INFORMATIKAI ÉS INFORMÁCIÓBIZTONSÁGI SZABÁLYZAT (ISZ)

A Pázmány Péter Katolikus Egyetem Egyetemi Tanácsa az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény, az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény, valamint a nemzeti felsőoktatásról szóló 2011. évi CCIV. törvény alapján, összhangban a vonatkozó kormányrendeletekben és egyéb jogszabályokban foglalt rendelkezésekkel, a Szervezeti és Működési Szabályzat mellékleteként az alábbi szabályokat alkotja.

I. rész
Általános rendelkezések

A szabályzat célja és alapelvei

1. § (1) A jelen szabályzat célja, hogy megteremtse és garantálja az Egyetem működése számára a magas színvonalú, egységes, biztonságos, stabil, fejlődőképes informatikai működés szabályozási környezetét, egyértelműen meghatározza az Egyetem által biztosított informatikai szolgáltatások határait és a kapcsolódó felelősségeket, továbbá könnyen áttekinthető módon meghatározza az informatikai működés irányelveit, az üzemeltetést végzők és a felhasználók jogait, kötelességeit, illetve a szabályoknak nem megfelelő használatból eredő következményeket, és ezáltal az Egyetem informatikai infrastruktúrájának és szolgáltatásainak felhasználói számára átfogó útmutatást nyújtson a megbízható és biztonságos használatot garantáló szabályok megismeréséhez.

A szabályzat hatálya és értelmezése

2. § (1) A jelen szabályzat hatálya kiterjed az Egyetem valamennyi szervezeti egységére, hallgatójára, munkavállalójára, és a bármely egyéb jogviszony keretében foglalkoztatott személyekre.
(2) A jelen szabályzat hatálya kiterjed az Egyetemmel jogviszonyban nem álló olyan természetes vagy jogi személyekre is, akik bármely módon igénybe veszik az Egyetem információtechnológiai szolgáltatását.
(3) Kétség esetén a rektor jogosult hitelesen értelmezni a jelen szabályzatot, és szükség esetén kibocsátani a végrehajtásához szükséges rendelkezéseket, nem csorbítva ezzel a Nagykancellárnak az Egyetem Szervezeti és Működési Szabályzatában rögzített azon jogát, hogy az Egyetem szabályzatainak hiteles értelmezésére jogosult.
(4) A jelen szabályzathoz kari kiegészítő rendelkezések csak a jelen szabályzatban kifejezetten meghatározott esetekben és terjedelemben fűzhetők. Kari kiegészítő rendelkezéssel a jelen szabályzat rendelkezéseitől csak a jelen szabályzatban kifejezetten meghatározott esetben van mód eltérni.

Értelmező rendelkezések

3. § A jelen szabályzat alkalmazásában
1. Felhasználó: Az Egyetemmel jogviszonyban álló, vagy jogviszonyban nem álló természetes vagy jogi személy, aki bármely módon igénybe veszi az Egyetem információtechnológiai szolgáltatását.
2. Adatalany: Olyan természetes személy, akiről az Egyetem bármely informatikai rendszere személyes adatot tartalmaz, illetve kezel.
3. Üzemeltetői dokumentáció: a szolgáltatáshoz szükséges hardver és szoftver komponensek, valamint azok konfigurációját és üzemeltetői útmutatást tartalmazó leírás.

4. Szoftver: A számítógépes programokon túl szoftvernek tekintendő a licence igazolás, az ún. egyéb szoftver használati megállapodás, és a gyártói támogatói megállapodás is.
5. Informatikai incidens: Minden olyan eset, amikor a felhasználó a szolgáltatás megszűnését, annak minőségi romlását, vagy ezek bekövetkezésére utaló jelenséget tapasztal.
6. Szakterületi vezető: Az Informatikai Osztály szervezeti keretein belül az egyes elkülönült szakterületek vezetői, akik irányítják és szervezik a szakterület szakmai feladatainak ellátását, illetve a szakterület feladataiból eredően szakmai szintű kapcsolattartási feladatokat látnak el a külső szervezetek felé.

Információbiztonsági politika

4. § (1) Az információbiztonsági politika célja, hogy a Felhasználók részére egységes és általános értelmezést adjon az informatikai rendszerekben kezelt adatok bizalmassága, hitelessége, sértetlensége, rendelkezésre állása és funkcionalitása biztosítása érdekében követendő irányelvekre, amelyek figyelembe vételével meghatározható az informatikai rendszerek biztonsági osztályba sorolása, kidolgozhatók a rendszer szintű informatikai biztonsági szabályozások.
(2) Az információbiztonsági politikát az Informatikai Osztály vezetőjének javaslata alapján a rektor bocsátja ki, és azt az Informatikai Osztály honlapján kell – a változáskövetés megfelelő biztosítása mellett – közzétenni.
(3) Az információbiztonsági politikát szükség szerint – de legalább évente egy alkalommal – felül kell vizsgálni.

II. rész
Szervezeti szabályok

Az Informatikai Osztály

5. § (1) Az Egyetem szervezeti egységei számára a működéshez szükséges informatikai és kommunikációtechnikai szolgáltatási, fejlesztési és koordinációs feladatokat az Informatikai Osztály látja el.
(2) Az Informatikai Osztály feladatai körében
a) az innovációt, az Egyetem céljaihoz vezető informatikai megoldások ajánlását és megvalósulását tekinti feladatának,
b) szolgáltatói feladatainak ellátására vonatkozóan az informatika pillanatnyi legjobb gyakorlatában foglaltakat tekinti általános irányelvnek, folyamatos fejlesztési célnak,
c) az egyetemi célokkal összehangolt költséghatékony gazdálkodást, annak megfelelő rendelkezésre állás biztosítását, és a legkorszerűbb biztonsági irányelveknek való megfelelést tekinti feladatának,
d) a törvényes, etikus és környezettudatos értékeket hordozó működést tekinti követendőnek.
(3) Az Informatikai Osztály feladat- és hatáskörébe tartozik, hogy
a) ellátja az Egyetem valamennyi informatikai eszközének (kliens oldal, szerver oldal, hálózat) üzemeltetését,
b) javaslatot tesz, és megvalósítja a központi infrastruktúra fejlesztését, figyelemmel az Egyetem hosszú távú érdekeire,
c) javaslatot tesz a felhasználói informatikai eszköznormatívákra, a költséghatékony eszköz portfólió kialakítása és a gazdaságos üzemeltethetőség érdekében,

d) informatikai szakértelemmel támogatja az Egyetem beszerzési tevékenységét, amelynek keretében véleményezi az informatikai beszerzési igényeket, és informatikai tárgyú szerződéseket,
e) üzemelteti az Egyetem működését támogató informatikai szolgáltatásokat, alkalmazásokat.
f) támogatást biztosít az Egyetem informatikai alapú oktatástechnikai eszközeinek használatához,
g) üzemelteti az Egyetem telephelyein található vezetékes telefonhálózatokat, alközpontjait és végberendezéseit,
h) a kezelésében lévő eszközökhöz és szolgáltatásokhoz kapcsolódóan informatikai tevékenységre vonatkozó felhasználói támogatást biztosít,
i) központi menedzsment eszközökkel biztosítja az Egyetem eszközeinek biztonságos és optimális működését,
j) létrehozza és folyamatosan karbantartja az Egyetem Informatikai Stratégiáját,
k) saját szervezetén belül kialakítja az Egyetem információbiztonsági szervezetét,
l) hazai és nemzetközi szervezetekkel, cégekkel kapcsolatot tart a feladatkörébe tartozó informatikai, telekommunikációs eszközök, szolgáltatások vonatkozásában,
m) gondoskodik a jelen szabályzat szerinti adatszolgáltatási feladatok ellátásáról,
n) gondoskodik saját szervezete szakmai színvonalának fenntartásáról, fejlesztéséről,
o) ellát minden olyan feladatot, amelyet jogszabály, egyetemi szabályzat, az Egyetemi Tanács, rektori vagy gazdasági főigazgatói utasítás a hatáskörébe utal.

