felmerülése esetén, a kockázatelemzés frissítése szükséges.

(2) Az informatikai biztonsági kockázatok felmérése az Információbiztonsági Felelős feladata.

(3) Valós (ügyfél) adatok csak anonimizálást követően használhatók fejlesztési és teszt célokra (synthetic/anonymised database). Az adatgazda részéről előzetes jóváhagyás szükséges, amennyiben éles adatok kerülnek átmásolásra a teszt- vagy fejlesztési rendszerbe. A tesztrendszerben és az éles rendszerben beállított jogosultságoknak azonosnak kell lenni. Amennyiben a teszt végrehajtásához magasabb jogosultság szükséges a tesztelést végző személynek, abban az esetben csak anonim adatbázis használata szükséges. A fejlesztői környezeten és külső partnerek számára elérhető adatbázisban csak anonimizált adatok szerepelhetnek.

(4) A tesztelési tervek és jegyzőkönyvek meglétét, a dokumentumok tartalmát az Információbiztonsági Felelős bármikor ellenőrizheti. A kért dokumentumokba mind az informatikai szolgáltató, mind a külső fejlesztő biztosítja az Információbiztonsági Felelős betekintését.

Kártékony kódok elleni védelem

Rosszindulatú szoftverek (malware) elleni védekezés

50. § (1) Az elektronikus információs rendszerek kilépési és belépési pontjain úgy kell kialakítani a kártékony kódok elleni védelmi eljárásokat, a kapcsolódó szabályozást és intézkedési tervet, hogy elsősorban felderítsék és megsemmisítsék azokat, továbbá

a) lehetővé tegyék a folyamatos felügyelet ellátását;
b) a valós riasztások kiszűrését támogassák;
c) a súlyos gondatlanságot, esetleg szándékosságot jelentő esetek kiszűrését támogassák;
d) a kártékony kódok elleni védekezés általános helyzetének értékelését lehetővé tegyék;
e) az új fenyegetések időben történő felismerését biztosítsák;

(2) A vírusvédelmi rendszer információbiztonsági szempontból történő kiválasztása és jóváhagyása az Információbiztonsági Felelős felelőssége. A kártékony kódok elleni védelemmel kapcsolatos üzemeltetési feladatokat, a konfigurációkezelési szabályokkal és eljárásokkal összhangban a vírusírtó rendszerhez és operációs rendszerekhez kapcsolódó frissítések kezelését az i3 látja el.

(3) Felhasználói számítógépeket (PC, notebook) – legyen az egyetemi vagy saját tulajdonú, mellyel a foglalkoztatottak egyetemi belső hálózathoz, szolgáltatáshoz, vagy erőforráshoz csatlakoznak - az i3 által központilag biztosított Desktop Menedzsment rendszerbe bevonni szükséges, mellyel a felhasználói számítógépek frissítési, biztonsági állapotának felügyelete (operációs rendszer, szoftverek, vírusvédelem), valamint a bekövetkezett biztonsági események központi naplózása biztosított.

Vírusvédelmi eljárások és védelmi eszközök

51. § (1) Az Egyetem hálózatában az i3 központilag biztosítja és felügyeli az általa üzemeltetett területeken a többszintű vírusvédelmi rendszert. Amennyiben egy számítógép, felhasználói munkaállomás vírussal

fertőződik az i3 az ellenőrzés és a vírusírtás idejére kizárhatja azt a hálózatból, ebben a folyamatban a felhasználó köteles együttműködni az i3 munkatársaival. Az i3 jogosult több munkaállomás egyidejű fertőzése esetén adott hálózati szegmens kizárására vagy izolálására.

(2) Az egyetemi infrastruktúra használatára csak azok az eszközök jogosultak, amelyeknél a vírusvédelem központilag biztosított. Elavult, nem frissíthető (pl. műszert vezérlő) operációs rendszerrel működő számítógépet szeparált, zárt hálózatban kell üzemeltetni, internetre csatlakoztatni tilos.

(3) A vírusvédelemre vonatkozó elemi szabályokat és előírásokat valamennyi felhasználó köteles betartani. Amennyiben a felhasználó rosszindulatú szoftver, kártékony kód jelenlétére gyanakszik, akkor a gyanús eszköz vagy rendszer használatát lehetőleg fel kell függesztenie az Egyetem IT Ügyfélszolgálatának egyidejű értesítése mellett.

(4) A felhasználók kötelesek az adathordozón kapott bármilyen állományt a számítógépre telepített vírusvédelmi szoftverrel leellenőrizni. Ahol lehetséges, az ellenőrzést az automatikus beállításokkal kell kikényszeríteni.

(5) A vírusvédelmi rendszer frissítése központilag, felhasználói beavatkozás nélkül történik. A vírusvédelmi ellenőrzések és frissítések időpontját lehetőség szerint úgy kell meghatározni, hogy azzal a felhasználókat ne akadályozzák a feladatuk elvégzésében. Az ellenőrzések eredményeit vírusvédelmi naplókban kell megőrizni és visszakereshetővé kell tenni.

Hozzáférés a rendszerekhez

Jogosultságkezelés

52. § (1) A szükséges jogosultságok beállítása a legkisebb jogosultság elvén alapszik. A jogosultságbeállítás célja, hogy a felhasználói hozzáférés teljes életciklusában biztosítsa, hogy a felhasználó csak azokhoz az informatikai rendszerekhez, azokban tárolt adatokhoz, programokhoz és szolgáltatásokhoz férjen hozzá, mely a munkakörének ellátásához feltétlenül szükségesek. Ennek betartásáért a foglalkoztatott közvetlen munkahelyi vezető felel.

(2) Az informatikai szolgáltatások esetében minden üzemeltető, fejlesztő vagy felhasználó csak a munkaköri leírásában rögzített feladatok ellátásához szükséges, legszűkebb körű jogosultságokkal rendelkezhet.

(3) Az Egyetem informatikai szolgáltatásainak igénybevételéhez az I3 az adott szolgáltatás használatában szerzett jártasságot igazoló vizsga teljesítését írhatja elő. A kritériumok teljesítésének költsége a hozzáférést igénylő szervezeti egységét terheli.

(4) A jogosultsági szintek, valamint a felhasználóknak kiosztott jogosultságok ellenőrzése és azok nyilvántartása az adatgazdák feladata, amelyhez az i3 adatszolgáltatást nyújt.

(5) Minden informatikai szolgáltatás esetében az adatgazdának meg kell határozni a hozzáférésre jogosultak körét és az elérhető jogosultsági szinteket, jogosultsági rendszert.

(6) Minden hozzáférési kísérlet esetén – függetlenül annak szintjétől – a jogosultságot ellenőrizni kell, azaz azonosítást szükséges végezni (pl. számítógépbe vagy alkalmazásba történő bejelentkezés).

(7) Az intézményi adatokhoz történő hozzáférést lehetővé tevő alkalmazások jogosultsági köreit olyan módon kell kialakítani, hogy a foglalkoztatottak csak a munkakörükkel kapcsolatos adatokat láthassák, illetve kezelhessék.

(8) Informatikai szolgáltatásokhoz módosítást és kritikus adatok lekérdezését lehetővé tevő hozzáférésre, kizárólag másik szolgáltatás vagy természetes személy lehet jogosult. Természetes személyek egy csoportja, közös használatú hozzáféréssel kizárólag mindenki számára hozzáférhető adatokhoz, vagy egy szervezeti

egységen belül mindenki számára hozzáférhető adatokhoz történő hozzáféréshez (pl. egységen belüli közös hálózati meghajtó elérése közös használatú számítógépekről) rendelkezhet jogosultsággal.

(9) A jogosultságok nyilvántartását napra készen kell tartani és az adatgazda rendelkezése alapján, de minimum évente felül kell vizsgálni.

(10) Az informatikai szolgáltatások felhasználóinak azonosítása és a jogosultság elbírálása központilag, erre a célra szolgáló központi címtárral kell megvalósítani azért, hogy a felhasználói adatbázis kezelése egységesen és konzisztensen valósuljon meg. Kivételt ez alól csak az i3 igazgató engedélyével, indokolt esetben tehető. Lehetőség van továbbá szerződések alapján létrejött ún. föderációs azonosítási rendszerek (pl. eduID) használatára, azonban ilyen szolgáltatások esetében is az egyetemi felhasználók azonosítását a központi címtár alapján kell megoldani.

(11) A felhasználók egyedi azonosítását, jogosultságigénylés -és kezelés folyamatát dokumentálni kell a Pécsi Tudományegyetem Informatikai Szabályzatában, a kapcsolódó eljárásrendekben foglaltaknak megfelelően.
A munkavállalók esetében a Pécsi Tudományegyetem Informatikai Szabályzatának a Jogosultsági szintek meghatározása, hozzáférés szabályozása pontja tartalmazza a részletes leírást.

(12) Külső partnerek hozzáférését a 7/2017. kancellári utasítás a PTE informatikai rendszereihez a külső partnerek részére biztosított hozzáférések rendjéről szóló utasítás tartalmazza.

(13) Amennyiben a felhasználó felügyelet nélkül hagyja a munkaállomást - akár csak egy rövid időre -, köteles azt zárolni, hogy az információkhoz való jogosulatlan hozzáférést megakadályozza.

Jelszókezelés szabályai

53. § (1) Jelszavak használata az informatikai biztonság egyik meghatározó része. Az informatikai rendszer minden felhasználójának tisztában kell lennie a jelszavak fontosságával és a nem megfelelő jelszókezelés következményeivel. A felhasználói azonosítók és jelszavak átadásának bizalmasan kell történnie.

(2) A felhasználói jelszavak kezelése a felhasználónak kötelessége a jelszó megváltoztatása az alábbi esetekben:
a) a felhasználói fiók létrehozása utáni első belépéskor;
b) az i3 általi új jelszó beállítását követően;
c) amennyiben felmerül a gyanú, hogy a jelszava más tudomására jutott;
d) érvényességi idő lejártakor.

(3) A jelszavakat titokban kell tartani, ennek érdekében:
a) a jelszót tilos másoknak elmondani, a jelszóról mások előtt beszélni;
b) a jelszót se a munkáltatói jogkör gyakorlóinak, közvetlen munkahelyi vezetőknek, se a rendszergazdáknak, adminisztrátoroknak nem szabad elárulni, ha kifejezetten kérik ezt, akkor sem;
c) a felhasználónak tilos más felhasználó jelszavát megkérdeznie és tilos más felhasználó azonosítóját használnia annak belépése után. Hasonlóképpen, a felhasználó nem engedheti meg más felhasználónak az azonosítója használatát és nem engedheti át annak használatát a bejelentkezés után.

(4) A jelszó kiválasztása során:
a) tilos a felhasználó nevet jelszóként használni;
b) tilos titkosítatlan formában tárolni;
c) azonos vagy az abc-ben, a billentyűzeten egymást követő számokból vagy betűkből álló jelszót választani;
d) nem javasolt a programok jelszó megjegyző funkciójának alkalmazása;
e) javasolt olyan jelszavakat választani, melyek nehezen visszafejthetőek, de könnyen megjegyezhetőek, nem személyes adatokon alapulnak (pl. nem tartalmaz telefonszámot, gyermek nevét, születési dátumot, kedvenc háziállat nevét, cégnevet, rendszámot stb.) és nem szótári szó;

f) a jelszavaknak minimálisan 8 karakter hosszúnak kell lenniük és tartalmazniuk kell minimum 3 karaktertípust az alábbiakból: nagybetűk, kisbetűk, számok;
g) Jelszóváltoztatáskor a felhasználó nem használhatja az utolsó 12 jelszavát.

