A Pécsi Tudományegyetem
Informatikai Szabályzata

Pécs
Hatályos 2018. december 20. napjától

Tartalomjegyzék

A Pécsi Tudományegyetem (továbbiakban: Egyetem) Szenátusa az Egyetem oktatási, egészségügyi és kutatási–fejlesztési feladatainak támogatása, a tanulás, információszerzés elősegítése, a kapcsolatteremtés- és tartás új lehetőségeinek, valamint az információ szabad áramlásának informatikai eszközökkel történő biztosítása érdekében, a nemzeti felsőoktatásról szóló 2011. évi CCIV. (továbbiakban: Nftv.) törvényben, az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvényben (továbbiakban: Infotv.), valamint az Európai Parlament és a Tanács a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről szóló 2016/679. számú Rendelete (a továbbiakban: Rendelet) megfogalmazottak alapján az alábbi szabályzatot alkotja.[1]

I.fejezet
Általános rendelkezések

A szabályzat célja

1.§ (1) A szabályzat célja, hogy egy olyan keretet biztosítson az Egyetem informatikai működésének, ami megteremti a lehetőségét annak, hogy az Egyetem eleget tudjon tenni azon jogszabályban meghatározott követelményeknek, amelyek alapján informatikai feladatait ellátja.

(2) A szabályzat célja továbbá, hogy az Egyetem informatikai működését és szabályozását a világszerte elfogadott ITIL (IT Infrastructure Library) de facto IT szolgáltatásirányítási szabvány szerkezetéhez igazítsa, valamint az, hogy az Egyetem informatikai szolgáltatásainak kialakítása, üzemeltetése és igénybevétele a hatályos egyetemi szabályzatok és jogszabályok, különösen a személyes adatok védelméhez való jog figyelembe vételével történjen.

(3) A szabályzatnak erősítenie kell továbbá az Egyetem informatikai szolgáltatásaival kapcsolatos szolgáltatói szemléletmódot mind felhasználói, mind szolgáltatói oldalon.

(4) A szabályzat az Egyetem informatikai működését, eszközgazdálkodását, szolgáltatásainak kialakítását, üzemeltetését, igénybevételét és ellenőrzési lehetőségeit szabályozza. A szabályzat meghatározza továbbá az eszközök beszerzésének, használatának, selejtezésének módjára és feltételeire vonatkozó szabályokat is az Egyetem Közbeszerzési Szabályzatával, közbeszerzési eljárás nélkül lebonyolított beszerzési eljárások szabályzatával, valamint felesleges vagyontárgyak selejtezéséről, belső hasznosításáról szóló szabályzatával összhangban.

A szabályzat hatálya

2.§ (1) A szabályzat tárgyi hatálya kiterjed az Egyetem teljes informatikai infrastruktúrájának valamennyi szoftver és hardver elemére, beleértve a személyi használatú eszközöket (például számítógépek, perifériák, nyomtatók), az egyetemi szolgáltatások igénybevételére használt saját tulajdonú eszközöket és a központi hardver eszközöket (például szerverek, adatok továbbítására alkalmas eszközök).

(2) A szabályzat személyi hatálya kiterjed:

---

[1] *A módosítást a Szenátus 2018. december 20-ai ülésén fogadta el. Hatályos: 2018. december 20. napjától.*

a) PTE SZMSZ 77-78. §-okban meghatározott karokra, önálló szervezetekre, valamint az Egyetem által fenntartott köznevelési intézményekre;

b) az Egyetemmel közalkalmazotti jogviszonyban, munkaviszonyban, vagy munkavégzésre irányuló egyéb jogviszonyban álló személyekre,

c) az Egyetemmel hallgatói jogviszonyban álló személyekre (továbbiakban együttesen felhasználókra).

(3) A szabályzat területi hatálya kiterjed:

a) az Egyetem teljes területére,
b) az Egyetem eszközeit az Egyetem területén kívül történő igénybevétel 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).

Értelmező rendelkezések

3.§ E szabályzat alkalmazásában:

1. **Informatikai (IT) infrastruktúra**: információ, adat feldolgozására, továbbítására, tárolására alkalmas hardver elemek összessége.
2. **Informatikai szolgáltatás (rendszer, vagy szolgáltatás):** olyan, IT infrastruktúrán üzemelő szolgáltatás, amely adatokat tartalmaz (például alkalmazások, nyilvántartások), vagy adatokhoz való hozzáférést valósít meg (például hálózati szolgáltatások). Az egyes informatikai szolgáltatások pontos határai a szolgáltatások leírásában (a továbbiakban: szolgáltatás leírás) kerülnek meghatározásra.
3. **Informatikai alkalmazás**: az informatikai szolgáltatások egy szűkebb értelmezése. Informatikai alkalmazások esetében egy konkrét szoftver és kiszolgáló környezetének segítségével valósul meg a szolgáltatás.
4. **Adatgazda**[2]: azon természetes vagy jogi személy, szervezeti egység, akinek, amelynek az érdekében egy informatikai szolgáltatásban az adatok tárolása, kezelése történik.
5. **Szolgáltatás- vagy alkalmazásgazda**: azon természetes személy (munkavállaló), aki az adott szolgáltatás vagy alkalmazás üzemeltetéséért felelős.
6. **Felhasználó:** a szolgáltatást igénybe vevő természetes vagy jogi személy.
7. **Incidenskezelés:** adott szolgáltatással kapcsolatos hibakezelési folyamat, amely a hiba bejelentésétől, azonosításától az elhárításáig tart.
8. **Egyszerű változáskezelés**: olyan előre jóváhagyott folyamat mentén végbemenő változás a szolgáltatásokban, amelyeknek a kockázata alacsony, tipikus beavatkozást igényel és valamilyen eljárást, vagy munkautasítást követ. Ilyen lehet például egy jelszómódosítás, vagy mobiltelefon készülék cseréje.
9. **Kiemelt adatok:** személyes adatok, különösen betegadatok, hallgatói, tanulmányi adatok, bér és munkaügyi adatok, továbbá a gazdálkodási, valamint a kutatási adatok.

[2] *A módosítást a Szenátus 2018. december 20-ai ülésén fogadta el. Hatályos: 2018. december 20. napjától.*

10. **Központi címtár:** Az egyetemi polgárok és a külső felhasználók informatikai szolgáltatásokban történő azonosításához szükséges adatokat tároló címtár, amelynek az üzemeltetését az Informatikai Igazgatóság végzi.
11. **Szolgáltatás üzemeltetés:** szolgáltatásonként eltérő feladat, ami meghatároz minden olyan tevékenységet, ami az adott szolgáltatás folyamatos biztosításához szükséges. Például: karbantartás, mentés, telepítés, stb.
12. **Informatikai rendszer gyengesége:** olyan – általában szoftver – hiba, aminek a kihasználásával a rendszer kötöttségeit (például jogosultsági rendszer) megkerülve az informatikai szolgáltatáshoz nyerhető hozzáférés, vagy a rendszer működésében idézhető elő zavar.
13. **Adatvédelmi incidens:**[3] a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az adatokhoz való jogosulatlan hozzáférést eredményezi.

II.fejezet
Az Egyetem átfogó informatikai menedzsmentje

4.§ (1) Az Egyetem informatikai tevékenységének részletes szabályozását és koordinálását a Kancellária Informatikai Igazgatósága (továbbiakban: IIG) látja el. Az IIG működésével kapcsolatos minden információ a Kancellária weboldalán érhető el, melynek címe: http://kancellaria.pte.hu/szervezet/informatikai_igazgatosag.