6. § (1) Az Informatikai Osztály szervezetén belül az egyes szakterületekhez önálló szakterületi vezetők rendelhetők. A szakterületek vezetői irányítják és szervezik a szakterület szakmai feladatainak ellátását, illetve a szakterület feladataiból eredően szakmai szintű kapcsolattartási feladatokat látnak el a külső szervezetek felé.
(2) Az Informatikai Osztály szervezetén belül külön IT biztonsági felelős gondoskodik az informatikai és információbiztonság követelményeinek érvényesítéséről.
(3) A nem az Informatikai Osztály üzemeltetésében álló informatikai rendszerek szakmai felügyeletét (Pl. elkülönült kutatói szakrendszerek) az üzemeltető szervezeti egység vezetője látja el. A szervezeti egység vezetője gondoskodik az informatikai és információbiztonság követelményeinek érvényesítéséről. Az Informatikai Osztály vezetője jogosult az egyes szolgáltatások, rendszerek IT szabályzatoknak való megfelelőség-ellenőrzésére.
(4) Az IT által biztosított szolgáltatások színvonalának felügyeletét külön szolgáltatásmenedzser látja el. A szolgáltatásmenedzser felelős a szolgáltató és a szolgáltatás igénybevevője között a szolgáltatás tartalmának és egyéb paramétereinek egyeztetéséért, a megállapodás betartásának ellenőrzéséért.

III. rész
Informatikai rendszerek üzemeltetése

Az informatikai rendszerek biztonsági besorolása

7. § (1) Az Egyetemen működő informatikai rendszereket üzembehelyezéskor az alábbi kategóriák valamelyikébe kell besorolni
a) kritikus rendszerek („A”)
b) kiemelt rendszerek („B”)
c) normál rendszerek („C”)
d) egyéb rendszerek („D”)

(2) Az intézmény informatikai infrastruktúrája és informatikai alapszolgáltatások szempontjából kritikus rendszerek, különösen:

a) az authentikációs rendszerek (LDAP, AD)
b) a határvédelmi és hálózati forgalmi szolgáltató rendszerek (BSD, Távközlési szolgáltatók rendszerei)
c) a virtualizációt támogató rendszerek (Hyper-V, KVM)

(3) Az intézmény működése szempontjából kritikus, az intézmény egészére kiterjedő rendszerek, amelyek szenzitív, illetve (különleges) személyes adatokat tartalmaznak, és adatvédelmi szempontból kiemelt védelmet igényelnek, különösen:

a) a bér- és munkaügyi rendszer (Nexon)
b) a gazdasági, ügyviteli rendszer (SAP)
c) az iktatási rendszer (Poszeidon)
d) az ECM dokumentumkezelő rendszer
e) a tanulmányi rendszer (Neptun)
f) a központi levelező kiszolgálók
g) a központi és tárhely-kiszolgálók (szerverek, storage-ek, NAS)

(4) Az intézmény működése szempontjából kiemelt rendszerek, amelyek elsősorban technikai jellegűek, a rajtuk tárolt adatok nem személyes jellegűek, ugyanakkor működési zavaruk vagy kiesésük az Egyetem számára jelentős vagyoni vagy nem vagyoni kárt okozhat, különösen:

a) a telekommunikációs hálózat
b) a technológiai rendszerek
c) a géptermi rendszerek (pl. hűtés, UPS, aggregátor stb.)
d) a kommunikációs rendszerek
e) a honlap szolgáltató rendszerek

(5) Normál rendszerek a teljes intézmény napi működése szempontjából nem kritikus, illetőleg az intézménynek csak egyes részeire kiterjedő olyan rendszerek, amelyek indítása/üzemeltetése során központi felülvizsgálat történik, illetőleg teljes körű dokumentáció készül, különösen:

a) az interaktív kiszolgáló szerverek
b) a kutatói rendszerek alapinfrastruktúrája
c) a szuperszámítástechnika (High Performance Computing – HPC) alapinfrastruktúrája

(6) Egyéb rendszerek az előző kategóriák egyikébe sem besorolható rendszerek.

(7) Minden „A” illetve „B” besorolású rendszer esetén rendelkezni kell olyan kockázatelemzéssel, ami a rendszer által nyújtott szolgáltatások részleges vagy teljes kimaradásának az intézmény működőképességére tett hatásait tartalmazza. Külön kell kezelni a szolgáltatás elérhetetlenségéből, illetőleg az adatbázis sérüléséből származó hatásokat. A kockázatelemzési dokumentumban ki kell térni arra is, hogy milyen hatással jár az adott rendszer vagy szolgáltatás kiesése az Egyetem működési folyamataira. A kockázatelemzési dokumentum előállítása és karbantartása körében az Informatikai Osztály feladatköre csak az informatikai, és üzemeltetési kockázatokra terjed ki, a működési kockázatok megadása az adott rendszert használó szervezeti egység vezetőjének feladata.

Szolgáltatási feltételek

8. § (1) Az egyes informatikai rendszerek leírását és működtetésének legfontosabb paramétereit rendszerenként az Informatikai Osztály által kibocsátott szolgáltatási feltételek tartalmazzák.

(2) A szolgáltatási feltételek tartalmazzák:

a) az adott rendszer nevét (egyedi megnevezését),
b) a szolgáltatási feltétel dokumentum verziószámát,
c) a szolgáltatási feltétel dokumentum lezárás dátumát,
d) az adott rendszer rövid leírását / összegzés (pár mondatban, röviden összefoglalva a szolgáltatás célját, tartalmát),

e) a szolgáltatási feltétel dokumentum érvényességi idejét,
f) az adott rendszer részletes leírását [kulcs funkciók, felhasználók számára szükséges technikai leírás, paraméterek, rendszer besorolása („A–D")],
g) a rendszer szolgáltatási időszakát,
h) a használatba vétel módját [igénybe vevők köre, szolgáltatási helyszínek, kapcsolattartó/ szolgáltatás gazda elérhetősége, igénylés módja, szolgáltatásbiztosítás átfutási időtartama, szolgáltatás biztosítás feltételei (adott munkakör, adott tanszék, képzettség, stb.),
i) a rendszerrel kapcsolatos tájékoztatás módját,
j) a tervezett karbantartási időszakokat,
k) a rendelkezésre állást (%), és mérési módját,
l) a rendszerhez biztosított támogatás leírását (tartalma, elérhetősége, rendelkezésre állása),
m) a rendszerhez kapcsolódó incidens-kezelést (hol, hogyan lehet az incidenseket bejelenteni, mennyi időn belül kerül feldolgozásra a bejelentés, van-e és ha igen mekkora a javítási időablak, visszajelzés menete az incidens lezárásakor),
n) a rendszer teljesítmény- és minőségadatait - Optimális teljesítményadatok (pl.: elérési idő, válaszidő, ami értelmezhető az adott szolgáltatás esetében, stb.),
o) a változáskezelési eljárásokat,
p) a rendszerbiztonsággal kapcsolatos sajátosságokat,
q) fogalomtárat (azok a technikai, speciális kifejezések, amelyek szerepelnek a dokumentumban és magyarázatra szorulnak),
r) amennyiben az adott rendszert nem az Informatikai Osztály üzemelteti, úgy az üzemeltető megnevezését.