(5) A jelszószabályok betartása minden felhasználónak jól felfogott érdeke. A felhasználó felelőssége, ha neki felróható mulasztása miatt a jelszava megismerése révén valaki visszaélést követ el.

(6) Hibás jelszóval történő bejelentkezési kísérletek száma rendszerenként eltérő. Ilyen esetekben a felhasználó fiókja zárolásra kerül és az Egyetem IT Ügyfélszolgálata automatikusan értesítést kap.

A felhasználói jogosultságok felülvizsgálata

54. § (1) Az adatgazdáknak rendszeresen, de legalább évente egyszer felül kell vizsgálniuk a felhasználói hozzáférési jogosultságokat.

(2) A jogosultságok változásait dokumentált, visszakereshető formában szükséges nyilvántartani, függetlenül attól, hogy kiadásról, érvényesítésről vagy visszavonásról van szó.

Távoli elérés

55. § (1) A VPN alkalmazásának célja az Egyetem dolgozói és a harmadik felek számára a biztonságos távmunka lehetőségének kialakítása. Az Egyetem által biztosított VPN rendszert csak munkavégzés céljából, a felhasználó feladatkörében foglalt tevékenységek elvégzése során lehet használni.

(2) A felhasználók az Egyetem hálózatához távolról kizárólag VPN alkalmazás használatával kapcsolódhatnak. A távoli elérés létesítése kiemelt információbiztonsági kockázatot jelent, melyre az ezt biztosító jogok és az üzemeltetés teljes időszaka alatt figyelemmel kell lenni. A VPN segítségével csatlakoztatott eszközök fokozott védelme, karbantartása, vírusvédelme, az illetéktelen hozzáférés megakadályozása a felhasználó kötelessége.

(3) Az i3 Infrastruktúra Szolgáltatási Főosztály munkatársa felelős a VPN kapcsolatok szabályos beállításáért, az adott szervezeti egység vezetője felelős a VPN igénylés jóváhagyásáért.

(4) A felhasználó köteles a távoli munkavégzésre előírt szabályokat teljeskörűen betartani. A távoli munkavégzés és home office részleteit a HR Kézikönyv tartalmazza.

(5) A VPN kapcsolat kizárólag személyi tűzfal és vírusvédelmi szoftver használata mellett engedélyezett.

(6) A VPN hozzáférésre vonatkozó igényt a https://sm.pte.hu oldalon keresztül elérhető online formanyomtatványon kell bejelenteni.

Hálózat biztonság

56. § (1) Az egyetemi hálózat használata során mindenki köteles betartani és magára nézve kötelezőnek elfogadni a vonatkozó hatályos kancellári utasításban megfogalmazottakat (UPNET AUP).

(2) Az Internethez történő hozzáférés esetén a felhasználó köteles az Egyetem internet-szolgáltatójának (Kormányzati Informatikai Fejlesztési Ügynökség) szabályzatát betartani.

(3) Az egyetemi hálózathoz való hozzáférés csak megfelelő azonosítás esetén lehetséges.

(4) Az egyetemi hálózathoz való hozzáféréseket az adatbiztonsági követelmények biztosítása, valamint minőségbiztosítási okokból naplózni szükséges (fizikai cím, IP cím, felhasználónév hozzárendeléseket).
(5) A naplózott adatokat 6 hónapig meg kell őrizni, utána meg kell semmisíteni.

(6) A további, szolgáltatás-specifikus naplózási intézkedéseket a szolgáltatás leírások tartalmazzák. A naplózási intézkedések során figyelembe kell venni az adatbiztonsági követelmények teljesítését.

(7) Személyes adatokat tartalmazó naplóbejegyzések rögzítése kizárólag legitim adatkezelési cél érdekében, megfelelő adatkezelési jogalappal, és a további adatvédelmi szabályok betartása mellett jogszerű. A személyes adatokat tartalmazó naplózás során az Informatikai Szabályzat 12-13. §-ait megfelelően alkalmazni kell.

(8) Személyes adatok, különösen betegadatok, hallgatói, tanulmányi adatok, bér és munkaügyi adatok, továbbá a gazdálkodási, valamint a kutatási adatok továbbítása informatikai hálózaton kizárólag megfelelő titkosítás mellett végezhető.

(9) Az informatikai szolgáltatások biztonságos távoli, nem egyetemi hálózatból történő elérését hitelesített, vég-vég titkosított VPN-en, vagy más titkosított, a két végpont között racionális időn belül vissza nem fejthető csatornán (pl. HTTPS) keresztül kell biztosítani.

(10) Egyetem informatikai rendszereinek biztonsága érdekében a hálózatot egymástól jól elkülöníthető logikai tartományokba kell osztani. Az egyes tartományok közti adatforgalmat tűzfal alkalmazásával szűrni kell. A hálózatok menedzselését és felügyeletét az I3 Infrastruktúra Szolgáltatási Főosztály Hálózatüzemeltetési Csoportja lát el.

(11) A rendszert a túlterheléses (szolgáltatás megtagadás jellegű) támadásokkal szembeni védelemmel kell ellátni, amely elhárítja, vagy korlátozza azok kihatásait.

Biztonsági mentés, archiválás

57. § (1) Az Egyetem kezelésében, használatában lévő, elektronikus formában tárolt információkról rendszeres, meghatározott időközönként és indokolt esetben soron kívüli biztonsági mentéseket kell készíteni.

(2) A rendszerekben kezelt, feldolgozott, tárolt adatállományokat, amennyiben azok elérése a felhasználók számára napi munkavégzésük során már nem szükséges, azonban őrzésük indokolt, archiválni kell. Az őrzési idő elteltével a törlésükről gondoskodni szükséges.

(3) A részletes mentési, archiválási és visszatöltési rendszer leírását, az üzemeltetés kapcsán felmerülő feladatokat, illetve azok felelőseit a Pécsi Tudományegyetem mentésekre vonatkozó eljárásrendje(i) tartalmazza.

(4) Minden informatikai szolgáltatás az Informatikai Szabályzat 1. számú mellékletében meghatározott adatlapjának tartalmaznia kell az adott szolgáltatásra vonatkozó mentési és archiválási rendet (minimálisan meghatározva a mentendő adatok körét, a mentés módját és gyakoriságát, a mentések tárolási rendjét, megőrzési idejét és példányszámát).

(5) Az elvárásoknak megfelelő mentési módszerek technológiai kidolgozása az i3 üzemeltetésért felelős vezetőjének a feladata.

(6) A mentési és archiválási rend betartásához szükséges erőforrások (hardver, szoftver, humán) biztosítása a Kancellár feladata.

(7) Az adatgazda döntése alapján a telephelyen kívüli tárolású (offsite) mentésekkel is kell rendelkezni.

(8) A mentési rendnek az alkalmazásra vonatkozó részét úgy kell megállapítani, hogy a szolgáltatás működőképessége tetszőleges komponens meghibásodása vagy adatvesztése esetén is helyreállítható legyen.

(9) A szolgáltatások konfigurációs beállításait minden változás esetén, de minimum hetente kell menteni. A mentési eljárásnak lehetővé kell tennie egy adott állapot célirányos betöltését. A konfigurációs mentéseknek 10 előző állapotra, illetve minimum az előző 30 szolgáltatási napra ki kell terjedniük.

(10) A mentési eljárásnak lehetővé kell tennie az adatok tesztrendszerbe történő betöltését.

(11) Az adatok mentését minden esetben – lehetőség szerint éjszaka – úgy kell elvégezni, hogy az a lehető legkisebb módon befolyásolja az adott szolgáltatás használatát.

(12) Minden szolgáltatás esetében évente minimum egy alkalommal visszatöltési gyakorlatot, tesztet szükséges végezni, amely a mentések felhasználhatóságát ellenőrzi. A visszatöltési gyakorlat az éles szolgáltatással funkcionálisan egyező tesztrendszeren is teljesíthető.

(13) A mentések elkészítéséért, meglétéért és a visszatölthetőségéért az adott szolgáltatást üzemeltető személyzet a felelős.

(14) Új szolgáltatások bevezetésénél figyelembe kell venni a mentéshez szükséges tárhely kapacitás rendelkezésre állására.

(15) Amennyiben a technológia és a rendelkezésre álló erőforrások lehetővé teszik, úgy a mentéseket titkosítva szükséges tárolni.

Biztonsági mentések adathordozóinak kezelése

58. § (1) Az informatikai szolgáltatások adatállományainak mentései intézményi és személyes adatokat tartalmazhatnak, ezért ezen adathordozók biztonságát biztosítani szükséges.

(2) A biztonsági mentéseket tartalmazó adathordozók kizárólag zárható, tűzálló páncélszekrényben tárolhatóak. A páncélszekrényeknek minden esetben zárt állapotban kell lenniük, amikor nem történik adathordozó mozgatás.

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

(4) A mentések adathordozóinak használatból történő kivonása után azokat meg kell semmisíteni, a megsemmisítésről jegyzőkönyvet kell felvenni.

Naplózás és monitoring

Naplózás általános szabályai

59. § (1) A naplózási architektúrát úgy kell kialakítani, hogy a különböző rendszerek naplóállományainak egységes értelmezhetősége biztosított legyen. A naplózási architektúra kialakítása Infrastruktúra Szolgáltatási Főosztály vezetőjének felelőssége.

(2) A rendszergazdák felelnek az egyes rendszerekben a naplózási beállítások naprakészen tartásáért.

(3) A naplóállományokhoz való hozzáférési jogosultságokat az i3 igazgató hagyja jóvá, az Információbiztonsági Felelős ellenőrzi, nyilvántartását az i3 végzi.

Naplózandó események

60. § (1) Az Egyetem informatikai rendszerében automatikus naplót kell vezetnie az informatikai rendszer biztonsági szempontból lényeges tevékenységéről.

(2) A naplózásnak ki kell terjednie:
a) a jelen Szabályzatban meghatározott eseményekre,
b) az arra felhatalmazással rendelkezők által meghatározott, ideiglenesen naplózandó eseményekre.

(3) Ideiglenes naplózást rendelhet el a naplózandó esemény és a naplózás időtartamának és céljának pontos megjelölésével, írásban:
a) az Adatgazda,
b) az i3 igazgató,
c) az Információbiztonsági Felelős,
d) a szakterületi vezető (igazgató, osztályvezető).

(4) A naplózandó események körét az i3 igazgató határozza meg, melyről tájékoztatja az Információbiztonsági Felelőst.

(5) A naplózandó események áttekintése része az Szabályzat rendszeres felülvizsgálatának.

(6) Az Információbiztonsági Felelős meghatározott időközönként ellenőrzi, hogy az egyes rendszerek naplózási beállításai megfelelnek-e a naplózási események nyilvántartásának.

Eseménynaplók tárolása

61. § (1) Bármilyen biztonsági esemény bekövetkezése esetén az eseménynaplók tartalmazzák azokat az információkat, melyek az utólagos vizsgálatok végrehajtásához szükségesek, ezért az eseménynaplók tárolásának minimum szabályai az alábbiak:
a) a naplóadatoknak sértetlenül rendelkezésre kell állniuk az elévülési időn belül;
b) az éles környezetben minimum a teljes mentések közötti időtartamnak megfelelő naplóállományokat kell tárolni;
c) biztosítani kell, hogy az adatokban keletkezésük után változtatást már ne lehessen végrehajtani;
d) az információk bizalmasságára tekintettel, az adatok nem juthatnak illetéktelenek kezébe.