(2) Az Egyetemen informatikai tevékenység (fejlesztés, beruházás, bővítés, felújítás, karbantartás) kizárólag az IIG tájékoztatásával és jóváhagyásával történhet. Amennyiben az IIG 30 napon belül nem emel kifogást a bejelentett tevékenységgel szemben, úgy az engedélyezettnek tekinthető.

Nyilvántartások

5.§ (1) Az Egyetemen az informatikai terület minden szintjéről naprakész nyilvántartást kell vezetni minimálisan a (2) bekezdésben meghatározott bontásban.

(2) A minimálisan nyilvántartandó szintek:
a) informatikai infrastruktúra, informatikai eszközök;
b) informatikai hálózatok;
c) egyetemi informatikai szolgáltatások és alkalmazások;
d) az egyetemen használt szoftverek;
e) külső szolgáltatótól igénybe vett szolgáltatások.

(3) A nyilvántartások vezetéséhez az IIG elektronikus adatbázist biztosít és üzemeltet.

(4) A nyilvántartások feltöltése és naprakészen tartása
a) eszközök és szoftverek esetén az eszköz leltári felelősének,

[3] *A módosítást a Szenátus 2018. december 20-ai ülésén fogadta el. Hatályos: 2018. december 20. napjától.*

b) informatikai hálózatok esetében az alhálózati menedzserek, azaz az adott hálózati szolgáltatást üzemeltető személyek,
c) informatikai szolgáltatások és alkalmazások esetében a szolgáltatás-, vagy alkalmazásgazdák,
d) külső szolgáltatóval kötött szerződés esetén a szerződés szakmai ellenjegyzőjének a feladata.

(5) A nyilvántartásban nem szereplő entitások elérése és hozzáférhetősége az IIG által bármikor megszüntethető. A hozzáférés megszüntetése előtt az IIG tájékoztatást küld az adott szolgáltatás adatgazdájának és öt munkanapos határidőt biztosít a hiány pótlására. Az adott szolgáltatás elérése és hozzáférhetősége megszüntetésre kerül a pótlás elmaradása esetén a határidő lejárta után. Indokolt esetben (például az Egyetem működését veszélyeztető rendszerek, vagy bűncselekmény gyanújának esetében) az informatikai szolgáltatások elérése és hozzáférhetősége előzetes tájékoztatás nélkül azonnal megszüntetésre kerülnek.

(6) Az IIG az egyetemi analitikus leltár mellett részletes nyilvántartást vezet a szabályzat hatálya alá tartozó szoftverekről és alkalmazásokról.

(7) A szoftverekről, alkalmazásokról és szolgáltatásokról vezetett nyilvántartásnak az **1. számú mellékletben** meghatározott attribútumokat szükséges tartalmaznia.

Eszköz- és szoftvergazdálkodás

6.§ (1) Az Egyetem informatikai eszközök tekintetében központosított eszközgazdálkodást folytat, az eszközgazdálkodással kapcsolatos teendőket az IIG látja el.

(2) Az Egyetemen informatikai és távközlési eszközök beszerzésére, bérlésére, vagy átvételére kizárólag az IIG előzetes engedélyével van lehetőség.

(3) Az egyes szervezeti egységek az informatikai eszközigényüket a tárgyévi rendes beszerzési tervvel adják le a Kancellária részére.

(4) Az évi beszerzési tervben le nem adott igények alapján történő beszerzésre az informatikai igazgató adhat engedélyt megfelelő indoklás alapján. Az indoklásnak tartalmaznia kell azt, hogy az adott igény vagy igények miért nem kerültek feltüntetésre az éves beszerzési tervben, valamint azt is, hogy az egyetemre nézve milyen hátránnyal járna a beszerzések következő évre történő halasztása.

(5) A Kancellária az éves beszerzési terv alapján, a hatályos jogszabályoknak megfelelően végzi az informatikai jellegű beszerzéseket. A cél elsősorban hosszútávon alkalmazható keretszerződések megkötése. Amennyiben keretszerződés megkötése nem lehetséges, úgy, minden évben legfeljebb négy alkalommal kerül lefolytatásra informatikai eszközbeszerzés.

(6) A beszerzések során a költséghatékonyság, a hosszú távú fenntarthatóság és az eszközpark egységesítése az elsődleges cél.

(7) A kategóriákba nem sorolható eszközök és az egyedi igények beszerzése egyedi eljárásokban történhet meg.

(8) Eszközbeszerzés általában, de nem kizárólag a **2. számú mellékletben** meghatározott kategóriákban lehetséges.

(9) Az egyes kategóriákon belüli eszközcsoportok minden évben december 15-ig kerülnek meghatározásra és az IIG weboldalán (http://kancellaria.pte.hu/szervezet/informatikai_igazgatosag) kerülnek közzétételre.

(10) A szervezeti egységektől, a gazdálkodási terv összeállítása során beérkező igények az egyes kategóriákon belül kialakított eszközcsoportokba kerülnek besorolásra.

(11) Informatikai eszközbeszerzés a hatályos egyetemi szabályzatoknak és jogszabályoknak megfelelően történhet.

(12) A költséghatékony beszerzés céljából az egyes kategóriáktól való eltérés, valamint egyedi igényekre szabott beszerzési eljárás indítása kizárólag előzetes kancellári engedéllyel történhet.

(13) Az anyagigények gyors kielégítése céljából a Kancellária a gyakran igényelt informatikai anyagokból raktárkészletet képez. Az aktuális raktárkészlet mindig elérhető a Műszaki Szolgáltatási Igazgatóság raktári igénylőrendszerében.

(14) Nagy értékű (például kiszolgálók, tárolók, hálózati eszközök, melyek értéke eléri, vagy meghaladja a nettó 500.000 forintot) valamint nagymennyiségű (minimum 50 darab), a (8) bekezdésben felsorolt kategóriákba tartozó eszközök beszerzésére egyedi beszerzési eljárás indítható.

(15) Az egyes szervezeti egységeknél feleslegessé vált eszközöket lehetőség szerint az Egyetemen belül kell újra felhasználni, az Egyetem hatályos szabályzataiban és utasításaiban foglaltak alapján.

(16) Szoftver termék beszerzése során, a használatba vétel előtt a szoftver beszerzését igénylő feladata a beszerzéshez szükséges adatok IIG részre történő megküldése.

(17) A szoftvertermékekben bekövetkező változás (például felhasználószám módosulása) esetén a szoftver beszerzését igénylő feladata a megváltozott adatok IIG részre történő megküldése.

(18) Olyan funkciók megvalósítására szolgáló szoftver beszerzése, amely funkciók megvalósítására az Egyetem már rendelkezik szoftverrel, csak abban az esetben lehetséges, amennyiben a már rendelkezésre álló szoftver kivezetésre kerül. Új szoftver beszerzése helyett minden esetben a már rendelkezésre álló szoftver felhasználói számát szükséges bővíteni.

(19) Az egyes szoftverek Egyetemen belüli felhasználói körét a szoftver beszerzését igénylő határozza meg.

(20) Szoftver beszerzésére csak az IIG engedélyével van lehetőség.