(3) A szolgáltatási feltételeket – az Informatikai Osztály erőforrásait figyelembe véve – az Informatikai Osztály vezetője jogosult meghatározni, illetve módosítani.
(4) A hatályos szolgáltatási feltételeket rendszerenként az Informatikai Osztály honlapján kell közzé tenni. Azonos feltételek esetén egy szolgáltatási feltétel dokumentum több rendszerre is vonatkozhat.
(5) Bármilyen informatikai rendszer működésbe helyezése csak azután történhet meg, hogy az adott rendszerre vonatkozó szolgáltatási feltételek kibocsátásra kerültek.
(6) A szolgáltatási feltételekben megadott szolgáltatási kulcsparaméterek monitorozásért az Informatikai Osztály kijelölt munkatársa a felelős. Az egyes szolgáltatási feltételek tartalmazzák az adott rendszer monitorozási feltételeit. Az egyes méréseket az Informatikai Osztály kijelölt munkatársai tekintik át. A monitorozás eredménye a szolgáltatás minőségének fejlesztését szolgálja.
(7) A szolgáltatási feltételekben előírt teljesítmény-mutatók figyelése során statisztikai értelemben vett idősorok jönnek létre, melyek elemzése az Informatikai Osztály kijelölt munkatársainak a feladata. Az ilyen módon képződött adatokat az Informatikai Osztály vezetője felhasználja a fejlesztési irányok és projektek kijelölésekor.

Üzemeltetési szabályok

9. § (1) Új rendszer üzembe helyezését a Karok és Központi szervezeti egységek vezetői írásban kezdeményezhetik az Informatikai Osztály vezetőjénél, a javasolt rendszer megjelölésével, vázlatos leírásával, és a rendszer bevezetésével elérni kívánt cél bemutatásával. A kérelemhez csatolni kell az új rendszer szolgáltatási feltételeinek tervezetét.
(2) Az Informatikai Osztály vezetője a kérelem alapján
a) gondoskodik a megjelölt rendszer bevezetéséről,
b) egyeztetést kezdeményez a kezdeményezővel a javasolt rendszer – vagy a cél elérésére alkalmas más alternatív megoldás – bevezetéséről, vagy
c) indokolt esetben a kérést elutasítja.

(3) Az Informatikai Osztály vezetője döntésének meghozatala során köteles figyelemmel lenni
a) a bevezetendő rendszer meglévő rendszerekre gyakorolt várható hatásaira, és esetleges biztonsági kockázataira,
b) a bevezetendő rendszer működtetésének költségvonzataira,
c) a bevezetendő rendszer megfelelőségére az általa elérni kívánt cél vonatkozásában.

(4) Új rendszer bevezetése esetén az Informatikai Osztály vezetője a kezdeményező egyidejű értesítése mellett kibocsátja a szolgáltatási feltételeket, az üzemeltetési dokumentációt, a rendszerkonfigurációt és a változáskezelési folyamatleírást.

(5) Az Informatikai Osztály vezetőjének elutasító döntésével szemben a kérelmező a rektorhoz fordulhat. A rektor döntésével szemben további jogorvoslatnak helye nincs.

(6) Új rendszer bevezetését megfelelő tesztelésnek kell megelőznie, amit az Informatikai Osztály illetékes munkatársa ellenőriz.

(7) Bármely az Informatikai Osztály szolgáltatási körébe nem tartozó környezet csak az Informatikai Osztály vezetőjével egyeztetett módon hozható létre.

10. § (1) Az Informatikai Osztály az általa központilag üzemeltetett rendszereket saját honlapján, a szolgáltatási jegyzékben közzéteszi. Ezek a szolgáltatások az Egyetem hivatalosan auditált szolgáltatásainak tekintendők.

(2) Az Informatikai Osztály vezetője felelős azért, hogy az „A” besorolású rendszerek teljes körű belső biztonsági felülvizsgálata dokumentált módon (belső felülvizsgálati jelentés) legalább háromévente megtörténjen. A felülvizsgálatok eredményei alapján az Informatikai Osztály vezetője rendelhet el javító, helyesbítő és megelőző intézkedéseket, melyeket mindig a soron következő belső vagy külső felülvizsgálat során kell dokumentált módon visszaellenőrizni.

(3) Az üzemeltetési tevékenység három logikailag elkülönült területen folyik:
a) éles környezet,
b) fejlesztői környezet és
c) teszt környezet.

(4) Az előre ütemezett (tervezett) informatikai szolgáltatás-kieséseket, illetve a meghibásodás miatti kieséseket a szolgáltatási feltételekben meghatározott módon publikálni kell, az események felhasználó irányú kommunikációja az Informatikai Osztály feladata és felelőssége.

(5) Az egyes rendszerekkel kapcsolatban nem csak reaktív, hanem preventív intézkedéseket is végezni kell a szolgáltatás zavartalan működtetésének érdekében. Ezek lehetnek általános és az adott szolgáltatásra speciálisan jellemző feladatok, különösen
a) igény szerinti újraindítás (reset),
b) a javítócsomagok, patchek, fixek telepítése,
c) a jelszavak és hozzáférési kódok rendszeres cseréje,
d) a naplóállományok rendszeres kiértékelése,
e) szakszemélyzet oktatása stb.

(6) A szolgáltató rendszerek üzemeltetési leírásának tartalmaznia kell szolgáltatásfolytonossági tervet, amelynek előállítása és karbantartása az Informatikai Osztály vezetőjének felelőssége. A szolgáltatásfolytonossági terv tartalmazza, hogy
a) milyen műszaki megoldások hivatottak biztosítani a szolgáltatás meghatározott elérési paramétereit (pl. redundanciát, failover-t biztosító rendszerkomponensek),
b) milyen helyettesítési lehetőségek (műszaki, technológiai és szervezési megoldások) vannak az adott szolgáltatás kiesése esetén (vészhelyzet),
c) milyen intézkedéseket kell megtenni a működés folytonosságának fenntartása érdekében,
d) kik az intézkedésre jogosultak,
e) kiket kell értesíteni az intézkedésekről.

(7) Az új hardvereszközök beüzemeléséről és rendszerbe illesztéséről az Informatikai Osztály gondoskodik. A műszaki, szakmai, biztonsági szempontból alkalmatlan eszközöknek az Egyetem informatikai infrastruktúrájába való illesztését az Informatikai Osztály megtagadhatja.
(8) Meghibásodás, rendellenes működés esetén az Informatikai Osztály munkatársait kell értesíteni, akik intézkednek a hibaelhárításról. A jogosulatlan hibaelhárításból eredő következményekért, károkért a jogosulatlan hibaelhárítást végző személy kártérítési felelősséggel tartozik.