(2) Biztonsági események, illetve incidensek kivizsgálása esetén az érintett rendszer (ügyviteli és technológiai egyaránt) üzemeltetőjének (legyen az az informatikai szolgáltató, a helyi üzemeltetés, vagy külső szállító) kötelessége átadni, betekintést biztosítani a kapcsolódó naplóállományokba a vizsgálatot koordináló Információbiztonsági Felelősnek.

(3) A naplózás során keletkező állományokat korlátozott hozzáféréssel, a bennük megjelenő adattartalom minősítése szerint kell kezelni, és a megjelenő adattartalom szerinti meghatározott ideig, központilag szükséges tárolni.

Rendszergazdák vagy más biztonsági szereplők által okozott biztonsági esemény kezelése

62. § A rendszergazda által okozott biztonsági esemény vagy annak gyanúja esetén az eszkalációs eljárás megegyezik az általános biztonsági esemény kezelési eljárással, azonban ilyen esetben tilos a rendszergazda tájékoztatása, míg az i3 igazgatóját és az Információbiztonsági Felelőst haladéktalanul értesíteni szükséges.

Monitorozás

63. § (1) Informatikai rendszerek esetében az alábbi esetekre szükséges azonnali riasztás beállítása:
a) szerverszoba fizikai biztonságának sérülése (illetéktelen behatolás, tűz, túlmelegedés, vízbeömlés stb.);
b) jogosulatlan hozzáférési kísérlet;
c) teljesítmény-problémák;
d) egyéb anomáliák.

(2) A monitorozott eszközökről és felhasználókról az IT infrastruktúra monitorozó rendszer üzemeltetőjének naprakész nyilvántartással kell rendelkeznie, melybe kérésre betekintési lehetőséget kell biztosítania az Információbiztonsági Felelősnek az üzemeltető felügyelete mellett.

(3) A monitorozás során keletkező állományokat korlátozott hozzáféréssel, a bennük megjelenő adattartalom információbiztonsági osztályozása szerint kell kezelni, és a megjelenő adattartalom szerinti meghatározott ideig szükséges tárolni, illetve a keletkezett fájlok esetében a jelen fejezetben foglaltak szerint kell eljárni.

Órajelek szinkronizálása

64. § Az Egyetemen belül, illetve adott biztonsági tartományban működő valamennyi érintett információ-feldolgozó rendszer órajelét szinkronizálni kell egy közösen megállapított pontos időforráshoz. A naplóbejegyzések időbélyegeinek előállításához ezt az órajelet kell használni.

Az informatikai szolgáltatások biztonsága

Elektronikus kommunikáció

65. § (1) A jelen Szabályzat az elektronikus kommunikáció alábbi, az Egyetemen belül elérhető eszközeire vonatkozóan tartalmaz előírásokat:

a) elektronikus levelezés;
b) internet;
c) webszolgáltatás;
d) PTE O365 szolgáltatás által biztosított kommunikációs csatornák.

(2) Ezen alkalmazások használata kizárólag a jogi követelményeknek megfelelően, az Egyetem előírásait és korlátozásait betartva, biztonsági, illetve hálózat menedzsment célú monitoring megvalósulása mellett megengedett az alábbiakban foglaltak szerint.

Elektronikus levelezés

66. § (1) Az elektronikus levelezési szolgáltatást az egyetemi tevékenységgel összefüggő ellátásának érdekében biztosítja az Egyetem. Az elektronikus levelezésre vonatkozó jogosultság az elektronikus levelezésre vonatkozó biztonsági szabályok megismerése után adható meg.

(2) Az elektronikus levelezésben lévő információkat védeni kell az alábbi módon:

a) biztosítani kell a pontos címzést és célba juttatást;
b) védeni kell az üzeneteket a jogosulatlan hozzáféréstől, módosítástól;
c) biztosítani kell a szolgáltatás megbízhatóságát és hozzáférhetőségét;
d) elektronikus aláírások használatát az arra feljogosítottaknak biztosítani kell;
e) azok a felhasználók használhatják az elektronikus levelezést, akik rendelkeznek az ehhez szükséges jogosultsággal.

Az elektronikus levelezés szabályai

67. § (1) Az e-mail címek lehetnek személyhez, szervezethez vagy egyéb csoporthoz (pl. projekt) rendelve.

(2) Az Egyetem Hálózatán biztosított levelezés a munkavégzést, az egyetemi célokat hivatott szolgálni, éppen ezért elsősorban az Egyetemen történő oktatással, kutatással, társadalmi élettel, munkaköri feladatokkal kapcsolatos feladatok felelősségteljes végzése támogatott.

(3) Egyetemi e-mail cím az egyetemi tevékenységgel összefüggésben használható, az alábbi alapvetésekre figyelemmel:

a) minden egyetemi felhasználó egyedi e-mail címet kap, azt kizárólag a felhasználó saját maga veheti igénybe;
b) a felhasználó saját azonosítójának és jelszavának átadása más felhasználó részére tilos;
c) a munkahelyi e-mail címmel magánjellegű regisztrációt tenni különböző szabadon hozzáférhető, nem a munkavégzés céljával összeegyeztethető weboldalakon tilos;
d) a felhasználó elektronikus levelezésébe incidens megalapozott gyanúja esetén az Információbiztonsági Felelős az i3 igazgató engedélye birtokában betekintést nyerhet az informatikai és biztonsági szolgáltatókkal együttműködve;

e) az elektronikus üzenetek bizalmasságának, illetve hitelességének, letagadhatatlanságának védelme érdekében – az adatok biztonsági osztályba sorolásának megfelelően – digitális aláírást és titkosítást kell alkalmazni;
f) az Egyetem levelezési rendszeréből a szervezeten kívülre csak olyan információkat lehet kijuttatni, amelyek kijuttatására a felhasználó más csatornán keresztül is jogosult.
g) az elektronikus levél mérete, a hozzá csatolható állománnyal együtt nem haladhatja meg a mindenkori szolgáltató által meghatározott korlátot, az ennél nagyobb levelek nem kerülnek elküldésre.

(4) Az e-mailek küldésére vonatkozó főbb előírások az alábbiak:
a) a feladó felelős az általa küldött e-mail tartalmáért információbiztonsági szempontból is;
b) más felhasználó nevében e-mailt küldeni tilos, kivéve a rendszerbeli meghatalmazási eljárás alkalmazásán keresztül (pl. asszisztens);
c) a rendszer a törölt elemeket meghatározott napig tárolja, utána véglegesen törlődnek a levelező rendszerből;
d) a leveleket mindig célzottan kell kiküldeni, a címzettek számosságára és megjelenítésére vonatkozó korlátozások figyelembevételével (egy levélben a címzettek száma nem haladhatja meg a maximálisan megengedett darabot);
e) automatikus válaszüzenetek tartalmát minden esetben úgy kell meghatározni, hogy a benne megadott információkkal rosszindulatú fél ne tudjon visszaélni;
f) az Egyetem levelezőrendszerében tiltott a lánclevelezés, a kéretlen levelek (spam), valamint az indokolatlan mértékű magáncélú tartalmak küldése. (A vizsgálat során biztosítani kell, hogy csak és kizárólag a biztonsági eseményhez kapcsolódó levelek kerüljenek vizsgálat alá.);
g) az elektronikus levelezési rendszerbe beérkező leveleket minden esetben ellenőrizni kell, hogy nem tartalmaznak-e valamilyen, az Egyetem informatikai rendszerét veszélyeztető programot, kódrészletet, scriptet;
h) a címinformáció hamisítása vagy a fejléc egyéb módon történő módosítása a feladó vagy a címzett személyazonosságának elrejtésére;
i) vírusos levelek szándékos küldése;
j) üzleti szempontból titkos, bizalmas, illetve belső információk jogosulatlan nyilvánosságra hozatala;
k) minden ismeretlen kiterjesztésű e-mailhez csatolt állomány megnyitása;
l) ismeretlen feladótól származó nem üzleti célú levelekben található csatolmány megnyitása;
m) kéretlen levelek küldése, továbbítása;
n) valótlan információt hordozó levelek tudatos továbbítása;
o) az elküldött levél járulékos adatainak (pl. feladó e-mail címe, küldés időpontja) meghamisítása;
p) munkahelyi postafiók tartalom automatikus továbbítása külső e-mail címre;
q) privát postafiók tartalom automatikus továbbítása munkahelyi e-mail címre;
r) az Egyetem elektronikus levelezési címjegyzékének kiadása harmadik fél számára.

(5) Az e-mailek fogadására vonatkozó főbb irányelvek az alábbiak:
a) Bizalmas információk továbbítását kérő elektronikus levelek esetében mindig meg kell győződni az információkérés hitelességéről;
b) ismeretlen, gyanús feladótól érkezett csatolmányok, linkek megnyitása tilos. Kérdéses tartalmak megnyitása esetén a felhasználónak Egyetem IT Ügyfélszolgálatához kell fordulnia;
c) téves címzés miatt kapott e-mailt, annak felismerése után a felhasználónak haladéktalanul jeleznie kell a feladó felé, és a levél tartalmának olvasása nélkül törölni kell. Az abban lévő tartalmak, információk, adatok jogtalan megismerése és kezelése tilos.

Levélszűrés (spamkezelés)

68. § (1) Az elektronikus levelezés biztonságának megteremtését kéretlen levél (spam) szűrő rendszer alkalmazásával, valamint vírusvédelmi rendszer használatával kell biztosítani, melyet rendszeresen frissíteni kell.

(2) A levelek kéretlennek (spam) minősítését a kéretlen levélszűrő rendszer alkalmazásával kell elvégezni. A nem gyanús leveleket változatlanul továbbítani kell a címzett számára. A rendszer által spamnek minősülő

levelet karanténba kell helyezni, a visszatartott levélről a címzettet tájékoztatni kell. A címzett a levelet a karanténban megtekintheti, kezelheti az i3 Infrastruktúra Szolgáltatási Főosztály (karbantartás, törlés, saját e-mail címére továbbítás). A karanténban található kéretlen levelet a rendszernek a beérkezéstől számított egy hónap múlva automatikusan törölnie kell.

(3) Csatolmányok visszaállítása: az elektronikus levelek csatolmányait információbiztonsági és vírusvédelmi szempontból szűri a levelezőrendszer. Azok visszaállítását az Egyetem IT Ügyfélszolgálatának továbbított levélben lehet kérni, a prioritás megjelölésével.

Hírlevelek kezelése

69. § Az Egyetem infrastruktúráját használó hírlevelek kiküldésnek szabályait a Pécsi Tudományegyetem infrastruktúráját használó hírlevelek kiküldésnek szabályait az egyetem informatikai infrastruktúráján, az egyetemi levelezőrendszeren keresztül kiküldendő egyetemi hírlevelek előkészítésének és jóváhagyásának szabályairól című utasítás tartalmazza.

Internethasználat

70. § (1) A megbízható (egyetemi hálózat) és a nem megbízható (pl.: internet) hálózatokat csak az Egyetem tűzfalán keresztül lehet összekapcsolni. Az Egyetem rendszerében a felhasználóknak az internet használat során törekedni kell, hogy az ügyviteli folyamatok támogatására, illetve azokhoz kötődő információáramlásra használják.