(21) A jogszerű működés bizonyítását lehetővé tevő licencek – amennyiben léteznek ilyen iratok – nyilvántartása az IIG feladata, a licencek tárolása a hatályos egyetemi iratkezelési szabályzat rendelkezéseinek megfelelően történik.

III.fejezet
Informatikai szolgáltatások

7.§[4] (1) Az Egyetem informatikai szolgáltatásaihoz – megfelelő jogosultság esetén – az egyetemi polgárok részére azonos módon és azonos mértékben kell hozzáférést biztosítani.

(2) Az Egyetem informatikai szolgáltatásainak minden esetben költséghatékonyan kell működnie, a túlzó, pazarló használatot el kell kerülni.

(3) Az Egyetemen informatikai szolgáltatást, vagy alkalmazást kizárólag az IIG nyújthat, üzemeltethet, ez alól kivétel csak kancellári engedéllyel tehető.

(4) Személyes adatokat kezelő szolgáltatásokat és alkalmazásokat kizárólag az IIG nyújthat és üzemeltethet az Egyetemen, ez alól kivétel csak kancellári engedéllyel tehető.

(5) Az Egyetem működéséhez elengedhetetlen adatokat kezelő informatikai szolgáltatások:

a) egészségügyi rendszerek,
b) tanulmányi rendszer és alrendszerei, távoktatást támogató rendszerek,
c) gazdálkodási rendszer,
d) munkaügyi rendszer,
e) e-mail kiszolgálók,
f) fájl szerverek,
g) hálózati tűzfalak, hálózatok,
h) web szerverek,
i) azonosítási rendszerek,
j) kutatási adatokat nyilvántartó rendszerek,
k) Kutatói Adminisztrációs Rendszer,
l) iktató, iratkezelő rendszerek,
m) integrált könyvtári rendszer,
n) intézményi repozitórium.

(6) A 7.§ (5) bekezdésében meghatározott szolgáltatásokhoz az IIG központi informatikai szolgáltatások keretében biztosítja az informatikai hátteret.

(7) Az összes egyetemi informatikai szolgáltatás esetében meg kell határozni és meg kell nevezni az adott szolgáltatás adatgazdáját.

(8) Az Egyetem Adatvédelmi Szabályzata 15. §-ban meghatározott kivételtől eltekintve az adatgazda felel az adott informatikai szolgáltatásban tárolt adatokhoz való hozzáférések engedélyezéséért, meghatározza az elvárt mentési és archiválási rendet, és megfogalmazza az egyes, az adatok elérhetőségét biztosító szolgáltatás elvárt rendelkezésre állását.

(9) Minden szolgáltatás esetében az Egyetemnek teljes körű leírással kell rendelkeznie a szolgáltatás működéséhez szükséges hardver és szoftver komponensekről, valamint azok konfigurációjáról (üzemeltetői dokumentáció). A leírás elkészítéséért, illetve vásárolt szoftverek esetén az üzemeltetői

---

[4] *A módosítást a Szenátus 2018. december 20-ai ülésén fogadta el. Hatályos: 2018. december 20. napjától.*

dokumentáció beszerzéséért az adatgazda felel. A dokumentum műszaki tartalmához az IIG adatot szolgáltat. Az üzemeltetői dokumentáció minimális tartalmát az **3. számú melléklet** tartalmazza.

(10) Minden szolgáltatás esetében létre kell hozni a szolgáltatási adatlapot és abban meg kell határozni az alábbiakat:

a) adatgazda,
b) elvárt rendelkezésre állás,
c) hozzáférés-, incidens-, változás- és problémakezelés folyamata és az ezekhez kapcsolódó nyomtatványok, űrlapok,
d) az adatgazda által elvárt mentési és archiválási rend,
e) normál karbantartási időablak.

(11) A leírásokat, adatlapokat, nyomtatványokat és dokumentációkat az IIG tárolja és kezeli.

(12) Minden informatikai szolgáltatás elsődleges futtatási környezete az egyetemi központi informatikai kiszolgáló infrastruktúra.

(13) Az egyetemi központi informatikai kiszolgáló infrastruktúra üzemeltetését az IIG végzi.

(14) Az egyetemi központi informatikai kiszolgáló infrastruktúrával kapcsolatos kapacitásmenedzsment feladatokat az IIG végzi, minden évben az adatgazdákkal egyeztetett várható igények alapján éves fejlesztési tervet készít.

Adatvédelmi és titoktartási szabályok

8.§ [5] (1) Minden olyan informatikai szolgáltatás esetén, amelynek keretében személyes adatok kezelésére kerül sor, adatkezelési törzskönyvet kell készíteni. Az adatkezelési törzskönyv elkészítésére az Adatvédelmi Szabályzat 9. §-át kell alkalmazni. A 3. § 2. pontban foglalt szolgáltatás leírások részeként a kapcsolódó adatkezelési törzskönyvek azonosítóját fel kell tüntetni.

(2) Személyes adatnak minősül a felhasználó IP címe is, amennyiben – felhasználói név és hitelesítés alkalmazásával – a bejelentkezésnek köszönhetően a szolgáltatásnyújtás során felépül az IP cím és a természetes személy közötti kapcsolat.

9.§[6] (1) Az informatikai szolgáltatások nyújtása és igénybevétele során a személyes adatokat, valamint az egyéb, titoknak minősülő adatokat (különösen a minősített adatokat, üzleti titkot vagy döntés megalapozását szolgáló adatokat) bizalmasan, a vonatkozó jogszabályokkal és egyetemi szabályzatokkal, különösen az Egyetem Adatvédelmi Szabályzatával összhangban kell kezelni.

(2) A személyes adatot vagy más, titoknak minősülő adatot kezelő vagy feldolgozó személyt titoktartási kötelezettség terheli, amelyet az Egyetem – többek között – titoktartási nyilatkozat aláírásával biztosít.

(3) A külső partnerek titoktartási kötelezettségére jelen szabályzat 30. §-a irányadó.

---

[5] *A módosítást a Szenátus 2018. december 20-ai ülésén fogadta el. Hatályos: 2018. december 20. napjától.*

[6] *A módosítást a Szenátus 2018. december 20-ai ülésén fogadta el. Hatályos: 2018. december 20. napjától.*

(4) A titoktartási kötelezettség nem terjed ki a közérdekű adatokra, a közérdekből nyilvános adatokra, valamint arra az esetre, ha az adatok közlését (továbbítását vagy nyilvánosságra hozatalát) jogszabály vagy a titok jogosultja jogszerűen elrendeli.

(5) Az informatikai szolgáltatásokból adatok továbbítása, vagy az ahhoz való hozzáférés az adott szolgáltatás adatgazdájának engedélyével, a vonatkozó jogszabályokkal és egyetemi szabályzatokkal, különösen az Egyetem Adatvédelmi Szabályzatának V. fejezében foglalt eljárásrendekkel és a Pécsi Tudományegyetem a közérdekű adatok nyilvánosságra hozataláról és a közérdekű adatok megismerésére irányuló igények teljesítésének rendjéről szóló szabályzata valamint az Egyetem által kötött szerződésekkel összhangban lehetséges.

Ügyfélszolgálat / incidenskezelés és egyszerű változáskezelés

10.§ (1) Az IIG ügyfélszolgálatot működtet, amelyen a bejelentéseket telefonon, e-mailben, vagy az önkiszolgáló ügyfélszolgálati rendszeren keresztül fogadja. Az ügyfélszolgálat minden bejelentést regisztrál.