Ügyfélszolgálat

11. § (1) Az Informatikai Osztály az incidenskezelés, felhasználói támogatás, illetve hibabejelentés kezelésének céljából elektronikus ügyfélszolgálatot biztosít a TopDesk szolgáltatás menedzsment rendszeren (a továbbiakban: ügyfélszolgálati rendszer) keresztül.
(2) Biztonsági esemény vagy gyengeség, illetve incidens bejelentése esetén a bejelentő köteles csatolni mindazon adatokat, amelyek az esemény megítéléséhez legjobb tudása szerint szükségesek (pl. időpont, tapasztalt jelenség, log file részlet, stb.) A bejelentés nem tartalmazhat adatvédelmi szempontból kifogásolható tartalmat (még képernyő másolat formában sem, pl. bér adat).
(3) Az ügyfélszolgálatnak minden bejelentést egyedi azonosítóval ellátott módon, számon kell tartani. A bejelentő számára az ügyfélszolgálati rendszerben tájékoztatást kell biztosítani a bejelentés életútjáról. A bejelentések megőrzése és rendelkezésre állásának biztosítása az Informatikai Osztály feladata, legalább 5 éves időtartamra visszamenőleg.
(4) A bejelentett incidensek kezelésére a rendszer besorolásától („A–D") két prioritási szinten (normál, magas) kerül sor. A priorizálás a bejelentést fogadó munkatárs feladata és felelőssége. Több incidens fellépésekor a magasabb rendű incidens megoldása elsőbbséget élvez.
(5) A bejelentett adatvédelmi incidenseket az Informatikai Osztály a rendszer integritásának és a kezelt adatoknak a védelmének érdekében köteles lehetőség szerint rövid reakcióidővel elbírálni, és a szükséges lépéseket (pl. hozzáférés korlátozás, biztonsági komponensek beállításainak módosítása) megtenni. Az Informatikai Osztály az adatvédelmi tisztviselőt tájékoztatja a biztonsági esemény következményeiről, és a megtett intézkedésekről. Tömeges érintettség esetén lehetőség van az Informatikai Osztály központi tájékoztató csatornáinak használatára is.
(6) Az ügyfélszolgálati rendszeren kívül tett bejelentés nem fogadható be – csak az adott szolgáltatási feltételek kifejezetten erre módot adó rendelkezése esetén.
(7) Az Informatikai Osztály csak a hatáskörébe tartozó rendszerekkel összefüggő műszaki problémákat old meg.
(8) Az incidens- és problémakezeléssel megbízott személy vagy munkacsoport automatikus incidens és/vagy probléma felderítő rendszereket üzemeltethet. A monitorozó rendszerek jelzéseit először az Informatikai Osztály munkatársa értékeli és minősíti. Amennyiben a jelzés incidensnek minősíthető, akkor az illetékes munkatárs elvégzi a bejelentés adminisztrációját az ügyfélszolgálati rendszerben.
(9) A visszatérő, több incidens kiváltó okaként megjelenő problémákat az Informatikai Osztály külön adatbázisban rögzíti. Az ismert hibák kiszűrése a hibafelvétel során történik. Az adott rendszerhez tartozó és meghatározott időn túl fennálló – kijavíthatatlan – ismert hibákat az informatikai Osztály hivatalos információs csatornáin keresztül publikálja a felhasználók felé.
(10) Az Informatikai Osztály által működtetett rendszerek esetén az ügyfélszolgálati rendszer felülete nyújt tájékoztatást az érintetteknek, azon hardver és szoftver elemek (kliensek) listájáról és elérhetőségéről, amelyek a szolgáltatás igénybevételéhez szükségesek. Kiegészítő tájékoztatás e-mailben is küldhető.
(11) Az Informatikai Osztály központosított szoftver disztribúciós és üzemeltetési célú felügyeleti szolgáltatást is nyújt a felhasználók számára.

(12) Terméktámogatást az Informatikai Osztály a szolgáltatási feltételekben meghatározott mértékben, és módon biztosít. Amennyiben az adott szolgáltatási feltételek máshogy nem rendelkeznek, úgy a terméktámogatás igénybevételének módja az ügyfélszolgálati rendszer.

Konfigurációkezelés

12. § (1) Minden rendszer esetében rendelkezni kell a szolgáltatáshoz szükséges információval a működéséhez szükséges hardver és szoftver komponensekről, valamint azok konfigurációjáról.
(2) Az Informatikai Osztály adott rendszerért felelős munkatársának feladata dokumentálni a gyártó által javasolt, valamint a rendelkezésre álló infrastruktúra paramétereit és gondoskodni ezek összhangjáról. A szükséges változtatásokról szóló javaslat a tervezés részét kell, hogy képezze.
(3) Az azonos alapinfrastruktúrán megvalósuló szolgáltatáscsoportok esetén csak a speciális, adott rendszerhez tartozó infrastruktúra elemeket szükséges dokumentálni, a közös infrastruktúra egyszeri dokumentálásán túl.
(4) Az Informatikai Osztály adott rendszerért felelős munkatársának minden rendszer esetében időrendben vezetnie kell a szolgáltatásban érintett komponenseket (konfigurációs elem, CI) leíró adatbázist.
(5) Minden jelentős változás esetén az alábbiakat kell megadni:

a) a változó komponensek egyértelmű azonosítását lehetővé tevő adatok,
b) a változás szükségességének indokai,
c) a tesztelésre vonatkozó adatok,
d) az aktuális visszaállási teendőket tartalmazó információt/hivatkozást is tartalmaznia kell a konfigurációs bejegyzésnek.

Változáskezelés

13. § (1) Az informatikai rendszerek változás-felügyeletét az Informatikai Osztály látja el.
(2) A nem az Informatikai Osztály által üzemeltetett, egyetemi rendszerek esetében az adott rendszer üzemeltetője a változtatás megkezdése előtt köteles konzultálni a rendszerek kialakítása és jelentős változtatása esetében az Informatikai Osztály illetékes munkatársával. A konzultáció a tervezési fázisban, a bevezetési fázisban és annak lezárásakor is kötelező az informatikai infrastruktúra integrált fejlesztésének fenntartása céljából.
(3) Jelentős változtatás az olyan változtatás, ami a rendszerek és kapcsolódó informatikai infrastruktúrák és szolgáltatások biztonságára (rendelkezésre állására, bizalmasságára és sérthetetlenségére), adatvédelmi előírásoknak való megfelelésére, erőforrás igényére, üzemeltetési feltételeire kihatással bír. A konzultáció a tervezési fázisban, a bevezetési fázisban és annak lezárásakor is kötelező az informatikai infrastruktúra integrált fejlesztésének fenntartása céljából.
(4) Külső szolgáltató nem végezhet változtatást semmilyen éles rendszerben, kivétel ez alól, amikor az Egyetem a változás jóváhagyására meghatalmazott, előzetesen megállapodott kapcsolattartója ezt engedélyezi. Egyetemi fejlesztői és teszt rendszerben a változtatások a szakterületi vezető iránymutatásai szerint, megállapodott célok és irányelvek mentén történhetnek külső szolgáltató részéről is.
(5) A rendszeres, üzemeltetési gyakorlat tevékenységébe tartozó változások végrehajtása a szakterületi vezető jóváhagyásával történhet meg, amely lehet vagy egyszeri, vagy az adott feladatra vonatkozóan folyamatos érvényű jóváhagyás. A nem a rendszeres üzemeltetési gyakorlat részét képező változások (különös tekintettel a szolgáltatás rendelkezésre állására jelentős kockázattal bíró változtatásokra), az Informatikai Osztály vezetőjének jóváhagyásával történhetnek meg.

(6) Az „A” és „B” besorolású rendszerek esetében az éles, teszt és fejlesztői környezet kialakítása kötelező. Éles rendszerben változás csak tesztelés után végezhető. Kivételes esetben az Informatikai Osztály vezetőjének engedélyével történhet az éles rendszerben változtatás.
(7) Az engedélyezett változtatásokat (hardver, szoftver, adatbázis, stb.) az Informatikai Osztály munkatársa, illetve a rendszer üzemeltetője az üzemeltetési leírásban foglaltak alapján hajthatja végre, sikeres végrehajtás esetén a rendszer leírásában azt dokumentálja.
(8) A nem az Informatikai Osztály által üzemeltetett egyetemi rendszerek esetében a változások felelőse az adott rendszer üzemeltetője. Az Informatikai Osztály által üzemeltetett rendszerek esetében a változás felelőse az illetékes szakterületi vezető. Külső szolgáltató üzemeltetésében (vagy közreműködő üzemeltetésében) álló rendszerek esetében a felelősségi határokat, és a felelősségek meghatározását az erre vonatkozó megállapodás kell, hogy tartalmazza.
(9) Az engedélyezett változtatásokat (hardver, szoftver, adatbázis, stb.) a szolgáltatás üzemeltetője az üzemeltetési leírásban foglaltak alapján hajthatja végre, sikeres végrehajtás esetén a rendszer leírásában azt dokumentálja.
(10) A változás végrehajtója felelős minden olyan beavatkozásért, amely nem a jóváhagyott gyakorlat mentén, nem a jóváhagyott módon történt, és azoknak a változtatásoknak az esetében, amelyek során a rendszer-üzemeltetési leírása nem lett betartva.