(2) Az internet használata során az Egyetem fenntartja a jogot arra, hogy a felhasználók internet-forgalmát a személyes adatok védelmére vonatkozó szabályok betartásával naplózza, illetve ellenőrizze.

(3) Tiltott tevékenységek az internet használat során:

a) minden olyan tevékenység, ami a hatályos jogszabályokba ütközik, különös tekintettel az alábbiakra:
   - mások személyiségi jogainak megsértése;
   - tiltott haszonszerzésre irányuló tevékenység (pl. piramis-, pilótajáték);
   - a szerzői jogok megsértése;
   - szoftver szándékos és tudatos illegális terjesztése;
b) a hálózat erőforrásaihoz, a hálózaton elérhető adatokhoz történő illetéktelen hozzáférés, azok illetéktelen használata, módosítása, megrongálása, megsemmisítésére irányuló tevékenység;
c) a hálózat biztonságos működését zavaró vagy veszélyeztető információk, programok terjesztése (pl. vírusok, trójai programok, hacker eszközök, férgek);
d) hálózati forgalom lehallgatása, megfigyelése, kivéve, ha ez az adott munkakörhöz kapcsolódik;
e) az internetről a legálisan hozzáférhető programok letöltése, kivéve, ha arra vezetői engedély vonatkozik;
f) a szolgáltatások blokkolását, lassítását célzó támadás, az azonosítási, illetve biztonsági intézkedések megsértésére irányuló kísérlet, valamint az egyéb azonosítóhoz, számítógéphez vagy hálózathoz történő illetéktelen hozzáférési kísérlet;
g) a felhasználói azonosítóval csak annak tulajdonosa jelentkezhet be. Az adatokhoz történő hozzáférés érdekében választott jelszó titkosságának megőrzése a felhasználó felelőssége. Egy adott azonosítóról folytatott tevékenységért mindig annak tulajdonosa felel, az azonosító kölcsönadása nem megengedett, így felelősségre vonás esetén ez az indok nem elfogadható;
h) minden felhasználó látogatására jogosult, ezért tilos továbbá:
   - sértő, társadalomra veszélyes, jó erkölcsbe ütköző szöveg, kép, ábra vagy egyéb formájú információ publikálása, letöltése;
   - az interneten elérhető szolgáltatást, bármilyen törvényt, szabályozást, szabványt, nemzetközi egyezményt vagy díjszabást sértő módon használni;
   - bármelyik számítógép-hálózat biztonságát rombolni, illetve gyengíteni, más felhasználó jogosultságát jogosulatlanul használni
   - bármilyen internetes végpontra, illetve hálózati eszközre jogosulatlanul csatlakozni, vagy ezzel próbálkozni;

- bármely végpont működését megzavarni vagy azt az Egyetem hálózatáról, vagy annak igénybevételével szándékos túlterhelni (DOS támadás);
- egyetemi tulajdonú eszközöket internetes számítógép erőforrás megosztásokhoz használni;
- a hálózatot a szerzői jogvédelem alá eső anyagok átvitelére használni (még közvetetten is), ha az átvitel során mások szerzői joga sérül;
- tilos kikapcsolni a munkaállomásra telepített biztonsági szoftvereket, eszközöket;

i) nem látogathatóak olyan oldalak, melyek megtekintése vagy használata a hivatalos egyetemi tevékenységgel össze nem egyeztethető:
- az Egyetem érdekeit sértik;
- rasszista tartalmúak;
- erotikus oldalak;
- kalóz oldalak;
- terrorizmust támogató oldalak;
- fegyverekre vonatkozó információkat tartalmaznak;
- illegális kábítószerekre vonatkozó információkat tartalmaznak;
- phishing (adathalász) oldalak;
- internetes fogadási oldalak, szerencsejáték oldalak;

j) az i3 informatikai üzemeltető személyzete által kialakított megoldásokon kívül tilos irodai munkaállomásokon külső frissítő szerverről való frissítés (pl. operációs rendszer-, vírusvédelmi rendszer-, alkalmazás-frissítések).

(4) A fentiekben meghatározott tiltott tevékenységeket végezni az i3 előzetes engedélyével lehetséges, amennyiben oktatási-kutatási tevékenység ellátásához kapcsolódik.

Fájlkezelés/címtárkezelés

71. § (1) A fájlok kezelése során törekedni kell, hogy a tároló rendszerben az adott fájlnak minél kevesebb példánya tárolódjon.

(2) Nyilvános mappában tilos elhelyezni kritikus adatot tartalmazó dokumentumot.

(3) A felhasználóknak tilos megosztani az egyéni mappájukat, illetve a saját helyi tárolójuk bármely mappáját. Az olyan fájlok megosztása, amelyek nem az egyetemi folyamatokkal vannak összefüggésben, az egyetemi közös tárterületeken nem lehetséges.

(4) A szervezeti és az egyéni mappákban magánjellegű fájlok tárolása nem megengedett.

(5) A munkaállomás helyi adathordozóján tárolt adatok teljeskörűen nem kerülnek központilag mentésre. Részleges mentés a PTE O365 szolgáltatás keretében nyújtott OneDrive megoldással biztosított. A OneDrive-on kívül állományok mentéséről a felhasználónak kell gondoskodnia.

Webszolgáltatás

72. § (1) Az egyetemi központi honlapok (pl. www.pte.hu) tartalmáért és módosításáért a Rektori Kabinet Kapcsolati Igazgatóság, karbantartásáért i3 Alkalmazás Szolgáltatási Főosztály felelőse. A központi portálrendszerben lévő egyéb egyetemi szervezeti egységek honlapjainak tartalmáért és módosításáért az adott szervezeti egységek vezetői, karbantartásáért i3 Alkalmazás Szolgáltatási Főosztály felelőse. Az egyéb nem központi üzemeltetésű honlapok tartalmáért, módosításáért, kezeléséért és karbantartásáért a létrehozó szervezeti egység vezetője a felelős. A honlapokon kizárólag nyilvános, közérdekű információ jeleníthető meg.

(2) Az egyes egyetemi szervezetekre vonatkozó információkért az adott szervezet a felelős.

(3) Az i3 felel a portál elérhetőségéért, az informatikai szolgáltatások rendelkezésre állásáért. A portál speciális információinak naprakészen tartása az adott terület tartalomfelelősének a feladata. A honlap igénylésével kapcsolatos előírások az i3 honlapján találhatók.

PTE O365 szolgáltatás által biztosított kommunikációs csatornák

73. § Az Egyetemen a PTE O365 szolgáltatás keretében elérhető kommunikációs csatornák (pl. Teams, melyen keresztül csevegőszolgáltatás és videókonferencia is elérhető további beépített szolgáltatások mellett) használatára az e-mailekre vonatkozó általános alapelvek az érvényesek.

Kriptográfiai eszközök használata

74. § Az Egyetem az általa kezelt bizalmas és annál magasabb biztonsági besorolású adatok tárolása és továbbítása során kriptográfiai eszközöket alkalmaz annak érdekben, hogy csökkentse az érintett adatok sérülésének kockázatát és megőrizze azok bizalmasságát

Titkosítás

75. § (1) A titkosítás alkalmazása nem kötelező a kizárólag közérdekű és a közérdekből nyilvános adatok esetében. Bizalmas, illetve titkos adatok továbbítása informatikai hálózaton kizárólag megfelelő titkosítás mellett végezhető. Amennyiben a titkosítás aránytalanul nagy teherrel járna vagy lehetetlen, abban az esetben kockázatcsökkentő intézkedésekről kell gondoskodni.

(2) A titkosítás végrehajtásáért a rendszert üzemeltető vagy adatot tartalmazó eszköz esetében az adatgazda vagy az adatot szállító személy felel.

Elektronikus aláírás

76. § A hatályos jogszabályoknak megfelelő esetekben elektronikus aláírás is alkalmazható. Ezeket az adott rendszerek dokumentációi határozzák meg.

Hitelesítés

77. § Az elektronikus aláírással kapcsolatban csak a Nemzeti Média- és Hírközlési Hatóság elektronikus aláírással kapcsolatos nyilvántartásában szereplő hitelesítésszolgáltatók által kibocsátott tanúsítványokat fogadhatják el az elektronikus információs rendszerek az érintett szervezeten kívüli felhasználók hitelesítéséhez.

6. fejezet Záró és hatályba lépő rendelkezések

78. § Jelen Szabályzat a 2022. július 1. napján lép hatályba. Jelen Szabályzat hatályba lépésével egyidejűleg hatályát veszíti a Pécsi Tudományegyetem – 2010. január 1. napján hatályba lépett – Információbiztonsági politikája.

79. § (1) Jelen Szabályzat a kapcsolódó szabályzatokkal, utasításokkal együtt érvényes. A jelen Szabályzatban nem szabályozott kérdésekben a mindenkor hatályos jogszabályokat, illetve belső rendelkezéseket kell érvényesíteni.

(2) A Szenátus felhatalmazza az Egyetem kancellárját, hogy a Szabályzat mellékleteit saját hatáskörben módosítsa.

(3) Szenátus felhatalmazza az Egyetem kancellárját, hogy jelen Szabályzat keretei között az információbiztonság zárt, teljes körű, folytonos és a kockázatokkal arányos védelmének biztosítása érdekében a részletszabályokat, kapcsolódó eljárásrendeket, (így különösen: a biztonsági események bejelentésére, kezelésére vonatkozó eljárásrendet, az adatgazdai tevékenységre vonatkozó eljárásrendet, a foglalkoztatott munkavégzésre irányuló jogviszonyának létesítése, megszűnése, valamint munkakörváltozása esetén érvényes eljárásrendeket) kancellári utasítás keretében határozza meg legkésőbb 2023. június 30. napjáig.

Pécs, 2022. június 23.

Dr. Miseta Attila s.k. rektor	Decsi István s.k. kancellár

Záradék:
A Szabályzatot a Szenátus 2022. június 23. napján tartott ülésén 78/2022. (06.23.) számú határozatával fogadta el.

PTE Informatikai Biztonsági Szabályzat 1. számú melléklet

Fogalomtár

Adat: az információ megjelenési formája, azaz a tények, elképzelések nem értelmezett, de értelmezhető közlési formája.

Adatbiztonság: az adatok jogosulatlan megszerzése, módosítása és tönkretétele elleni műszaki és szervezési intézkedések és eljárások együttes rendszere.

Adatbiztonság megsértése: az a cselekmény vagy mulasztás, amely ellentétben áll az adat védelmére vonatkozó biztonsági szabályokkal és amelynek következményei az adatot veszélyeztetik.

Adathordozó: az adat tárolására és terjesztésére alkalmas eszköz.

Adatkezelés: a személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés.

Adatgazda: annak a szervezeti egységnek a vezetője, ahová jogszabály, közjogi szervezetszabályozó eszköz, egyetemi szabályzat vagy utasítás az adat kezelését rendeli, illetve ahol az adat keletkezik.

Adatvédelem: az adatok kezelésével kapcsolatos törvényi szintű jogi szabályozás formája, amely az adatok előre meghatározott csoportjára vonatkozó adatkezelés során érintett személyek jogi védelmére és a kezelés során felmerülő eljárások jogszerűségére vonatkozik.

Adminisztratív védelem: szervezési és szabályozási úton megvalósított védelem.