(2) A bejelentés során minden esetben szükséges megadni a bejelentő nevét, elérhetőségét (telefon, e-mail) és az egyetemi azonosítóját (EHA/Neptun kód, vagy központi címtár felhasználó név).

(3) A bejelentéseknél egyértelműen meg kell adni, hogy a bejelentés melyik informatikai szolgáltatásra vonatkozik.

(4) A bejelentett incidensek és változások kezelésére priorizálva kerül sor. A priorizálás az ügyfélszolgálat feladata. Több incidens, illetve módosítási igény fellépésekor a magasabb prioritású megoldása elsőbbséget élvez.

(5) Az incidensek, illetve a módosítások lezárásáról a bejelentőt az ügyfélszolgálat minden esetben 30 napon belül tájékoztatja.

Rendelkezésre állás és üzletmenet folytonosság

11.§ (1) Az IIG a központi informatikai kiszolgáló infrastruktúrát és az azon futó szolgáltatásokat úgy üzemelteti, hogy azok rendelkezésre állása elérje az éves 99,9%-ot.

(2) A szükséges rendelkezésre állás eléréséhez a megfelelő háttérszolgáltatások (erősáramú betáplálás, klimatizálás, tűzoltórendszerek, stb.) üzemeltetése a Műszaki Szolgáltatási Igazgatóság feladata.

(3) A kiszolgáló infrastruktúra és a szolgáltatások tervezett karbantartásait minden esetben a hivatali időn kívüli időpontra szükséges időzíteni (munkaidő: munkanapokon 6:00 és 18:00 óra között).

(4) Minden szolgáltatás esetében az adatgazda feladata egy olyan, minimum heti 3 órás időintervallum kijelölése, amikor az adott szolgáltatás előzetes egyeztetés nélkül karbantartási célokból (például mentés) leállítható. Amennyiben az adott szolgáltatás adatgazdája a karbantartási időablakot nem határozza meg, úgy azt az IIG határozhatja meg.

(5) A karbantartások tervezhetősége végett minden héten, szombatról vasárnapra virradó éjszaka, a szombat este 22:00 és a vasárnap hajnali 5:00 óra közötti időintervallumban szükséges kijelölni a (4) bekezdésben megfogalmazott karbantartási időablakot.

(6) A karbantartási időablakon belül a kiszolgáló infrastruktúrán és a szolgáltatásokon olyan karbantartás végezhető, mely akár a teljes infrastruktúra leállásával is járhat.

(7) Lehetőség szerint a szolgáltatás kieséssel járó, karbantartási időablakban végzett karbantartási munkákat a szolgáltatás leállítása előtt 24 órával szükséges meghirdetni.

(8)[7] Vis maior esetekben a leállást nem szükséges 24 órával előre meghirdetni, azonban lehetőség szerint a leállás előtt a szolgáltatások felhasználóit a legnagyobb körben értesíteni szükséges.

(9) A szolgáltatás kieséssel járó karbantartási munkákról az IIG a szolgáltatás kiesésben érintett informatikai szolgáltatások adatgazdáit értesíti, a felhasználók értesítése az adatgazdák feladata.

(10) Az (5) és a (8) bekezdésekben meghatározott leállások az éves rendelkezésre állás idejét nem befolyásolják.

(11) Az egyes szolgáltatásokra vonatkozó karbantartási időablakok pontos időpontját az IIG a weboldalán közzéteszi.

(12) Az adatgazdáknak minden informatikai szolgáltatás esetében ki kell dolgozni egy olyan kockázatelemzést, amely az adott informatikai szolgáltatás részleges vagy teljes kiesésének, kimaradásának az Egyetem működésének képességére tett hatásait tartalmazza. Külön kell kezelni a szolgáltatás elérhetetlenségéből, illetőleg az adatok sérülésből származó hatásokat. A kockázatelemzési dokumentum előállítása és karbantartása a szolgáltatás adatgazdájának feladata, melyhez a műszaki adatok biztosítása a szolgáltatás üzemeltetőjének feladata.

(13) Minden informatikai szolgáltatás esetében az adott szolgáltatás adatgazdájának szükséges kidolgozni az üzletmenet folytonossági tervet.

(14) Az üzletmenet folytonossági tervnek tartalmaznia kell minden olyan információt, ami alapján az adott szolgáltatás felhasználói a munkájukat a szolgáltatás kiesése esetén is tovább tudják folytatni akár lassabb eljárásban, vagy akár papír alapú adminisztrációval.

(15) Minden szolgáltatás esetében a szolgáltatás üzemeltetőjének reaktív és preventív intézkedéseket szükséges tenni a szolgáltatás működésének zavartalansága érdekében. Ezek lehetnek általános és az adott szolgáltatásra speciálisan jellemző feladatok, így különösen:

a) igény szerinti újraindítás,
b) javítócsomagok, patchek, fixek, verziók telepítése,
c) jelszavak és hozzáférési kódok rendszeres cseréje,
d) naplóállományok rendszeres kiértékelése.

---

[7] *A módosítást a Szenátus 2018. december 20-ai ülésén fogadta el. Hatályos: 2018. december 20. napjától.*

(16) A (3) bekezdésben meghatározott tevékenységek közül a szolgáltatás kieséssel járó feladatokat az adott szolgáltatásra vonatkozó karbantartási időablakban szükséges megtenni.

Informatikai szolgáltatások tervezése, fejlesztése és bevezetése

12.§ (1) Az informatikai szolgáltatásokat – amennyiben a szolgáltatásnyújtás személyes adatok kezelésével jár együtt – úgy kell megtervezni, fejleszteni, beszerezni és bevezetni, hogy az az Infotv. és az adatkezelésre vonatkozó más szabályok alkalmazása során biztosítsa az érintettek magánszférájának védelmét (beépített adatvédelem elve).

(2) Az informatikai szolgáltatások fejlesztésére vonatkozó igényt minden esetben az IIG ügyfélszolgálatán, e-mailen, vagy az önkiszolgáló ügyfélszolgálati rendszerben kell jelezni. A telefonon, illetve nem az ügyfélszolgálaton jelzett igény az írásos megkeresést megelőzően nem kezelhető.

(3) Minden informatikai fejlesztési igénynek tartalmaznia kell egy átfogó működési leírást, koncepciót. A fejlesztési igényeket minden esetben az érintettség, a hatás és a sürgősség alapján priorizálni kell. A priorizálás jelen szabályzat **4. számú mellékletében** meghatározottak alapján történik.

(4) Új informatikai szolgáltatások csak abban az esetben vezethetők be, amennyiben jelen szabályzatnak megfelelnek.

(5) A tervezési (specifikációs) szakaszban részletesen le kell írni a megoldandó feladatot, definiálni kell a feladat határait, illetve azt is meg kell határozni, hogy a fejlesztésnek mi nem célja az adott témakörben. Meg kell határozni az érintett adatok, felhasználók, szervezeti egységek és egyéb alkalmazások körét. A specifikáció kizárólag az ügyfél oldalon felmerülő igények, elvárt funkcionalitások pontos meghatározását tartalmazza. A specifikációban meg kell fogalmazni sikerkritériumokat, illetve az átvétel feltételeit is. A fejlesztési specifikáció elkészítéséért az adott fejlesztéshez az igénylő és az IIG által delegált munkatárs felel. A specifikáció tartalmi elemeit jelen szabályzat **5. számú melléklete** tartalmazza.