Szoftvermenedzsment

14. § (1) Az Informatikai Osztály feladata a szoftverek ésszerű beszerzésének és felhasználásának biztosítása.
(2) A nem az Informatikai Osztály által üzemeltetett egyetemi szoftvert üzemeltetője köteles az Informatikai Osztály részére az általa üzemeltetett szoftverekről tájékoztatást adni. A tájékoztatás meghatározott tartalommal történik. Nem jár tájékoztatási kötelezettséggel az olyan kutatási célhardver részét képező szoftver, amely kizárólagosan az eszközhöz köthető, egyéb területi felhasználása nem lehetséges.
(3) A szoftverek rendelkezésre állásának, nyilvántartásának és jogszerű használatának biztosítása az Informatikai Osztály vezetőjének felelőssége.
(4) Minden új szoftver beszerzést az Informatikai Osztály véleményezi, függetlenül a beszerzés forrásától, vagy módjától. Szoftver leltári nyilvántartásba vétele, raktári kiadása, üzembe helyezése csak az Informatikai Osztály tájékoztatása mellett történhet.
(5) Az Informatikai Osztály által üzemeltetett szoftverek esetében az egyes szakterületek vezetői központosított módon tárolják és karbantartják a szoftverek eredeti példányait, licenceit és installációs csomagjait.
(6)A szakterületi vezető felelőssége:

a) a legfrissebb verziók letöltése, a csomagok frissítése,
b) patchek, hotfixek letöltése, közzététele,
c) csomagok kártékonykód-ellenőrzése,
d) hozzáférési jogosultságok kezelése.

(7) Szoftverek telepítésére az üzemeltetési rendszerekben kizárólag az Informatikai Osztálynak van joga.
(8) A hiteles licence nyilvántartás kidolgozása és fenntartása az Informatikai Osztály feladata.

Kapacitástervezés

15. § (1) Az Informatikai Osztály vezetője a felelős azért, hogy a felhasználóktól beérkező igények, a szolgáltatói környezet változása, a technikai fejlődés figyelembe vételével tervezze, és az elfogadott egyetemi költségvetés szerint biztosítsa az Egyetem működéséhez szükséges informatikai kapacitásokat.

(2) Az adott rendszer várható terhelését az Informatikai Osztály, illetve a nem az Informatikai Osztály által üzemeltetett rendszer üzemeltetője a korábbi használati trendek alapján évente előre jelzi a következő egy éves időtartamra. A beérkező információk alapján a központi informatikai kapacitások tervezését az Informatikai Osztály végzi. Az elkészített következő évi kapacitástervet tartalmazza az összes olyan rendszerkomponens listáját, amely a szolgáltatás zavartalan biztosítása érdekében a várható terhelést figyelembe véve módosítani vagy bővíteni kell, illetve a központi szolgáltatások fenntartásához szükséges üzemeltetési költségeket, továbbá a tervezett új szolgáltatások, fejlesztések, projekt jellegű beruházások tételeit és forrásigényét.
(3) A kapacitástervben kell rögzíteni az elavult, nem szervizlehető komponensnek a cseréjére vonatkozó javaslatot is.
(4) A nem az Informatikai Osztály hatáskörébe tartozó informatikai kiszolgáló beruházások esetében az üzemeltetéshez szükséges kapacitásokat a Műszaki Igazgatóság biztosítja (pl. szerverszobai szünetmentes áramellátás, hűtés vagy légkondicionálás, stb.) A várható kapacitásigényt, tervezett fejlesztéseket a Műszaki Igazgatóságnak egyeztetnie kell az Informatikai Osztállyal.
(5) A kapacitástervet az Informatikai Osztály a következő évi költségvetés tervezéséhez előzetesen rendelkezésre bocsátja, majd a költségvetés elfogadását követően szükség esetén a költségvetés által biztosított kereteknek megfelelően módosítja.
(6) A kapacitásterv alapján az informatikai szolgáltatások működtetésének következő éves költségtervét az Informatikai Osztály vezetője készíti el, és továbbítja a Gazdasági és Műszaki Főigazgatóság részére a megelőző év október 31. napjáig.

Beszerzés támogatás

16. § (1) Informatikai rendszer, eszköz, illetve szoftver csak az Informatikai Osztállyal szakmai véleményezését követően szerezhető be. A véleményezési eljárás a beszerzési folyamatba építve valósul meg.
(2) A beszerzés során törekedni kell
a) az egyéb rendszerekhez való műszaki illeszthetőségre,
b) a hosszú távú gazdaságos üzemeltethetőségre,
c) a kiszolgáló erőforrások rendelkezésre állására,
d) a biztonságra, szakértelem rendelkezésre állására,
e) az optimális ütemezésre,
f) a felhasználói elégedettségre.
(3) Az Informatikai Osztály felelőssége a beszerzést megelőzően előre jelezni, amennyiben a beszerezni kívánt eszköz infrastruktúrába illesztését várhatóan meg fogja tagadni.
(4) A beszerzési eljárás egyszerűsítése érdekében az Informatikai Osztály a tipikus informatikai eszközökre meghatározott konfigurációkat (a továbbiakban: normatívák) ajánl ki. A normatívák meghatározása beosztás és funkcionális megfelelés szerint történik. A felhasználói normatívák az egységes, biztonságosan üzemeltethető infrastruktúrát és költséghatékony gazdálkodást szolgálják. A normatívák meghatározásának műszaki vetületeiért az Informatikai Osztály felelős.
(5) A használható állapotú, de nem használt informatikai eszközökből az Informatikai Osztály puffer raktárt képez. Amennyiben a puffer raktárában van a feladat elvégzéséhez megfelelő informatikai eszköz, azt beszerzési igény esetén köteles a felhasználó elfogadni, függetlenül attól, hogy az eszköz esetlegesen már használt.
(6) A tartósan nem használt eszközöket a szervezeti egységek az Informatikai Osztály kezelésében álló puffer raktárba átadhatják.

Szolgáltatói kapcsolattartás

17. § (1) Az Informatikai Osztály a feladatkörébe tartozó informatikai, telekommunikációs eszközök, szolgáltatások vonatkozásában kapcsolatot tart a külső szolgáltatókkal, illetve szállítókkal.
(2) A külső szolgáltató által biztosított informatikai szolgáltatások ellenőrzését az Informatikai Osztály végzi. Minden szállítói szolgáltatási megállapodás megkötése során szükséges az Informatikai Osztály bevonása a szolgáltatási feltételek, az ellenőrzés és együttműködés módjának egyeztetése és rögzítése céljából.
(3) A szállítói megállapodásokban mérhető, számon kérhető, a teljesítési elvárásokat jól tükröző teljesítménymutatókat kell meghatározni. A mért eredményeket folyamatosan vagy időszakosan – a megállapodás és szolgáltatás jellegétől függően – kommunikálni szükséges.
(4) A szolgáltatási jelentéseket, riportokat a szolgáltatási szint egyeztetések keretében kell felhasználni a szolgáltatás minőségének javítására, illetve a szerződésben foglalt vállalások számonkérésére.
(5) Törekedni kell a szolgáltatások automatizmusokkal támogatott monitorozására, a proaktív szállítói tájékoztatásra, és a megelőző beavatkozások támogatására.
(6) Az Informatikai Osztály szerződés-nyilvántartást, eszkalációs kapcsolati listát vezet kapcsolattartási és teljesítésértékelési céllal.