Auditálás: előírások teljesítésére vonatkozó megfelelőségi vizsgálat, ellenőrzés.

Backup rendszer: az informatikai biztonság megvalósítása során az adatok rendelkezésre állását lehetővé tevő rendszer és programmásolatokat őrző rendszer.

Bizalmasság: Az Ibtv. szerint a bizalmasság az elektronikus információs rendszer azon tulajdonsága, hogy a benne tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról.

Biztonság: olyan szervezeti állapot, melyben az Egyetemnek a lehető legkisebb veszélyekkel kell számolnia, szolgáltatásait a vállalt és előírt feltételekkel és korlátozások nélkül képes nyújtani, a feladatait, funkcióinak ellátását illetően érdemi hatást gyakorló veszteség nem éri, a lehetséges fenyegetettségek bekövetkezési valószínűségéből és a lehetséges kárértékekből származtatott kockázat a szervezet számára elfogadhatóan alacsony és a kockázatkezelési eljárások eredményeként kialakuló maradvány kockázat a szervezet számára az elviselhető tartományban marad. A védeni kívánt informatikai rendszer olyan, az Egyetem számára kielégítő mértékű állapota, amely zárt, teljes körű, folytonos és a kockázatokkal arányos védelmet valósít meg. A biztonság az informatikai rendszerekben olyan előírások és szabványok betartását jelenti, amelyek a rendszer működőképességét, az információk rendelkezésre állását, sértetlenségét, bizalmasságát és hitelességét erősítik.

Biztonsági követelmények: a kockázatelemzés eredményeként megállapított, elfogadhatatlanul magas kockázattal rendelkező fenyegető tényezők ellen irányuló biztonsági szükségletek együttese.

Biztonsági esemény: az Ibtv. szerint a nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat, amely az elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, és amelynek hatására az elektronikus információs rendszer által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül.

Biztonsági esemény bejelentő csatorna: A biztonsági esemény bejelentésére szolgáló elektronikus levélcím, amelyen a biztonsági eseményt észlelőnek haladéktalanul jelenteni kell a biztonsági eseményt. A biztonsági

esemény bejelentő csatorna az Egyetemen az i3 által a honlapján közzétett elektronikus cím, jelenleg: sd@pte.hu

Biztonsági osztályba sorolás: az Ibtv. szerint a kockázatok alapján az elektronikus információs rendszer védelme elvárt erősségének meghatározása.

Biztonsági rendszer: a biztonsági rendszer az információbiztonsági rendszerek összessége (logikai védelmet valósít meg, pl.: tűzfal, vírusvédelmi rendszer, jogosultág-nyilvántartó rendszer, stb.).

Biztonsági szintbe sorolás: az Ibtv. szerint a szervezet felkészültségének meghatározása az e törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok kezelésére;

Biztonságos törlés: olyan eljárás, ahol a törlést végző munkatárs nemcsak törli, hanem a számítógépén lévő Lomtárból, levelező rendszer esetén a Törölt elemek könyvtárból is törli az adatállományokat. A biztonsági törlés egy fajtája a visszaállíthatatlan törlés, amit minden esetben csak megfelelő szoftver, hardver, vagy fizikai megsemmisítő által az informatikai szolgáltató végezhet.

Egyenszilárdság: a biztonság és a biztonsági szabályzat az intézmény egészét, annak valamennyi tevékenységét teljesen átfogja, és annak minden pontján azonos erősségű.

Elektronikus aláírás (digitális aláírás): az informatikai rendszerben kezelt adathoz rendelt, kódolással előállított olyan jelsorozat, amely az adat hitelességének és sértetlenségének, valamint letagadhatatlanságának bizonyítására használható.

Elektronikus információs rendszer: az Ibtv. szerint a) az elektronikus hírközlésről szóló törvény szerinti elektronikus hírközlő hálózat; b) minden olyan eszköz vagy egymással összekapcsolt vagy kapcsolatban álló eszközök csoportja, amelyek közül egy vagy több valamely program alapján digitális adatok automatizált kezelését végzi; vagy c) az a) és b) pontban szereplő elemek által működésük, használatuk, védelmük és karbantartásuk céljából tárolt, kezelt, visszakeresett vagy továbbított digitális adatok.

Elektronikus információs rendszer biztonsága: az Ibtv. szerint az elektronikus információs rendszer olyan állapota, amelyben annak védelme az elektronikus információs rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos

Elszámoltathatóság: azon követelmény, amely meghatározza minden, az információval vagy az informatikai rendszerrel kapcsolatos tevékenység egyértelmű azonosíthatóságát, utólagos visszakövethetőségét és az adott tevékenységet végrehajtó személyt.

Érintett: bármely meghatározott, személyes adat alapján azonosított vagy – közvetlenül, vagy közvetve – azonosítható természetes személy.

ETR: a Neptun rendszer bevezetését megelőzőn alkalmazott, a tanulmányi és oktatási adminisztrációt támogató rendszer. Ennek keretében ún. EHA (egységes felhasználói azonosító) kódok kerültek kiadásra, melyek bizonyos egyetemi rendszerekben jelenleg is használatban vannak. Az EHA kód felépítése 7 (hét) betű és .PTE végződés.

Felhasználó: az a személy/rendszer, szervezet vagy csoport, aki (amely) az Egyetem által biztosított rendszerekhez erőforrásokhoz csatlakozik és/vagy az Egyetem által biztosított eszközt használ, valamint ennek során egy vagy több informatikai rendszert igénybe vesz feladatai megoldásához.

Felhasználói azonosító: az egyetemi címtárban tárolt egyedi azonosításra szolgáló rövid karaktersorozat, amely általában a felhasználó nevéből képződik.

Felhasználói hitelesítés: a felhasználó hitelességének ellenőrzése (a belépéskor minden felhasználó ellenőrzése) és különböző azonosító eszközök (pl.: jelszó, chip-kártya, biometrikus azonosítás stb.) alkalmazása.

Felhőszolgáltatás: olyan információs társadalommal összefüggő szolgáltatás, amely lehetővé teszi konfigurálható számítási erőforrások – különösen hálózatok, kiszolgálók, tárolók, alkalmazások, szolgáltatások – osztott készletének igény szerinti, hálózaton keresztül történő elérését. Ezen szolgáltatásokat nem kizárólag az Egyetem hardvereszközein üzemeltetik, hanem az üzemeltetés részleteit a felhasználótól elrejtve a szolgáltató eszközein elosztva vannak. A szolgáltatásokat publikus felhő esetében az interneten

keresztül, privát felhő esetében a helyi hálózaton vagy ugyancsak az interneten érik el a felhasználók. Felhőszolgáltatás esetében az Egyetem nem szolgáltató és nem üzemeltető.

Folyamatosság: az üzleti, egyetemi tevékenységek zavarmentes rendelkezésre állása. Folytonos védelem: olyan védelmi megoldás, amely az időben változó körülmények és viszonyok ellenére is megszakítás nélkül megvalósul.

Hálózat: számítógépek (vagy általánosabban informatikai rendszerek) összekapcsolása és az összekapcsolt rendszerek legkülönbözőbb komponensei közötti adatcserét megvalósító logikai és fizikai eszközök összessége.

Határvédelmi felelős: az Infrastruktúra Szolgáltatási Főosztály keretében kijelölt felelős, amely az informatikai határvédelmi és határbiztonsági rendszerek felelőse. (Pl. tűzfalrendszerek, hálózati hozzáférés-védelem, behatolásérzékelő és -megelőző rendszerek, távoli biztonságos elérés, hálózat szegmentációja.)

Hitelesség: az adat/információ (és az adathordozó) tulajdonsága, amellyel igazolhatjuk, hogy az adat bizonyítottan vagy bizonyíthatóan az elvárt forrásból származik.

Hozzáférés: olyan eljárás, amely valamely informatikai rendszer használója számára – jogosultságának függvényében – meghatározott célra, helyen és időben elérhetővé teszi az informatikai rendszer erőforrásait, elérhetővé tesz a rendszerben adatokként tárolt információkat.

Hozzáférési jogosultság: az informatikai rendszerben elvégezhető tevékenységekre vonatkozó engedély a felhasználó számára.

Illegális szoftver: az a szerzői jog védelme alatt álló szoftvertermék, amelynek a legalitás igazolásához szükséges dokumentumok (pl. licenc, számla, szállítólevél) nem mindegyike áll rendelkezésre, valamint a szoftver használata nem felel meg a licenc szerződés előírásainak.

Illetéktelen személy: olyan személy, aki az adat megismerésére nem jogosult.

Incidens: minden olyan informatikai vonatkozású esemény, ami nem része a normál működésnek és a felhasználókat akadályozza feladataik ellátásában. A szolgáltatási hiba típusú incidensek a szolgáltatási szintek csökkenésével járnak (vagy ezzel fenyegetnek), míg a szolgáltatási igény típusú incidensek általában valamilyen eszköz vagy információ biztosítását, módosítások végrehajtását igénylik. Egy incidensnek lezárásáig többféle állapota lehet.

Információbiztonság: az információ bizalmasságának, sértetlenségének és rendelkezésre állásának megőrzése; továbbá, egyéb a hitelesség, a számon kérhetőség, a letagadhatatlanság és a megbízhatóság szavatolása.

Informatikai biztonság: az Egyetem informatikai rendszerének olyan kielégítő állapota, amely az informatikai rendszerekben kezelt adatok bizalmassága, hitelessége, sértetlensége és rendelkezésre állása, illetve az informatikai rendszerelemek rendelkezésre állása és funkcionalitása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos.

Információbiztonsági dokumentációs rendszer: többszintű, egymásra épülő rendszer, amely magába foglalja a biztonságpolitikai elvektől a szabályzatokon keresztül a munkautasítások szintjéig az információbiztonsági irányelveket, teendőket, szereplőket, azok feladatait, jogait, kötelességeit és felelősségeit. Informatikai rendszer: információs-, ügyviteli-, egyetemi folyamat vagy szolgáltatás működését támogató elektronikus adatfeldolgozó eszközök és eljárások, valamint az ezeket kiszolgáló emberi erőforrások és a kapcsolódó folyamatok összessége. A hardver-, szoftver-, kommunikációs eszközök és ezek kezelő / kiszolgáló szervezeteinek olyan együttese, amelyet az Egyetem működésével összhangban céljai megvalósítására használ.

Információ-feldolgozó eszköz: minden olyan számítástechnikai, telekommunikációs és egyéb kategóriájú elektronikai eszköz, mely képes a betáplált (input) adatokat manipulálni és a folyamat végén eredményeket, kimenő adatokat (output) produkálni – az azt használó személy számára értelmezhető formában.

Információs vagyon: adatok, információk, szellemi, erkölcsi javak összessége.

Információbiztonsági Felelős: az Ibtv. szerinti az elektronikus információs rendszer biztonságáért felelős személy, aki kinevezés útján látja el az információbiztonsági felelősi feladatokat; szakterületén ellenőriz,

tanácsot ad, véleményez. Az Egyetemen a Pécsi Tudományegyetem igazgatásának szervezetére vonatkozó szabályzata (PTE SZMSZ 32. számú melléklet) 41/D. §-ban meghatározott feladatokat látja el. Egyik legfontosabb feladata, hogy a teljes egyetemi szervezeten belül kialakítsa és ellenőrizze azokat az információbiztonsági szabályokat, amelyek az informatikai rendszerekkel kapcsolatba lépőkre vonatkoznak.