(6) Az Egyetemen informatikai szolgáltatások fejlesztése csak megfelelő specifikáció rendelkezésre állása esetén kezdhető meg. A (4) bekezdésben meghatározott specifikációt a fejlesztés megkezdése előtt a megrendelőnek/igénylőnek el kell fogadnia.

(7) A fejlesztésekben résztvevők személyét és feladatait minden esetben egy egyedi feljegyzésben kell rögzíteni, amely feljegyzés elkészítése az Alkalmazás- és Szolgáltatásfejlesztési Osztály vezetőjének a feladata.

(8) Új informatikai szolgáltatás az adatgazda kijelölése és az adott szolgáltatásra vonatkozó 5. § (7) bekezdésben hivatkozott adatlap hiánytalan kitöltése után vezethető be.

(9) Külső partner által fejlesztett, vagy szállított informatikai szolgáltatásokkal szemben támasztott elvárások megegyeznek a belső forrásokkal történő fejlesztésekkel szemben támasztott elvárásokkal.

(10) Az Egyetemen olyan informatikai szolgáltatás nem helyezhető éles üzembe, melynek üzemeltetését az Egyetem saját hatáskörben nem tudja elvégezni, vagy nem rendelkezik megfelelő támogatási szerződéssel és annak fenntartásához szükséges pénzügyi forrásokkal.

(11) Amennyiben az Egyetem működéséhez olyan informatikai szolgáltatás bevezetése szükséges, amely üzemeltetéséhez a belső erőforrás (személyzet, szaktudás, stb.) nem áll rendelkezésre, úgy a szükséges belső erőforrásokat biztosítani szükséges. Az üzemeltetői erőforrások biztosításáért a Kancellár felelős.

(12) Minden fejlesztési tevékenységet a szolgáltatás éles példányától elkülönülten kell végezni.

(13) Egyetemi fejlesztésű vagy vásárolt szolgáltatás csak sikeres funkcionális teszt után állítható éles üzembe. A funkcionális tesztnek minden paraméterre és funkcióra, valamint tipikus felhasználási mintára ki kell terjednie. A funkcionális tesztről írásos jegyzőkönyvnek kell készülnie, melynek az összes mért és ellenőrzött paramétert és funkciót tartalmaznia kell.

(14) Egyetemi fejlesztésű vagy vásárolt szolgáltatás csak végfelhasználó oktatás után állítható éles üzembe. Az oktatás megvalósulhat a szállító, kulcsfelhasználók és az üzemeltető személyzet által egyaránt. Az oktatás módját – távoktatás, elektronikus tananyag, tájékoztató körlevél, stb. – a szolgáltatások bevezetése során szükséges meghatározni.

(15) Amennyiben a bevezetés előtt az adott szolgáltatással kapcsolatban terhelésre vonatkozó elvárások is megfogalmazásra kerültek, úgy az éles üzembe állítást terheléses tesznek is meg kell előznie.

(16) Minden új szolgáltatás csak a szolgáltatás igénylője általi jóváhagyás után állítható éles üzembe.

Jogszabályi megfelelőség és a felelősség szabályozása

13.§ (1) Az informatikai szolgáltatások igénybevétele során elkövetett szabálysértésekért, illetve jogsértésekért a szolgáltatást igénybevevő munkajogi, polgári jogi és büntetőjogi felelősséggel tartozik.

(2) A szolgáltatások igénybevevőit a jelen szabályzatban leírtak megsértése esetén az alábbi szankciók terhelhetik, amelyekről az informatikai igazgató a Jogi Főosztály bevonásával dönt

a) a szolgáltatás korlátozása,
b) szolgáltatás megtagadás (kizárás a szolgáltatásból),
c) szervezeti integritást sértő esemény kezelését célzó eljárás kezdeményezése,
d) a munkáltatói intézkedés (pl. kártérítési eljárás) kezdeményezése,
e) szabálysértési vagy büntetőeljárás kezdeményezése,
f) hallgatói fegyelmi eljárás kezdeményezése.

(4) A szolgáltatások igénybe vevőinek szankcionálása csak akkor történhet meg, ha a szolgáltatás-, vagy alkalmazásgazda dokumentálta a szankció elrendelését kiváltó eseményt, incidenst, vagy egyéb módon a cselekmény bizonyítható.

(5) Az IIG nem felel a felhasználók által elkövetett jogsértésekért és hatósági megkeresés esetén a jogszabályban előírt adatokat az adott felhasználóval kapcsolatban az Egyetem adatvédelmi szabályzatban meghatározottak szerint ki kell adnia.

IV.fejezet
Informatikai biztonság

14.§[8] (1) Az Egyetem szervezeti egységei által kezelt informatikai infrastruktúra védelmét a szolgáltatás vagy alkalmazásgazdáknak 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.

(2) 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) a belső személyzetre és a külső partnerekre,
i) az MSZ OSI 7498-1 szabványban meghatározott nyílt rendszerek architektúrája minden rétegére, azaz mind a számítástechnikai infrastruktúra, mind az informatikai alkalmazások szintjén.

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

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

(5) A kockázatelemzés végrehajtásához az Egyetem Belső Kontroll Kézikönyvében meghatározottak alapján szükséges eljárni.

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

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

(8) A személyes adatok megfelelő szintű biztonságának garantálása érdekében az Egyetem megfelelő technikai és szervezési intézkedéseket hajt végre, ideértve különösen a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének biztosítását, integritását, rendelkezésre állását, ellenálló képességét, valamint egy incidens esetén a személyes adatokhoz való hozzáférés és az adatok rendelkezésre állásának kellő időben való visszaállítását.

---

[8] *A módosítást a Szenátus 2018. december 20-ai ülésén fogadta el. Hatályos: 2018. december 20. napjától.*

(9)

(10) A részletes adatbiztonsági intézkedéseket**, *i***deértve esetlegesen a személyes adatok álnevesítését és titkosítását, valamint az adatbiztonsági intézkedések hatékonyságának rendszeres tesztelésére, felmérésére és értékelésére szolgáló eljárást – jelen szabályzat rendelkezéseivel összhangban – a 3. § 2. pont szerinti szolgáltatás leírások tartalmazzák. A konkrét adatbiztonsági intézkedéseket az Egyetem a tudomány és technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembe vételével választja meg. A biztonság megfelelő szintjének meghatározásakor kifejezetten figyelembe kell venni az adatkezelésből eredő olyan kockázatokat, amelyek különösen a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítéséből, elvesztéséből, megváltoztatásából, jogosulatlan nyilvánosságra hozatalából vagy az azokhoz való jogosulatlan hozzáférésből erednek.

Vezetői elkötelezettség

15.§ (1) Minden szervezeti egység vezetője közreműködik az informatikai biztonság kultúrájának kialakításában és fenntartásában.

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

(3) Az informatikai biztonsági intézkedések megvalósításához szükséges erőforrások biztosítása az Egyetem vezetőinek a felelőssége.

Az informatikai szolgáltatásokkal kapcsolatos adatvagyon feletti rendelkezés

16.§ (1) Az Egyetem valamennyi informatikai szolgáltatásának intézmény-specifikus konfigurációs adatai és beállításai (minden olyan konfigurációs komponens, ami a vásárolt szolgáltatásban található állapottól eltér) felett az Egyetem kizárólagos rendelkezési joggal bír. Ezen adatok kezelése, felhasználása vagy az azokkal való bármilyen más rendelkezés kizárólag az Egyetem engedélyével lehetséges, amelyről a vonatkozó szerződésben rendelkezni kell.