IV. rész
Információbiztonság

Általános rendelkezések

18. § Az informatikai és információbiztonság területén az alábbi alapelveket kell folyamatosan érvényesíteni:

a) A védelem teljeskörűségének követelménye akkor teljesül, ha a fizikai, a logikai és az adminisztratív védelem kiterjed az összes információbiztonsági rendszerelemre, az informatikai rendszerek infrastrukturális környezetére, a hardver rendszerre, az alap- és felhasználói szoftver rendszerre, a kommunikációs és hálózati rendszerre, az adathordozókra, a dokumentumokra és feljegyzésekre, a belső személyzetre és a külső partnerekre, az MSZ OSI 7498-1. szabványban meghatározott nyílt rendszerek architektúrája minden rétegére, továbbá mind a központi, mind a végponti informatikai eszközökre és környezetükre.
b) A védelem zártsága akkor biztosított, ha az összes valószínűsíthető fenyegetés elleni védelmi intézkedés megvalósul.
c) A védelem kockázatarányossága akkor áll fenn, ha az informatikai rendszerek által kezelt adatok védelmének erőssége és költségei a felmért kockázatokkal arányban állnak.
d) A védelem folytonossága azáltal biztosítható, hogy az informatikai rendszerek fejlesztése és megvalósítása során kialakított védelmi képességeket a rendszerből történő kivonásig folytonosan biztosítani kell a rendszeres ellenőrzéssel és az ezt követő védelmi intézkedésekkel.
e) A zárt szabályozási ciklus úgy érvényesíthető, hogy az adminisztratív védelemmel biztosítani kell a szabályozás, érvényesítés, ellenőrzés és a védelmi intézkedések/szankcionálás zárt folyamatát.
f) A működés elsődlegessége azáltal érvényesül, hogy a többség működőképességét gátló vagy veszélyeztető felhasználó vagy rendszer azonnal kizárásra kerül, a gátló vagy veszélyeztető tevékenység megszűntetéséig.

19. § (1) Az informatikai rendszerek információbiztonsági szempontból való megfelelőségi vizsgálatát, illetőleg az ezzel kapcsolatos tanácsadást – a külön szerződésben vásárolt esetleges külső auditon kívül – az Informatikai Osztály IT biztonsági felelőse végzi.
(2) Az információbiztonsági megfelelőségi vizsgálatot az Informatikai Osztály vezetőjének vagy az adott rendszert használó szakmai szervezeti egység vezetőjének kezdeményezésére soron kívül le kell folytatni.
(3) Az információbiztonsági megfelelőségi vizsgálaton nem megfelelt rendszerek üzemeltetését haladéktalanul le kell állítani, kivéve amennyiben a leállás aránytalanul veszélyezteti, vagy akadályozza az Egyetem működését. A rendszer további ideiglenes működtetéséről az Informatikai Osztály vezetője és az adott rendszert használó szervezeti egység vezetője közösen – egyetértésük hiányában a rektor – dönt. A rendszer leállításával, vagy az ideiglenes működtetéséről szóló döntés meghozatalával egyidejűleg megfelelő intézkedési tervet kell kidolgozni a rendszer kiváltásáról, vagy információbiztonsági szempontból való megfeleltetésének biztosításáról.
(4) Az Informatikai Osztály IT biztonsági felelősének felelőssége az információbiztonsági események, incidensek tanulságainak és a pozitív példáknak a megjelenítése az Informatikai Osztály információs csatornáin.
(5) Az információbiztonsági szabályok betartásával és betartatásával kapcsolatban az „A” és „B” osztályú rendszerek üzemeltetői – illetve a szolgáltatási feltételek ilyen irányú kifejezett rendelkezése esetén a felhasználók is – titoktartási nyilatkozatot írnak alá. Az Egyetem olyan külső partnerei, akik a velük fennálló jogviszony alapján, közvetlen vagy közvetett módon ilyen rendszerekhez, vagy abban tárolt adatokhoz férnek hozzá szintén titoktartási nyilatkozatot írnak alá – hacsak erről a velük a kötött szerződés eleve nem rendelkezik.
(6) A jogszabályban előírt információbiztonsági adatszolgáltatási kötelezettség teljesítése az Informatikai Osztály vezetőjének joga és felelőssége.
(7) Az információbiztonsági kérdésekben az Informatikai Osztály vezetője látja el a kapcsolattartási feladatokat a különleges érdekközösségekkel – különösen az ISACA Budapest Chapterrel, a Hétpecsét Információbiztonsági Egyesülettel).
(8) Információbiztonsági szempontból indokolt esetben bizonyos rendszerek használatának előfeltételeként szakmai minősítés vagy vizsga írható elő, az adott rendszer szolgáltatási feltételeiben.
(9) Az Egyetem információvagyona magában foglal minden, az Egyetem érdekkörébe tartozó, informatikai eszközön tárolt adatot, alkalmazást, kódot, illetve az azok rendelkezésre állásához, használatához kapcsolódó dokumentációt. Az információvagyon megőrzése, rendeltetésszerű használata minden alkalmazott, hallgató és az Egyetemmel szerződésben álló fél kötelessége

Az információvagyon védelme

20. § (1) Minden szervezeti egység vezetője személyesen felel az információbiztonság kultúrájának fenntartásáért. A vezetők elkötelezettségüket személyes példamutatással (szabályozások betartása) és személyes felelősségvállalással demonstrálják.
(2) Az Egyetem információvagyona kiterjed minden az Egyetem érdekkörébe tartozó, informatikai eszközön tárolt adatra, alkalmazásra, kódra, azok rendelkezésre állásához, használatához kapcsolódó dokumentációra, tudásra. Az információvagyon fenntartásához és használatához szükséges tudásanyag dokumentálása kötelező minden érintett részére.
(3) A fentiekben meghatározott információvagyon az Egyetem tulajdona. Kivételt képez az olyan eset, ahol a vonatkozó szerződés másként.
(4) Az információvagyon megőrzése, rendeltetésszerű használata minden egyetemi alkalmazott, hallgató és az Egyetemmel szerződésben álló fél kötelessége.

21. § (1) Az információvagyon kezeléséhez szükséges technikai feltételeket az Informatikai Osztály biztosítja.
(2) Az adatvédelmi tisztviselő köteles vizsgálni és jelezni az információvagyon személyes adatokat érintő biztonsági kockázatait.
(3) Az információvagyon védelmét szolgáló előírásokat minden felhasználó és üzemeltető köteles maradéktalanul betartani.
(4) Az egyetemi információvagyon alkalmas formában való maradéktalan visszaszolgáltatása kötelessége minden azt kezelő, használó felhasználónak, üzemeltetőnek, vagy szerződött félnek, amennyiben azt a feladata tovább nem indokolja.
(5) Az információvagyon felhasználása kizárólag az Egyetem érdekeinek megfelelően történhet. Annak harmadik fél számára való elérhetővé tétele csak az adatvédelmi tisztviselő és az Informatikai Osztály vezetőjének együttes hozzájárulásával történhet, kivéve szerződéses és törvényi kötelezettségeket.
(6) Az információvagyont az információbiztonság irányelvei szerint az adatvédelmi tisztviselő – illetve szükség esetén az adott rendszert használó szervezeti egység vezetőjének – bevonásával osztályozni kell. Az információosztályok a következők:

a) Nyilvános információk osztálya: Az Egyetem által nyilvános módon működtetett felületeken (egyetemi, kari és tanszéki honlapok) megjelenített közérdekű információk.
b) Alapbiztonsági osztály: Személyes adatok, üzleti titok, pénzügy adatok.
c) Fokozott biztonsági osztály: Szolgálati titok, különleges személyes adatok, banktitok.
d) Kiemelt biztonsági adatok: Államtitok, nagy értékű üzleti titkok.