Információvédelem: az informatikai rendszerek által kezelt adatok által hordozott információk bizalmasságának, hitelességének és sértetlenségének védelme.

Internet: a világháló.

Intranet: az intézményen belüli Hálózat és annak szolgáltatásai.

ITIL (IT Infrastructure Library): az 1980-as években, Angliában több, információtechnológiával (IT) foglalkozó cég által a brit kormány támogatásával létrehozott dokumentumsorozat, amiben az üzleti folyamatok IT eszközökkel megvalósított támogatására a gyakorlatban alkalmazott, jól bevált, gyártótól független üzemeltetési ajánlásokat gyűjtötték össze. Jelen szabályzat hatálybalépésekor a harmadik verziónál tart, 5 fő kötetből, és az ezekhez kapcsolódó kiegészítő anyagokból áll. Az ITIL a leginkább használt megközelítés az IT szolgáltatás-menedzsmentre, és főképp Európában az üzemeltetés de facto szabványa. Kizárólag az informatika üzemeltetési és üzemeltetés-szervezési kérdéseivel foglalkozik, dokumentált, kidolgozott oktatási és vizsgarendszere van.

Jogtiszta szoftver: olyan számítógépes program – alkalmazás – amelynek használatára a felhasználó (pl.: jellemzően késztermék vételi vagy szoftver-fejlesztési vállalkozási szerződésbe foglalt licenc megállapodással) megszerezte a jogosultságot.

Jogosultság: a lehetőség megadása az informatikai rendszerben végzendő tevékenységek végrehajtására.

Katasztrófa: az informatikai rendszer folyamatos és rendeltetésszerű működésének megszakadása.

Katasztrófahelyzet elhárítás tervezés: az informatikai rendszer rendelkezésre állásának megszűnése, nagy mértékű csökkenése utáni visszaállításra vonatkozó tervezés (DRP – Disaster Recovery Planning).

Kockázat: az informatikai fenyegetettség mértéke, amely valamely fenyegető tényezőből ered és amelyet a kockázatelemzés során a fenyegető tényezők értékelése révén tárunk fel. A kockázat két részből, a kárnagyságból és a bekövetkezés gyakoriságából tevődik össze. Az Ibtv. szerint a kockázat a fenyegetettség mértéke, amely egy fenyegetés bekövetkezése gyakoriságának (bekövetkezési valószínűségének) és az ez által okozott kár nagyságának a függvénye.

Kockázatelemzés: olyan elemző és értékelő jellegű szakértői vizsgálat, amely az informatikai rendszerekben kezelt adatok és alkalmazások értékelése, gyenge pontjainak és fenyegetettségeinek elemzése útján meghatározza a potenciális kárértékeket és azok bekövetkezési valószínűségét és gyakoriságát. Az Ibtv. szerint a kockázatelemzés az elektronikus információs rendszer értékének, sérülékenységének (gyenge pontjainak), fenyegetéseinek, a várható károknak és ezek gyakoriságának felmérése útján a kockázatok feltárása és értékelése.

Kockázatkezelés: védelmi intézkedések kidolgozása, elemzése és meghozatala, amelyet követően a maradványkockázatok elviselhető szintűre változnak. Az Ibtv. szerint az elektronikus információs rendszerre ható kockázatok csökkentésére irányuló intézkedésrendszer kidolgozása.

Kockázatarányos védelem: az a védelem, mely a kockázatokat a releváns fenyegetettségek bekövetkezési valószínűsége és a fenyegetettség bekövetkezésekor keletkező kár függvényeként kezeli, és ahol a védelemre fordított erőforrások értéke arányos a védendő értékek nagyságával, illetve kockázatcsökkentő képességével. Az Ibtv. szerint sz elektronikus információs rendszer olyan védelme, amelynek során a védelem költségei arányosak a fenyegetések által okozható károk értékével.

Kontrollok-óvintézkedések: mindazok a fizikai-, adminisztratív-, technikai-, technológiai módok, eljárások, amelyeket védelmi célból tettek meg és a kockázatot csökkentik.

Kriptográfia: mindazoknak a matematikai eljárásoknak, algoritmusoknak és biztonsági rendszabályoknak a kutatása és alkalmazása, amelyek elsődleges célja az információnak illetéktelenek előli elrejtése.

Különleges adat: a személyes adatok különleges kategóriáiba tartozó minden adat, azaz a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló

személyes adat, valamint a genetikai adatok, a természetes személyek egyedi azonosítását célzó biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok.

Külső közreműködő (harmadik fél): olyan külső szervezet, hatóság, szerződéses partner (jogi vagy természetes személy), akinek tevékenysége indokolttá teszi az Egyetem belső használatú és annál magasabb minősítésű adataihoz vagy bármely informatikai rendszeréhez történő hozzáférést.

Legális szoftver: az a szerzői jog védelme alatt álló szoftvertermék, amelynek legalitásának igazolásához minden szükséges dokumentum (pl. licenc, számla, szállítólevél, ajándékozási szerződés) rendelkezésre áll, valamint a használata a szoftver licenc szerződés előírásainak megfelelő módon történik.

Letagadhatatlanság: a letagadhatatlanság azon követelmény, amely meghatározza, hogy a felhasználók egy későbbi időpontban ne tudják valamilyen okból önkényesen megtagadni az előzőekben általuk végrehajtott tranzakciót.

Maradványkockázat: az a tudatosan felvállalt kockázat, amely alapvetően – kis mértékben – annak ellenére is fennmarad, hogy a fenyegető tényezők ellen intézkedések eredményesen végrehajtásra kerültek.

Megbízható működés: az informatikai rendszerek, és az általuk kezelt adatok által hordozott információk rendelkezésre állásának és funkcionalitásának védelme.

Mentés: informatikai folyamat, amelynek során az informatikai rendszerben digitálisan tárolt vagy használatban lévő fontos adathalmazokról egy speciális eszközzel egy speciális adathordozóra (mentési médium) másolatokat készítenek.

Mentési médium: adathordozó (a legtöbbször mágneses elven működő szalagos egység), amelyen a mentések által duplikált adattartalmat tárolják.

Mobil eszköz: Minden olyan számítástechnikai eszköz, amely fizikailag szabadon mozgatható és funkcionalitását betölti mozgás közben is. Ide sorolhatók a hordozható számítógépek, illetve a velük azonos adattárolási, adatkezelési és adatmegjelenítési funkciókkal bíró telekommunikációs eszközök (pl. tablet, notebook, okostelefon stb.), valamint a hordozható adattárolók (pl. külső merevlemez, pendrive stb.).

Mobil kód: olyan szoftver vagy kód, mely általában egy távoli számítógépről, hálózaton keresztül letöltve, határozott telepítési vagy indítási procedúra nélkül fut vagy futtatható a kliens gépen. Ilyenek például a scriptek (JavaScript, VBScript), Flash animációk, Java kisalkalmazások, MS Office dokumentumok makrói, ActiveX vezérlők.

NEPTUN kód: a NEPTUN rendszerszolgáltatásaihoz hozzáférést biztosító betűkből és számokból álló, legalább 6 karakter hosszúságú kód.

Rendelkezésre állás: az informatikai rendszer tényleges állapota, amely megvalósul, ha a rendszer szolgáltatásai állandóan, illetve egy meghatározott időben hozzáférhetők és a rendszer működőképessége sem átmenetileg, sem pedig tartósan nincs akadályozva. Az Ibtv. szerint annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek.

Sértetlenség: az adat olyan tulajdonsága, amely arra vonatkozik, hogy az adat fizikailag és logikailag teljes, ép, módosulatlan. Informatikai rendszer tulajdonság, amely adott, ha a rendszerben kezelt adatokat, illetve az adatkezelést megvalósító összes többi rendszer komponenst csak az arra jogosultak és csak dokumentáltan változtatják meg, emellett minden egyéb (véletlen vagy szándékos) módosulás kizárt — vagyis az adatok és feldolgozási folyamataik pontosak és teljesek. Az Ibtv. szerint a az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az az elvárt forrásból származik (hitelesség) és a származás ellenőrizhetőségét, bizonyosságát (letagadhatatlanságát) is, illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható.

Személyes adat: azonosított vagy azonosítható természetes személyre (továbbiakban: érintett) vonatkozó bármely információ, amely alapján az érintett közvetlen vagy közvetett módon, különösen valamely azonosító, (például név, szám, helymeghatározó adat, online azonosító) vagy a természetes személy testi, fiziológiai,

genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható.

A személyes adat az adatkezelés során mindaddig megőrzi e minőségét, amíg kapcsolata az érintettel helyreállítható. Az érintettel akkor helyreállítható a kapcsolat, ha az adatkezelő rendelkezik azokkal a technikai feltételekkel, amelyek a helyreállításhoz szükségesek.

Szolgáltatás- vagy alkalmazásgazda: azon természetes személy (foglalkoztatott), aki az adott szolgáltatás vagy alkalmazás üzemeltetéséért felelős.

Teljes körű védelem: teljes körűnek nevezik az informatikai rendszer védelmét, ha az informatikai rendszer összes elemére kiterjed.

Üzleti titok: a működéshez, az üzletmenethez és a gazdasági tevékenységhez kapcsolódó minden olyan tény, információ vagy adat, amelynek titokban maradásához a jogosultnak méltányolható érdeke fűződik, és amelynek titokban tartása érdekében a jogosult a szükséges intézkedéseket megtette.

Üzletmenet folytonosság tervezés: az egyetemi folyamatok rendelkezésre állásának olyan szinten történő fenntartása, hogy a kiesésből származó károk a szervezet számára még elviselhetőek legyenek.

Védelmi intézkedés: a fenyegetettség bekövetkezési valószínűsége, illetve a bekövetkezéskor jelentkező kár csökkentésére szervezési- vagy technikai eszközökkel tett intézkedés.

Tűzfal: A tűzfal (angolul firewall) célja annak biztosítása, hogy egy adott hálózatra vagy számítógépbe ne történhessen illetéktelen behatolás. A tűzfalak általában folyamatosan jegyzik a forgalom bizonyos adatait, a bejelentkező gépek és felhasználók azonosítóit, a rendkívüli és kétes eseményeket, továbbá riasztásokat is adhatnak. A tűzfal megpróbálja a privát hálózatot, illetve a hálózati szegmenst a nem kívánt támadásoktól megóvni. Szabályozza a különböző megbízhatósági szintekkel rendelkező számítógép-hálózatok közti forgalmat.

Változáskezelés: azon szabályok összessége, amelyek meghatározzák egy informatikai alkalmazás adatszolgáltatási folyamataiban, az azokat kiszolgáló informatikai eljárásokban és szolgáltatásokban, valamint az alkalmazás üzemeltetését lehetővé tevő informatikai infrastruktúrában bekövetkező módosítások, változások biztonságos végrehajtását és nyilvántartását, változásainak nyomon követhetőségét.

Védelmi rendszer: a védelmi rendszer az informatikai rendszer megfelelő szintű biztonságának garantálása érdekében alkalmazott fizikai-, logikai- és adminisztratív védelmi intézkedések összessége.