(2) A szolgáltatásokban tárolt személyes és más adatok feletti rendelkezés jogára az adott adattípusra vonatkozó jogszabályok és egyetemi szabályzatok, különösen az Egyetem adatvédelmi szabályzata és a közérdekű adatok nyilvánosságára vonatkozó szabályok irányadóak.

Jogosultsági szintek meghatározása, hozzáférés szabályozása

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

(2) A szolgáltatásainak igénybevételéhez, az igénybevételt megelőzően a szolgáltatás adatgazdája tanfolyam/oktatás és/vagy vizsga teljesítését írhatja elő. A kritériumok teljesítésének költsége a hozzáférést igénylő szervezeti egységét terheli.

(3) A jogosultsági szintek, valamint a felhasználóknak kiosztott jogosultságok ellenőrzése az adatgazdák feladata, amelyhez az IIG adatszolgáltatást nyújt.

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

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

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

(7) Informatikai szolgáltatásokhoz módosítást és védett 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 (például egységen belüli közös hálózati meghajtó elérése közös használatú számítógépekről) rendelkezhet jogosultsággal.

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

(9) 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 informatikai igazgató engedélyével, indokolt esetben tehető.

(10) A (9) bekezdésben megfogalmazottakon túl lehetőség van szerződések alapján létrejött ún. föderációs azonosítási rendszerek (például eduID) használatára, azonban ilyen szolgáltatások esetében is az egyetemi felhasználók azonosítását a központi címtár alapján kell megoldani.

Eljárás a dolgozó közalkalmazotti jogviszonyának létesítése, megszűnése, valamint munkakörváltozása esetén

18.§ (1) Közalkalmazotti jogviszonyt létesítő dolgozó esetén az automatikusan létrejövő felhasználói azonosítón és az automatikusan hozzárendelésre kerülő szolgáltatásokon (eduroam hálózat hozzáférés, email cím) kívül minden informatikai hozzáférést igényelni szükséges.

(2) Hozzáférés igénylés nélkül nem létesíthető, kizárólag előterjesztett kérelem formájában igényelhető.

(3) A dolgozó közalkalmazotti jogviszonyának megszűnése esetén minden informatikai szolgáltatás esetében az üzemeltetői, fejlesztői és felhasználói jogosultságokat, illetve az ilyen tevékenységet lehetővé tevő belépési kódokat a szolgáltatás üzemeltetőjének vissza kell vonni.

(4) A közalkalmazotti jogviszony megszűnése, vagy munkakörváltozás esetén a mindenkor hatályos HR Kézikönyv útmutatása alapján szükséges eljárni.

(5) A késedelmes jelzésből eredő károkért az IIG nem vállal felelősséget.

(6) Amennyiben a jelzés nem tartalmaz ellentétes igényt, úgy a felhasználó minden jogosultsága megvonásra kerül. A tévesen kitöltött távozási lap alapján törölt jogosultság csak a hozzáférés újbóli igénylése után állítható vissza.

(7) A kilépő dolgozó az informatikai szolgáltatásokban a (kizárólag) személyes adatainak elérésére szolgáló belépési kódjait a munkáltatójának eseti engedélye alapján a távozást követő maximum 180 napig megtarthatja.

Fizikai biztonság

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

(2) A géptermeket vagyonvédelmi célból kamerás megfigyelőrendszerrel szükséges ellátni és a vonatkozó jogszabályok szerint kell azokat üzemeltetni.

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

(4) A géptermek villám- és túlfeszültségvédelmét biztosítani kell.

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

(6) A telephelyi kábelrendezőknek, telefonközpontoknak, gerinchálózati eszközöknek helyt adó helyiségeket (egyéb helyiségek) biztonsági zárral kell ellátni. Ezen helyiségekbe történő belépéseket az adott helyiséghez tartozó, belépések naplózására szolgáló füzetbe szükséges rögzíteni.

(7) Mind a géptermek, mind a telephelyi egyéb helyiségek esetében a bejárati ajtónak zárt állapotban kell lennie, nyitva tartásuk csak a közlekedés idejére engedélyezett.

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

(9) A géptermekbe való belépési jogosultságot az IIG igazgatója, vagy az üzemeltetésért felelős főosztályvezetője engedélyezheti, a helyiségek és a végezhető munka felsorolásával. A belépési jogosultsággal rendelkezők e jogosultságukat nem ruházhatják át másra.

(10) Amennyiben a géptermekbe belépési jogosultsággal rendelkező egyetemi polgár jogosultságát átruházza vagy a jogosultságával egyéb módon visszaél, továbbá amennyiben a géptermekbe 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.

(11) 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.

(12) A (11) bekezdésben megfogalmazott erősáramú és gépészeti berendezéseknek redundánsnak kell lenniük, azaz egy meghibásodása nem okozhatja a helyiségben üzemelő eszközök leállását.

(13) A géptermekben és egyéb helyiségekben minden olyan munkavégzés, ami az informatikai szolgáltatásokat vagy azok működését veszélyezteti, csak előzetes egyeztetés alapján, felügyelet mellett végezhető.

(14) Az egyeztetést, a munkálatokat végző szervezeti egység vagy cég, és az IIG üzemeltetésért felelős főosztályvezetője vagy osztályvezetője végzi.

(15) A helyiséget kiszolgáló gépészeti és erősáramú berendezések működését veszélyeztető munkák csak az IIG üzemeltetésért felelős főosztályvezetője vagy osztályvezetője előzetes engedélyével folytathatók.

(16) 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.

(17) A géptermeket és egyéb helyiségeket kiszolgáló gépészeti és erősáramú rendszerekre külön karbantartási tervet kell készíteni, amelyet a Műszaki Szolgáltatási Igazgatóság üzemeltetésért felelős vezetője állít össze és gondoskodik a végrehajtásáról. A tervet az IIG üzemeltetésért felelős vezetői véleményezik és hagyják jóvá.

(18) 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.

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

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

(21) Az informatikai célú helyiségekkel kapcsolatos kérdésekben, a ki- és átalakítás koordinációjáért, a szakmai biztonsági szempontok betartásáért az adott helyiséghez tartozó szervezeti egység vezetője, és IIG üzemeltetésért felelős vezetője a felelős.

(22) Az Egyetem területén kifejezetten informatikai szolgáltatások biztosítását lehetővé tévő, informatikai eszközöknek helyt adó „informatikai helyiségekhez”, azaz géptermekhez az informatikai igazgató által hitelesített, fényképes igazolvánnyal rendelkező közalkalmazott férhet hozzá fizikailag, a helyiségben található eszközök üzemeltetését kizárólag ezen személyek végezhetik. Egyéb személyek

kizárólag ezen közalkalmazottak felügyelete mellett léphetnek és tartózkodhatnak ezekben a helyiségekben.

(23) A géptermekben és egyéb 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.

(24) A géptermeken és egyéb 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 IIG üzemeltetéséért felelős vezetőinek előzetes engedélyével lehet.

Eszközbiztonság

20.§ (1) Az informatikai eszközökért a mindenkori leltárfelelős, az Egyetem Leltározási és Leltárkészítési Szabályzatában meghatározottak szerint felel.

(2) Minden felhasználónak kötelessége az informatikai eszközök és adatok védelme.