(7) Az Egyetem információvagyonának elsődleges tárolási helye az Egyetemi informatikai infrastruktúra. Egyetemi információvagyon csak központi tárolón tárolható.
(8) Magántulajdonú eszközön vagy idegen tulajdonú tárolón az Egyetemi információvagyon tárolása – az erre vonatkozó kifejezett engedély, vagy ilyen tárgyú szerződés hiányában – tilos.
(9) Az Egyetem tulajdonában lévő mobil eszközöket megfelelően titkosítani kell. Az Egyetem területéről kizárólag titkosított formában vihető ki mobil eszközön információ.
(10) A notebookok titkosítását az Informatikai Osztály végzi el az üzembehelyezéskor vagy a felhasználó kérésére.
(11) A mobiltelefonokhoz és tabletekhez (ún. „okos” eszközök) kapcsolódó információbiztonsági követelmények érvényesítése központi menedzsment program használatával történik. Külső adatkártyán az Egyetem információvagyonába tartozó adatot tárolni tilos.
(12) A külső adathordozókon (pl. mobil HDD, pendrive, DVD) az Egyetem információvagyonába tartozó adatot tárolni csak titkosított formában lehet, amihez a technikai feltételeket az Informatikai Osztály biztosítja.
(13) Az Egyetem tulajdonában álló eszközöket megbízott félnek javításra csak az Informatikai Osztály – vagy az általa megbízott személy – adhat át. Az eszközökön adat csak titkosított formában adható ki, de törekedni kell az adathordozó nélküli átadásra.
(14) Amennyiben a javítás során az adathordozó átadása szükséges, nem titkosított adatokkal, a javítás csak az Informatikai Osztály munkatársának személyes részvételével lehetséges. Ez alól kivételesen indokolt esetben az Informatikai Osztály vezetője – az adatvédelmi tisztviselő előzetes véleményének kikérése után – felmentést adhat.
(15) Az Egyetemről kikerülő eszközök (pl. értékesítés, selejtezés) adathordozóin található adatok a kor színvonalának megfelelő felülírással, az adathordozó eltávolításával vagy megsemmisítésével távolíthatók el. Az elszállítás, átadás előtt az Informatikai Osztály munkatársa köteles írásos nyilatkozatban igazolni a törlést.
(16) Informatikai eszközt selejtezési céllal elszállítani vagy harmadik fél számára elérhetővé tenni kizárólag az Informatikai Osztály előzetes engedélyével lehetséges. Az Informatikai Osztály köteles a kor színvonalának megfelelő szintű adatmegsemmisítésről gondoskodni

minden kiadott adathordozó esetében, a selejtezésre elszállítás esetén az adathordozó fizikai használhatatlanná tétele kötelező. (pl. fizikai roncsolás fúróval). A selejtezést végző és átadó munkatárs is köteles meggyőződni arról, hogy adathordozó vagy papír alapú dokumentum nem maradt az eszközben.
(17) Adathordozó szállítása esetén a szállítást végző köteles kellő gondossággal eljárni az adathordozók és adatok biztonságának megőrzése érdekében. Az adatok eredeti forrása és mentése nem szállítható ugyanazon eszközzel.
(18) Indokolt esetben – az Informatikai Osztály vezetője és az adatvédelmi tisztviselő közös döntése alapján – az információ értékének megfelelő külön védelmi intézkedés, biztosítás szükséges.

22. § (1) Az informatikai kiszolgáló infrastruktúra kulcselemeinek elhelyezése szerverszobában vagy hálózati eszközök esetében zárt szekrényekben történhet.
(2) A zárt infrastruktúrához csak az Informatikai Osztály munkatársai férhetnek hozzá – ide nem értve a veszélyhelyzet esetére a portaszolgálatnál található kulcsokat.
(3) Az információtároló eszközök, helységek, szerverszobák megválasztása és kialakítása csak a biztonsági szempontok teljes körű figyelembe vételével történhet. Az informatikai eszközök elhelyezését balesetmentesen üzemeltethető formában kell megoldani.
(4) A szerverszobába csak naplózott módon lehetséges bejutni. A szerverszobában csak az Informatikai Osztály munkatársa tartózkodhat, egyéb személy csak Informatikai Osztály munkatársának jelenlétében és felügyelete alatt látogathatja a helyiséget. A szerverszobában egyedül az Informatikai Osztály munkatársai is csak bejelentés mellett tartózkodhatnak. A bejelentést a helyi portán, a helyszíni Informatikai Osztályos munkatársaknál, vagy az Informatikai Osztályvezetőnél lehet megtenni. A szerverszobában – ha az adott szoba méretéből kisebb létszám nem következik – legfeljebb 8 fő tartózkodhat egyidejűleg.
(5) A szerverszoba áram, szünetmentes, túlfeszültség védelmi és hűtés ellátását, videó és beléptetési és távközlési kapcsolati, tűz és vagyonvédelmi szolgáltatását az Üzemeltetési Osztály szolgáltatja. Az informatikai szolgáltatások rendelkezésre állást érintő, befolyásoló tevékenységekre vonatkozóan az Informatikai Osztály tudomása és jóváhagyása nélkül változtatás, karbantartás, egyéb tevékenység nem végezhető.
(6) A szerverszobában csomagolóanyag, használaton kívüli eszközök nem tárolhatók. A szerverszoba raktározásra nem használható.
(7) Az informatikai eszközöket kiszolgáló szolgáltatások működés-folytonosságáról az Üzemeltetési Osztály köteles gondoskodni. Az Üzemeltetési Osztály köteles minden tudomására jutó működés-folytonossági kockázatra felhívni az Informatikai Osztály vezetőjének a figyelmét (pl. útfelbontási, elektromos és felújítási tevékenység).
(8) A felhasználó leltári felelőssége alá tartozó eszközök fizikai biztonságáért a felhasználó felel. Az informatikai eszközök tárolása a felhasználó távollétében használati szempontból zárolt állapotban, elzártan történik. Az eszköz használat szempontjából lezártnak minősül, ha tevékenység csak felhasználói bejelentkezést, azonosítást, jogosítást követően végezhető, illetve a tevékenységre utaló adat nem látható, nem visszaállítható (pl. kijelzőn adat, nyomtatóban lap).

23. § (1) Az informatikai eszközök tároló helyiségeinek forgalmát, az eszközök fizikai védelmét (pl. közösségi területen elhelyezett rack szekrények) és az informatikai eszközök mozgását a portaszolgálat kiemelt figyelemmel kezeli.
(2) Azok az irodák, amelyekben informatikai eszközök vannak elhelyezve, használaton, felügyeleten kívül kulcsra zárva tartandók.