Kártékony kódok (malware): olyan rosszindulatú számítógépes program vagy programtörzs (pl.: vírus, trójai zsarolóvírus, kémprogram stb.), amely illegálisan készült egy felhasználói program részeként. A felhasználói program alkalmazása során átterjedhet, "megfertőzhet" más, az informatikai rendszerben lévő rendszer-, illetve felhasználói programot, sokszorozva önmagát (ami lehet mutáns is) és a logikai bomba hatás révén egy beépített feltételhez kötötten (pl.: konkrét időpont, szabad lemezterületi helyek száma stb.) trójai faló hatást indít el.

Vírusvédelmi rendszer: a vírusvédelmi rendszer és a hozzá kapcsolódó védelmi mechanizmusok feladata az informatikai rendszerhez kapcsolódó rosszindulatú számítógépes programok (például vírusok) felkutatása, működésük, aktív vagy passzív károkozásuk megakadályozása, illetve – lehetőség szerint – megsemmisítésük.

Visszaállítási eljárás: olyan eljárásrend, amelynek részeként elvégzett tevékenységek, feladatok biztosítják, hogy a helyreállítási eljárással beindított informatikai szolgáltatás alternatívájáról az ügyviteli folyamat visszaáll a normál üzemmenetre.

VPN: Virtual Private Network. A virtuális magánhálózat a magánhálózat kiterjesztése, amely megosztott vagy nyilvános hálózatokon (például interneten) keresztüli kapcsolatokat tartalmaz. Virtuális magánhálózattal úgy lehet adatokat küldeni két számítógép között, mintha a két gép közvetlen kapcsolatban lenne egymással. A VPN kapcsolatok segítségével a szervezetek földrajzilag különálló irodákkal vagy más szervezetekkel is létesíthetnek kapcsolatot úgy, hogy a kommunikáció biztonságos maradjon.

Zárt védelem: az összes számításba vehető fenyegetést figyelembe vevő védelem.

PTE Informatikai Biztonsági Szabályzat 2. számú melléklet

Kapcsolódó jogszabályok, szabályozások listája

1. Jogszabályi háttér

–

1.1. Jogszabályok

- 1997. évi CLIV. törvény az egészségügyről
- 1997. évi XLVII. törvény az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről
- 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (Infotv.)
- 2011. évi CXC. törvény a nemzeti köznevelésről
- 2011. évi CCIV. törvény a nemzeti felsőoktatásról (Nftv.)
- 2012. évi I. törvény a munka törvénykönyvéről
- 2012. évi C. törvény a Büntető Törvénykönyvről
- 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről
- 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról (Ibtv.)
- 2013. évi V. törvény a Polgári Törvénykönyvről
- 2013. évi LXXVII. törvény a felnőttképzésről
- 2015. évi CXLIII. törvény a közbeszerzésekről
- 2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól
- 2019. évi LXXX. törvény a szakképzésről

–

1.2. Uniós jogszabályok

- Az Európai Parlament és az Európai Tanács (EU) 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) (a továbbiakban GDPR)
- 2016/1148 (EU) európai parlamenti és tanácsi irányelv a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről

–

1.3. Kormányrendeletek

- 65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról
- 187/2015. (VII. 13.) Korm. rendelet az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról
- 246/2015. (IX. 8.) Korm. rendelet az egészségügyi létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről
- 451/2016. (XII. 19.) Korm. rendelet - az elektronikus ügyintézés részletszabályairól
- 271/2018. (XII. 20.) Korm. rendelet az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének és műszaki vizsgálatának, továbbá a sérülékenységvizsgálat lefolytatásának szabályairól
- 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági,

valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről
- 26/2013. (X. 21.) KIM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról
- 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról
- 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról
- 1/2018. (VI. 29.) ITM rendelet a digitális archiválás szabályairól

2. Kapcsolódó belső szabályozások

- A Pécsi Tudományegyetem Szervezeti és Működési Szabályzata (PTE SZMSZ);
- A PTE SZMSZ 4. számú melléklete – A Pécsi Tudományegyetem foglalkoztatási követelményrendszere;
- A PTE SZMSZ 32. számú melléklete - A Pécsi Tudományegyetem igazgatásának szervezetére vonatkozó szabályzata;
- A PTE SZMSZ 37. számú melléklete – A Klinikai Központ szervezeti és működési szabályzata;
- A Pécsi Tudományegyetem Informatikai Szabályzata;
- A Pécsi Tudományegyetem Távközlési Szabályzata;
- A Pécsi Tudományegyetem Belső Kontroll Kézikönyve;
- Egységes Felsőoktatási Tanulmányi Rendszer (NEPTUN) működési rendjéről szóló szabályzat;
- A Pécsi Tudományegyetem Adatvédelmi Szabályzata;
- A Pécsi Tudományegyetem Egészségügyi Adatvédelmi Szabályzata;
- A Pécsi Tudományegyetem a közérdekű adatok nyilvánosságra hozataláról és a közérdekű adatok megismerésére irányuló igények teljesítésének rendjéről szóló Szabályzata;
- A Pécsi Tudományegyetem Rendészeti és Vagyonvédelmi Szabályzata;
- A Pécsi Tudományegyetem Tűzvédelmi Szabályzata;
- A Pécsi Tudományegyetem Belső Kontroll Kézikönyve
- Kritikus alkalmazások üzemeltetési utasításai;
- A Pécsi Tudományegyetem közbeszerzési szabályzata
- A Pécsi Tudományegyetem közbeszerzési eljárás nélkül lebonyolított beszerzési eljárások szabályzata; továbbá a mindenkor hatályos Üzemeltetési és Beszerzési Igazgatói utasítások

–

3. Kapcsolódó szabványok és ajánlások

- MSZ EN ISO 9000:2015 Minőségirányítási rendszerek. Alapok és szótár,
- MSZ EN ISO 9001:2015 Minőségirányítási rendszerek. Alapok és követelmények,
- ISO/IEC 27000:2014 Information technology - Security techniques – Information security managements systems. Overview and vocabulary,
- MSZ ISO/IEC 27001:2014 Informatika. Biztonságtechnika. Információbiztonsági irányítási rendszerek. Követelmények,
- MSZ ISO 31000:2015 Kockázatfelmérés és -kezelés. Alap- és irányelvek,
- ITIL. (Information Technology Infrastructure Library) informatikai rendszerek üzemeltetésére és fejlesztésére szolgáló kormányzati ajánlás, „de facto” szabvány.
- a MABISZ biztonságtechnikai ajánlása B/I. pontja szerinti teljes mechanikai, fizikai védelem;
- a MABISZ biztonságtechnikai ajánlása C/I/2. pontja szerinti részleges elektronikai jelzőrendszer;
- a MABISZ biztonságtechnikai ajánlása C/II. pontja szerinti beléptető rendszer.

PTE Informatikai Biztonsági Szabályzat 3. számú melléklet

Információbiztonsági Politika

A Pécsi Tudományegyetem (továbbiakban: PTE) a Dél-Dunántúli régió meghatározó felsőoktatási intézménye, mely komoly múlttal és tradíciókkal rendelkezik, ugyanakkor a jövőben regionális szinten vezető, országos szinten meghatározó, nemzetközi szinten mértékadó szereplővé kíván válni.

Ennek elengedhetetlen feltétele – összhangban Magyarország Nemzeti Kiberbiztonsági Stratégiájával – az adatvagyon, az elektronikus információs rendszerek magas szintű védelme, a kiberbiztonsági elemek fokozottabb implementációja. A PTE alaptevékenységei – úgy, mint az oktatás, a tudományos kutatás, a művészeti alkotótevékenység, a gyógyítás, – által, létfontosságú rendszerelem üzemeltetőként az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény hatálya alá tartozik, ezért minden szervezeti egységének és munkavállalójának alapvető érdeke a biztonságos és megbízható kibertéren belül az informatikai rendszerek és rendszerelemek folyamatos működési biztonságának megvalósítása, megerősítése.

Információbiztonság szempontjából a technikai védelmi megoldások mellett a PTE nagy hangsúlyt fektet a felhasználói tudatosság információbiztonság szempontjából történő fejlesztésére is, tekintettel arra, hogy a támadók a rendszerek sérülékenységeit kihasználva egyre nagyobb mértékben veszik célba a felhasználót.

1. Célkitűzés

Jelen Információbiztonsági Politika célja magas szinten támogatni (és szabályozni) a PTE alapfeladatainak zavartalan ellátásához szükséges információbiztonsági alapelveket, hogy mind a rendszerek állapotát, mind a bekövetkezett biztonsági eseményeket figyelemmel lehessen kísérni egységes módon, központilag.

2. Alapelvek

A PTE az informatikai biztonság területén az alábbi alapelveket érvényesíti:

1. **Bizalmasság:** az elektronikus információs rendszerekben tárolt információkat csak az arra jogosultak és csak a jogosultsági szintjüknek megfelelően ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásukról.

–

2. **Sértetlenség:** az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az az elvárt forrásból származik (hitelesség) és a származás ellenőrizhetőségét, bizonyosságát (letagadhatatlanságát) is, illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme kizárólag rendeltetésének megfelelően használható.

–

3. **Rendelkezésre állás:** az elektronikus információs rendszerek az arra jogosult számára elérhetőek és az abban kezelt adatok felhasználhatók.

–

4. **Védelem teljeskörűsége:** jelen elvet a fizikai-logikai és az adminisztratív védelem területén három dimenzióban kell megvalósítani:
    a. az összes rendszerelemre;
    b. a rendszerek architektúrájának valamennyi rétegére, alkalmazások és infrastruktúra területén egyaránt;
    c. a központi, illetve a végponti informatikai eszközökre és környezetükre.

–

5. **A védelem zártsága:** az összes valószínűsíthető fenyegetés ellen megelőző védelmi intézkedések megvalósításra kerültek és azok szabályozott, szerves egységet alkotnak.

–

6. **A védelem kockázatarányossága:** az elektronikus információs rendszer olyan védelme, amelynek során - egy kellően nagy időintervallumban - a védelem költségei arányosak a fenyegetések által okozható károk értékével. Célkitűzés a minimális költséggel elért maximális védelmi képesség.

–

7. **A védelem folytonossága:** a kialakított védelmi intézkedések az időben állandóan változó biztonsági környezet és viszonyok mellett is megszakítás nélkül fennállnak a rendszer teljes életciklusa alatt.

A PTE az információbiztonsági védelmi intézkedések megvalósítása során mind az információbiztonsági szabályozás kialakítása, mind a napi operatív intézkedések során három, egymásra épülő és egymást kiegészítő kontrollra épít, továbbá figyelembe veszi, hogy a lehetséges veszélyek teljes kizárása lényegében lehetetlen, így a veszélyek feletti kontrollra fókuszál.

A beépített biztonsági kontrollok az alábbiak:

a) preventív (megelőző) kontroll;
b) detektív (észlelő) kontroll;
c) korrektív (elhárító) kontroll.

A PTE a fenti alapelvek figyelembevételével tervezte meg, alakította ki, működteti és fejleszti információbiztonsági szabályozását és folyamatait annak érdekében, hogy a kezelésében lévő adatvagyon bizalmasságát, sértetlenségét és rendelkezésre állását, valamint az elektronikus rendszerek elemeinek rendelkezésre állását, sértetlenségét veszélyeztető mindenkori fenyegetések kockázataival arányos, zárt, teljes körű és folyamatos, a rendszerek teljes életciklusára kiterjedő védelmét biztosítsa logikai, fizikai, és adminisztratív védelmi intézkedések bevezetésével.