(3) A telephelyekről kivitt eszközök és adatok használata során bekövetkező károkért az a személy viseli a felelősséget, aki az eszközt a telephelyről kivitte. A telephelyen kívüli használat, munkavégzés során mindazon elvek és gyakorlat követendő, amelyeket a telephelyen belüli használat esetén is irányadók.

Eszközök biztonságos megsemmisítése vagy újrahasznosítása

21.§ (1) A feleslegesség vált, használhatatlan, vagy elavult eszközök selejtezése az Egyetem felesleges vagyontárgyak hasznosításának, selejtezésének szabályzatában foglaltak szerint történik.

(2) Működőképes, még gazdaságosan üzemeltethető, más területen felhasználható eszközöket selejtezni tilos.

(3) Speciális eszközök selejtezése esetén az üzemeltető gondoskodik a szakszerű elhelyezésről.

(4) Az eszközök selejtezésénél a selejtezést indító feladata és felelőssége az eszközökön esetlegesen tárolt adatok fizikai törlése, amelyhez igény esetén az IIG segítséget nyújt.

Dokumentálás

22.§ (1) 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.

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

Biztonsági mentések

23.§ (1) Minden informatikai szolgáltatás 5. § (7) bekezdésben 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).

(2) Az elvárásoknak megfelelő mentési módszerek technológiai kidolgozása az IIG üzemeltetésért felelős vezetőinek a feladata.

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

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

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

(6) 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.

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

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

(9) 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.

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

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

Biztonsági mentések adathordozóinak kezelése

24.§ (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.

Informatikai szolgáltatások közötti adatcsere

25.§ (1) Az informatikai szolgáltatások esetében az automatikus adatcserét lehetővé tevő kapcsolatok létesítéséhez érintett szolgáltatások adatgazdáinak hozzájárulása szükséges. A hozzájárulás megadása előtt részletezni kell az elérendő adatok körét, valamint az adatkezelési célt és az alkalmazott informatikai megoldást, különös tekintettel a jogosulatlan adatcserét kizáró biztonsági megoldásokra.

(2) Az adatcsere környezetét, technológiai megvalósítását dokumentálni kell.

(3) Az adatcserének minden esetben naplózottan kell megtörténnie, minimálisan az adatcsere tényét és időpontját rögzíteni szükséges.

(4) Személyes adatokat érintő adatcsere esetén az Egyetem Adatvédelmi Szabályzatának 15. §-a megfelelően alkalmazandó.

Monitorozás

26.§ (1) Az IIG által üzemeltett informatikai szolgáltatások esetében az IIG automatikus szolgáltatás monitorozó komponenseket üzemeltet.

(2) Az esetleges meghibásodásokról, szolgáltatás kiesésekről az üzemeltetőket a monitorozó rendszer automatikusan e-mailben vagy SMS-ben tájékoztatja.

(3) Az IIG vezetőjének felelőssége a monitorozó és tájékoztató rendszer működéséhez szükséges források biztosítása (például mobiltelefonok, mobilinternet előfizetések, stb.).

(4) A Kancellária a weboldalán áttekintő tájékoztatást nyújt az egyes szolgáltatások állapotáról, valamint ezen a felületen hirdeti meg az esetleges tervezett leállásokat is.

Hálózat biztonság

27.§ (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 szabályzatát (HBONE AUP) betartani, amely elérhető a https://niif.hu/hu/aup címen.

(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 3. § 2. pontban nevesített szolgáltatás leírások tartalmazzák. A naplózási intézkedések során figyelembe kell venni az adatbiztonsági követelmények [14. § (8)-(10)] 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 e szabályzat 8-9. §-ait megfelelően alkalmazni kell.

(8) Kiemelt 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 (például HTTPS) keresztül kell biztosítani.

Biztonsági események és gyengeségek jelentése és kezelése

28.§ (1) Az adott informatikai szolgáltatás szolgáltatásgazdájának a felelőssége a publikált, ismert sérülékenységek elleni védekezés megvalósítása. A publikált, ismert és a gyártó által kritikusnak minősített sérülékenységek elleni védekező intézkedés az észlelést követő első munkanapon végrehajtandó, a végrehajtást nem szükséges az adott szolgáltatás karbantartási időablakához igazítani. Amennyiben a végrehajtás szolgáltatás kieséssel jár, úgy erről széleskörű tájékoztatást szükséges közzétenni.

(2) Az informatikai szolgáltatások felhasználása közben tapasztalt gyengeségek jelentése a szolgáltatás működőképességének fenntarthatósága érdekében minden felhasználónak kötelessége. Ennek elmulasztása vagy a gyengeség kihasználása az Egyetem működésének veszélyeztetését jelenti, ezért ebben az estben az Egyetem megteszi a szükséges intézkedéseket.

(3)

(4)[9] Aki az Egyetem informatikai szolgáltatásaival kapcsolatban ***személyes adatokat érintő incidenst (***adatvédelmi incidenst***)*** észlel, köteles ***haladéktalanul megtenni az Adatvédelmi Szabályzat 23. §-ban rögzített intézkedéseket.***

[9] *A módosítást a Szenátus 2018. december 20-ai ülésén fogadta el. Hatályos: 2018. december 20. napjától.*

V.fejezet
Külső kapcsolatok

Kapcsolattartás szakmai érdekközösségekkel

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

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

A külső partnerek

30.§[10] (1) A külső partnerekkel történő kapcsolattartás szabályai:

a) Személyes vagy intézményi adatok kiadása~~,~~ csak a hatályos jogszabályoknak megfelelően történhet.
b) Az átadott adatok jogi és technikai védelméért a szerződő fél tartozik felelősséggel.
c) A kapcsolattartó információbiztonsági kérdésekben az informatikai igazgatótól, a személyes adatok védelmével kapcsolatos kérdésekben az egyetemi adatvédelmi tisztviselőtől, egészségügyi adatok esetén az egészségügyi adatvédelmi tisztviselőtől tájékoztatást vagy állásfoglalást kérhet.

(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 adatfeldolgozói jogviszony keretében, erre vonatkozó írásos szerződés (adatfeldolgozói megállapodás) alapján lehetséges. Az adatfeldolgozói megállapodásra az Egyetem Adatvédelmi Szabályzatának 4. §-a alkalmazandó.

(3) Külső partnerek egyetemi informatikai szolgáltatásokhoz történő hozzáférését a vonatkozó kancellári utasítás szabályozza.

Átmeneti rendelkezések

31.§ (1) Az 5. § (2) bekezdésben meghatározott nyilvántartásokat a szabályzat hatálybalépést követő ötödik hónap első napjáig létre kell hozni és a feltöltésükhöz szükséges felméréseket, a hiteles adatokkal való feltöltést el kell végezni.

(2)[11] A szolgáltatások leírását és az adatlapokat az adatgazdák készítik el és töltik fel az IIG által üzemeltetett nyilvántartásba.

---

[10] *A módosítást a Szenátus 2018. december 20-ai ülésén fogadta el. Hatályos: 2018. december 20. napjától.*

[11] *A módosítást a Szenátus 2018. december 20-ai ülésén fogadta el. Hatályos: 2018. december 20. napjától.*

(3) Azon szervezeti egységek esetében, melyek nem rendelkeznek a Kancellária által delegált területi informatikai referenssel, a (2) bekezdésben meghatározott feladatok végrehajtásáért az adott szervezeti egység vezetője felelős.

(4) A szabályzatban hivatkozott Kancellári utasításokat legkésőbb a szabályzat elfogadását követő negyedik hónap végéig kell elkészíteni és kiadni.

Záró és hatályba lépő rendelkezések

32.§ (1) Jelen szabályzat a Szenátus által történő elfogadásának napján lép hatályba. Jelen szabályzat hatályba lépésével egyidejűleg hatályát veszíti a Pécsi Tudományegyetem informatikai üzemeltetési szabályzata, valamint a Pécsi Tudományegyetem informatikai biztonsági szabályzata.

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

Pécs, 2017. május 25.

Dr. Bódis József sk.	Jenei Zoltán sk.
rektor	kancellár

Záradék:

A Szabályzatot a Szenátus 2017. május 25. napján tartott ülésén 62/2017. (05.25.) számú határozatával fogadta el.

A Szabályzat módosítását a Szenátus 2018. december 20. napján tartott ülésén 165/2018. (12. 20.) számú határozatával fogadta el. A módosítások a Szenátus által történő elfogadás napján lépnek hatályba.

Dr. Miseta Attila	Jenei Zoltán
Rektor	Kancellár

PTE Informatikai Szabályzat 1. számú melléklete

A szoftverekről, alkalmazásokról és szolgáltatásokról vezetett nyilvántartáshoz szükséges attribútumok

1. név;
2. leltári számát (amennyiben van);
3. a szoftver gyártóját (amennyiben releváns);
4. a forgalmazót (amennyiben releváns);
5. bevezetés, beszerzés, vagy bérlés (leltárba kerülés) évét;
6. verzióját (amennyiben releváns);
7. kapcsolódó szolgáltatásokat (pl. szoftverkövetés);
8. beszerzési, vagy bevezetési árat;
9. havi, vagy évi szoftverkötési díjat (amennyiben értelmezhető);
10. letölthető telepítőkészlet elérhetőségét (amennyiben értelmezhető);
11. felhasználói számot (amennyiben értelmezhető, egyedi, vagy konkurens);
12. az alkalmazás, vagy szolgáltatás célját, feladatát, leírását;
13. bevezetés dátumát;
14. megvásárolt licencek számát és típusát (amennyiben releváns);
15. elérhetőségét (lokális, intranet, internet);
16. felhasználó szervezeti egységet (amennyiben releváns);
17. dokumentációs rendet;
18. mentési- és archiválási rendet;
19. adatgazdát;
20. központi címtár alapú azonosítás alkalmazhatósága;
21. egyebeket (pl. az adatkapcsolatokat más rendszerekkel).

PTE Informatikai Szabályzat 2. számú melléklete

Az informatikai eszközbeszerzések során alkalmazott kategóriák

1. asztali PC
2. notebook
3. nyomtatók
4. multi-funkciós eszközök
5. projektor
6. perifériák
7. hálózati eszközök

PTE Informatikai Szabályzat 3. számú melléklete

Üzemeltetési dokumentáció

1) Bevezetés
   a) verzió, lezárás dátuma.
2) A szolgáltatás alapfunkciója
3) A szolgáltatás architektúrája
   a) az adatfolyam,
   b) külső és belső kapcsolatok,
   c) elhelyezés, hardver és operációs rendszer környezet.
4) Üzemeltetési feladatok
   a) rendszeres üzemeltetési feladatok,
      i) rendszeres karbantartási feladatok;
      ii) eseti üzemeltetési feladatok;
      iii) leállítás, indítás;
   b) jogosultság kezelés.
5) Üzemmenet felügyelet, eseménykezelés
   a) szolgáltatási szint paraméterek és felügyeletük,
   b) az alkalmazás üzemképességi felügyeletének eszközei,
      i) rendszer SMS-ek;
      ii) szolgáltatás által küldött mailek;
      iii) az alkalmazás saját felügyeleti felülete;
      iv) a szolgáltatás által generált naplóállományok helye és elemzése, megőrzési ideje;
   c) incidenskezelés,
   d) biztonsági mentések,
   e) katasztrófa elhárítási terv (DRP),
   f) üzletmenet folytonossági terv (BCP).
6) Az üzemeltetés személyi feltételei
   a) az alkalmazás üzemeltetéséhez szükséges ismeretek,
   b) az alkalmazás használatához szükséges ismeretek,
   c) kiemelt felhasználók, szakmai adminisztrátorok, felelősségi körök,
   d) támogató személyzet és a támogatás szintjei.

PTE Informatikai Szabályzat 4. számú melléklete

A fejlesztési igények priorizálása

Érintettség/Hatás: Az adott szolgáltatást igénybevevők érintettsége alapján a felhasználók milyen széles körét érinti a változás.
Sürgősség: A szolgáltatás/alkalmazás további használhatósága alapján az adott változtatási igény milyen mértékben érinti a szervezet alaptevékenységét, illetve ha kiemelt felhasználó (pl.: rektor, kancellár, dékán, stb.) az érintett.

Érintettségi szintek:
1. szint: A fejlesztési igény egy felhasználót érint.
2. szint: A fejlesztési igény több felhasználót vagy adott szakterületen dolgozókat érint.
3. szint: A fejlesztési igény a szervezet egészét érinti.

Sürgősségi szintek:
1. szint: nem a napi munkavégzéssel/finanszírozással van összefüggésben a fejlesztési igény, vagy a napi munkavégzést kis mértékben érinti.
2. szint: a napi munkavégzést nagymértékben érinti a fejlesztés (pl.: változik a dokumentációs folyamat).
3. szint: a napi munkavégzést érintő igény, a felhasználó az adott részfeladatot nem tudja ellátni a korábban megszokott módon, beavatkozás (oktatás, tájékoztatás) finanszírozási veszteség érheti az Egyetemet, vagy a változás a szolgáltatás teljes egészére hatással van, a napi munkavégzést akadályozza (pl.: új, kötelező mező egy alkalmazásban, melynek feltöltése nehézkes).

Prioritási szintek: 1=NINCS, 2=ALACSONY, 3=KÖZEPES, 4=MAGAS, 5=KRITIKUS

Érintettség/Sürgősség	Sürgősség 1. szint	Sürgősség 2. szint	Sürgősség 3. szint
Érintettség 1. szint	Prioritás1	Prioritás2	Prioritás3
Érintettség 2. szint	Prioritás3	Prioritás4	Prioritás5
Érintettség 3. szint	Prioritás4	Prioritás5	Prioritás5

PTE Informatikai Szabályzat 5. számú melléklete

A fejlesztési specifikáció (rendszerterv) tartalma

1. Fejlesztés célja, várt jövőbeli előnyök *
2. Feladat általános leírása, koncepció *
3. Sikerkritériumok *
4. Kockázatelemzés
5. Kapacitáselemzés
6. IT biztonsági és megfelelőségi elemzés
7. Gazdasági elemzés
8. Folyamatábra, folyamat leírása *
9. Adatok származási helye (ki, mikor szolgáltatja, amennyiben releváns) *
10. Mentendő adatok, mentési gyakoriság (amennyiben releváns) *
11. Speciális esetek
12. Kimutatások, riportok
13. Hozzáférések, szerepkörök
14. Infrastruktúra
15. Hardver, szoftver szükségletek
16. Integrációk más szolgáltatásokkal
17. Tesztelési terv

*: kötelezően megadandó