A PTE minden munkatársának, szerződéses partnerének elemi érdeke és kötelessége az információbiztonsági szempontok figyelembevétele és az információbiztonsági szabályozások betartása, ennek érdekében folyamatosan növeli és fejleszti a munkavállalók biztonságtudatossági szintjét.

PTE Informatikai Biztonsági Szabályzat 4. számú melléklet
Elektronikus információs rendszerek biztonsági osztályba sorolása

Rendszer	Felelős	Biztonsági osztály
Neptun Egységes tanulmányi rendszer	IIG	4
eMedSolution Kórházi információs rendszer (HIS)	KK	4
Aspyra PACS Medikai képtároló és továbbító rendszer	KK	3
SAP Integrált vállalatirányítási rendszer (ERP)	IIG	3
Nexon Bér- és humánügyviteli információs rendszer	IIG	4
Poszeidon irat és dokumentumkezelő rendszer	IIG	3
PTE KPVK Informatikai rendszer	KPVK	3
PTE BTK web szerverek	BTK	3
GLIMS laboratóriumi információs rendszer	KK	4
Corvina integrált könyvtári rendszer	EKTK	3
Központi DNS szolgáltatás	IIG	3
Alkörzeti DNS szolgáltatás	Alegységek	3
Vezetékes számítógép hálózat	IIG	3
Moodle e-Learning CMS	IIG	2
Egyetemi PSTN és VoIP távközlési rendszer	IIG	2
Eduroam vezeték nélküli számítógép hálózat	IIG	2
Egyetemi levelező rendszer	IIG	3
Alegységek levelező rendszerei	Alegységek	3
Alegységek oktatástámogató információs rendszerei	Alegységek	2
Egészségügyi informatikai támogató rendszerek	KK	3
Központi portál rendszer	IIG	2
Kutatás támogató információs rendszerek	Alegységek	2
Microsoft 365 felhő alapú információs rendszer	IIG	3
Központi Active Directory címtárszolgáltatás	IIG	3
Nagios hálózati és rendszer monitorozó infrastruktúra	IIG	4
Fizikai és logikai riasztó és megfigyelő rendszerek	Alegységek	2
Központi fájl szerverek, tárolórendszerek	IIG	3
Központi virtualizációs környezet	IIG	3
Határvédelmi rendszerek	IIG	4
Központi adatbázis szolgáltatás	IIG	3
Egyetemi Vezetői Információs Rendszer (VIR)	IIG	2
Medbakter mikrobiológiai informatikai rendszer	KK	4
Foglalkozás-egészségügyi nyilvántartó rendszer	KK	3
Időszerver szolgáltatás	IIG	3
Alegységek egyéb informatikai rendszerei és szolgáltatásai	Alegységek	2
PTE Service Manager	IIG	2
CATO	KK	3
POCT (Point of Care Testing)	KK	3

PTE Informatikai Biztonsági Szabályzat5. számú melléklet

Szervezetek biztonsági szintbe sorolása

Szervezet/Szervezeti egység	Biztonsági szint
Pécsi Tudományegyetem általános besorolás	3
Klinikai Központ általános besorolás	3
Szőlészeti és Borászati Kutatóintézet	2
Pécsi Tudományegyetem Informatikai és Innovációs Igazgatóság	4

PTE Informatikai Biztonsági Szabályzat 6. számú melléklet

Adatosztályozó lap

Adatgazda: (név, beosztás)		
Szervezeti egység:		
Adatcsoport megnevezése (rendszer):		

Az adatcsoport rövid leírása (célja, funkciója, rendeltetése):

Osztályozás:	
Bizalmasság és sértetlenség szempontjából (Nyilvános, Belső, Bizalmas, Titkos)	
Rendelkezésre állás szempontjából (1-5 skála)	

Dátum: ……,

……

Adatgazda

KITÖLTÉSI ÚTMUTATÓ

Adatbiztonsági kategóriák:

Adatbiztonsági kategória (Hozzáférés)	Jelölés	Tárolás	Továbbítás	Megsemmisítés
Nyilvános adatok	Jogszabály által nem védett adatok	Nincsen speciális követelmény, bármilyen adathordozón, titkosítatlan formában tárolható.	Nincsen speciális követelmény, szabadon továbbítható.	Nincsen speciális követelmény, speciális megsemmisítést nem igényel.
Belső	A védett adatokat tartalmazó adathordozókat „Belső használatra” kell ellátni.	Az adathordozókat zárható helyiségben kell tárolni. Az informatikai rendszerben biztosítani kell az adatokhoz való hozzáférés vezérlését.	Szervezeten belüli továbbítása hozzáférési jogosultság függvényében engedélyezett. Szervezeten kívülre való továbbítása csak a vezető adatgazda engedélyével lehetséges az elfogadott titkosítási módszer alkalmazásával.	Megsemmisítés az adatgazda engedélyével. Megsemmisítés előtt az adathordozón levő adatokat visszaállíthatatlanul törölni kell.
Bizalmas	A bizalmas adatokat tartalmazó adathordozókat „Bizalmas” jelöléssel kell ellátni.	Az adathordozókat zárható helyen szekrényben, vagy zárható asztalfiókban kell tárolni. Az informatikai rendszerben biztosítani kell az adatokhoz való hozzáférés vezérlését.	Szervezeten belüli továbbítása hozzáférési jogosultság függvényében engedélyezett. Szervezeten kívülre való továbbítása csak a vezető adatgazda engedélyével lehetséges az elfogadott titkosítási módszer alkalmazásával.	Megsemmisítés a vezető adatgazda engedélyével. Megsemmisítés előtt az adathordozón levő adatokat visszaállíthatatlanul törölni kell.

Titkos	A titkos, illetve fokozottan védett adatokat tartalmazó adathordozókat „Titkos” jelöléssel kell ellátni.	A titkos, illetve fokozottan védett adatokat tartalmazó adathordozókat páncélszekrényben kell tárolni. Az informatikai rendszerben biztosítani kell az adatokhoz való hozzáférés hitelesítésen alapuló vezérlését.	Titkos, illetve fokozottan védett adatokat csak titkosított csatornán, hitelesített felhasználónak szabad küldeni, vagy csak helyi hozzáférés lehetséges.	Megsemmisítés az adatgazda külön engedélyével. Megsemmisítés előtt az adathordozón levő adatokat visszaállíthatatlanul törölni kell.

Azon adatok, amelyek egyértelműen máshova nem kerültek besorolásra, azok belső kategóriába tartoznak.

Az információrendszerben elektronikusan tárolt adatok esetén az adatok azon halmazát, amelyekre a tárolás körülményeiből adódóan jellemzően azonos védettség valósítható meg (közös adatbázis, azonos könyvtár), ugyanabba az adatbiztonsági osztályba kell sorolni, mégpedig oly módon, hogy a halmaz egészére ki kell terjeszteni a halmaz legérzékenyebb elemének besorolását, vagy a különböző adatbiztonsági osztályokba sorolható adatokat külön kell bontani.

Az Egyetem egyes folyamatai, szervezeti egységei nevében, az általuk használt adatok vonatkozásában az Adatgazdák határozzák meg az adat besorolási/adatosztályozási kategóriákat.

Az Egyetem informatikai rendszerében az adatok bizalmasságának, sértetlenségének és rendelkezésre állásának biztosításáért az IIIG Igazgatója a felelős.

Rendelkezésre állás szempontjából kategóriák:

Biztonsági osztály	**Leírás**
1	2.2. Az 1. biztonsági osztály esetében csak jelentéktelen káresemény következhet be, mivel 2.2.1. az elektronikus információs rendszer nem kezel jogszabályok által védett (pl.: személyes) adatot; 2.2.2. nincs bizalomvesztés, a probléma azérintett szervezeten belül marad, és azon belül meg is oldható; 2.2.3. a közvetlen és közvetett anyagi kár az érintett szervezet költségvetéséhez képest jelentéktelen;
2	2.3. A 2. biztonsági osztály esetében csekély káresemény következhet be, mivel 2.3.1. személyes adat sérülhet; 2.3.2. az érintett szervezet üzlet-, vagy ügymenete szempontjából csekély értékű, és/vagy csak belső (intézményi) szabályzóval védett adat vagy elektronikus információs rendszer sérülhet; 2.3.3. a lehetséges társadalmi-politikaihatás az érintett szervezeten belül kezelhető; 2.3.4. a közvetlen és közvetett anyagi kár eléri az érintett szervezet költségvetésének 1%-át.
3	2.4. A 3. biztonsági osztály esetében közepes káresemény következhet be, mivel 2.4.1. különleges személyes adat sérülhet, személyes adatok nagy mennyiségben sérülhetnek; 2.4.2. az érintett szervezet üzlet-, vagy ügymenete szempontjából érzékeny folyamatokat kezelő elektronikus információs rendszer, információt képező adat, vagy egyéb, jogszabállyal (orvosi, ügyvédi, biztosítási, banktitok stb.) védett adat sérülhet; 2.4.3. a lehetséges társadalmi-politikai hatás: bizalomvesztés állhat elő az érintett szervezeten belül, vagy szervezeti szabályokban foglalt kötelezettségek sérülhetnek; 2.4.4. a közvetlen és közvetett anyagi kár eléri az érintett szervezet költségvetésének 5%-át.
4	2.5. A 4. biztonsági osztály esetében nagy káresemény következhet be, mivel 2.5.1. különleges személyes adat nagy mennyiségben sérülhet; 2.5.2. személyi sérülések esélye megnőhet (ideértve például a káresemény miatti ellátás elmaradását, a rendszer irányítatlansága miatti veszélyeket); 2.5.3. az érintett szervezet üzlet-, vagy ügymenete szempontjából nagy értékű, üzleti titkot, vagy különösen érzékeny folyamatokat kezelő elektronikus információs rendszer, vagy információt képező adat tömegesen, vagy jelentősen sérülhet; 2.5.4. a káresemény lehetséges társadalmi-politikai hatásaként a jogszabályok betartása, vagy végrehajtása elmaradhat, bekövetkezhet a bizalomvesztés a szervezeten belül, az érintett szervezet felső vezetésében, vagy vezetésében személyi felelősségre vonást kell alkalmazni;

	2.5.5. a közvetlen és közvetett anyagi kár eléri az érintett szervezet költségvetésének 10%-át.
5	2.6. Az 5. biztonsági osztály esetében kiemelkedően nagy káresemény következhet be, mivel 2.6.1. különleges személyes adat kiemelten nagy mennyiségben sérülhet; 2.6.2. emberi életek kerülnek közvetlen veszélybe, személyi sérülések nagy számban következik be 2.6.3. a nemzeti adatvagyon helyreállíthatatlanul megsérülhet; 2.6.4. az ország, a társadalom működőképességének fenntartását biztosító létfontosságú információs rendszer rendelkezésre állása nem biztosított;2 .6.5. a lehetséges társadalmi-politikai hatás: súlyos bizalomvesztés az érintett szervezettel szemben, alapvető emberi, vagy a társadalom működése szempontjából kiemelt jogok sérülhetnek; 2.6.6. az érintett szervezet üzlet-vagy ügymenete szempontjából nagy értékű üzleti titkot, vagy kiemelten érzékeny folyamatokat kezelő elektronikus információs rendszer, vagy információt képező adat tömegesen vagy jelentősen sérülhet; 2.6.7. a közvetlen és közvetett anyagi kár eléri az érintett szervezet költségvetésének 15%-át.