(3) Az informatikai eszközök raktározása a központi raktározási eljárásrend szerint történik, amely meg kell, hogy feleljen az adat és vagyonbiztonság arányos kockázatainak. Raktárban csak adat-tartalom nélküli eszköz tárolható.
(4) Szállítási és rakodási területen informatikai eszköz felügyelet nélkül nem maradhat a rakodás idejére sem. A szállítási és rakodási területek kijelölése a Műszaki Igazgatóság feladata.
(5) Az informatikai eszközök, adathordozók elhelyezése, mozgatása (rakodás, raktározás) az egészségügyi, balesetvédelmi, adatbiztonsági és vagyonvédelmi kockázatok figyelembe vételével, és ilyen szabályok betartása mellett lehetséges.
(6) Az Informatikai Osztály az informatikai eszközök tömeges mozgatását, illetve nagy tömegű informatikai eszközök mozgatását nem végzi, csak a szállításra előkészítés, illetve az üzembe helyezés a feladata.
(7) Az Informatikai Osztály az oktatástechnikai eszközök informatikai vonatkozású technikai működtetését támogatja. Azok biztonságos tárolása, sérülés elleni védelme, szállítása, telepítése (pl. mennyezeti projektortelepítés) nem feladata.
(8) Fizikai karbantartási tevékenység központi kiszolgálók esetében külső megbízott által csak az Informatikai Osztály felügyelete alatt, annak engedélyével, személyes részvétel mellett, a szerződésben foglaltak szerint lehetséges.

24. § (1) Informatikai üzemeltetési vagy egyéb felhasználói információ, amely a rendszerbe történő illetéktelen behatolást, biztonsági incidens eredményezhet, használaton kívül is elzártan, arra alkalmas szekrényben, páncélszekrényben tárolandó.
(2) Licenc, telepítő média, amelynek elvesztése, illetéktelen kezekbe jutása anyagi, erkölcsi hátrányt, biztonsági incidenst eredményezhet, csak arra kijelölt, zárt szekrényben tárolható. A licenc dokumentumok, média központi technikai nyilvántartása, tárolása az Informatikai Osztály feladata. Az Informatikai Osztály leltári, gazdasági jellegű nyilvántartást nem vezet, a műszaki jellegű adatok kezelése a feladata.
(3) Adathordozóval szerelt berendezések (pl. HDD-vel szerelt multifunkciós eszközök) elzáratlan területen (pl. folyosó) csak abban az esetben helyezhetők el, ha azokra 24 órás biztonsági megfigyelés garantálható (pl. portaszolgálati kamera).
(8) Az Informatikai Osztály feladatkörébe tartozik az üzemeltetésében lévő eszközök, illetve a központi kiszolgáló, és hálózati eszközök megfelelő, teljeskörű karbantartása, illetve a felhasználói eszközök szoftveres karbantartása.

25. § (1) Minden olyan rendszer esetében, ahol kártékony kód fenyegetés fennáll, és lehetséges installálni kártékony kód elleni rendszert, akkor azt az Informatikai Osztály telepíti, és ennek a szoftvernek felhasználói megkerülése tilos.
(2) Nem egyetemi tulajdonú eszközök használatából eredő kártékony kód által okozott károkért az Egyetem rendszereiben felhasználóként belépett személy a felelős.
(3) Az Informatikai Osztály biztonsági mentést készít minden központi tárolón elhelyezett dokumentumról, az Informatikai Osztály vezetője által kibocsátott mentési eljárási rendben foglaltak szerint.
(4) A mentési eljárási rendnek tartalmaznia kell az alkalmazások és adatok mentési rendjét, a mentendő adatok körét, a mentés módját és gyakoriságát, a mentésért felelős személyt, a mentés tárolási rendjét.
(5) A mentési rendnek alkalmasnak kell lennie arra, hogy az üzemeltetési környezet visszaállítható legyen.
(6) Minden „A” és „B” osztályú rendszer esetében mentés tesztelési környezetet kell létrehozni, és évente legalább egy alkalommal visszatöltési gyakorlatot (tesztelés) kell tartani, amely a mentések felhasználhatóságát ellenőrzi.

(7) A biztonsági mentések az éles rendszerek tárolási helyétől telephelyileg elkülönülő helyen kerülnek elhelyezésre.
(8) Támogatandó a gyors mentésből történő visszaállás, és törekedni kell a tartalék infrastruktúra elemek és rendszerek kialakítására.

26. § (1) Az Informatikai Osztály folyamatosan – napi 24 órában – monitorozza az egyetemi informatikai rendszerek működését. A monitorozás eredményeként megjelenő riasztások kezelése az Informatikai Osztály munkaidejében történik.
(2) A naplófájlokba az adott rendszert használó szervezeti egység vezetőének kérésére az Informatikai Osztály betekintési lehetőséget ad.
(3) A naplófájlok hitelességét óraszinkronizálással kell biztosítani.
(4) Az egyes rendszerekben történő üzemeltetési tevékenységek naplózása külső szolgáltató esetén a szerződésben szabályozott módon és mértékben, Informatikai Osztály munkatársak esetében az üzemeltetői jogokkal való visszaélésekre alkalmat kínáló tevékenységek esetében kötelező. Az üzemeltetési tevékenység ésszerű határokon belüli, de az esetleges biztonsági incidensek, üzemeltetési események követhetőségét lehetővé tevő szinten való naplózására törekedni kell.
(5) A tevékenységet és hozzáféréseket leíró napló- és rendszerfájlok védelmének biztosítása az Informatikai Osztály feladata.
(6) Az informatikai rendszerekkel kapcsolatos üzemeltetési szerződésekben a hozzáféréseket, a naplózás módját, és az üzemeltetői tevékenységgel kapcsolatos felelősségeket meg kell határozni. A feltételek teljesülést az Informatikai Osztály ellenőrizheti.

27. § (1) Az adott szakterület vezetője felelős az alkalmazások publikált technikai sérülékenységek elleni védekezés megvalósításáért. Az Informatikai Osztály infrastruktúráért felelős munkatársának kötelessége az infrastruktúra elemek védelmének sebezhetőség elleni biztosítása.
(2) Alaprendszerek esetében (pl. operációs rendszerek, virtualizációs rendszerek, kártékony kódok elleni védekező rendszerek, stb.) törekedni kell a publikált sérülékenységek elleni védekező intézkedés (pl. patch-ek és fixek alkalmazása) mielőbbi végrehajtására, tekintettel az adott rendszereket használó alkalmazások és az ésszerű erőforrás gazdálkodás korlátaira.
(3) Alkalmazások esetében a gyártói ajánlás alapján, a szakma gyakorlata szerint kell eljárni.
(4) Hardver elemekhez kapcsolódó frissítések végrehajtása esetében az alaprendszerek esetében meghatározott módon kell eljárni.
(5) Azokban az esetekben, ahol az alkalmazás jelenti a naprakészség biztosítását, törekedni kell a rendszerek kiváltására, vagy kivonására, a biztosított szolgáltatások köréből.
(6) A hozzáférési jogosultságok elbírálását végző komponensek bármely rendszer esetében a felhasználói jelszavakat csak titkosítva tárolhatják.
(7) Az Informatikai Osztály vezetője jogosult a nem megfelelően frissített rendszer/szolgáltatás azonnali kizárására az egyetemi informatikai környezetből. A kizárás feloldására a megfelelő frissítés elvégzését követően van lehetőség.

28. § (1) A kommunikációs hálózatok (kivétel a szolgáltatók által biztosított rendszerelemek és szolgáltatások (pl. távközlési hálózatok, mobil hálózat, idegen eszközök, alépítmények stb.) biztonságos üzemeltetése során a hálózati eszközök kiválasztásánál a magas rendelkezésre állási minőségre, a központi menedzselhetőségre, a homogén (kapcsolható, ésszerűen tartalékolható, cserélhető) elemekből építkezésre, a hosszú távon gazdaságosan üzemeltethető megoldásokra (lehetőség szerint fix költség választására, rendszeres licence díjak kerülése) kell törekedni.
(2) A passzív hálózat változtatása kizárólag az Informatikai Osztály hozzájárulásával történhet.

(3) Aktív hálózati eszközt az egyetemi tulajdonú eszközökön kívül csatlakoztatni a hálózathoz tilos.
(4) Az aktív eszközök beállítását és illesztését az Informatikai Osztály végzi. A hálózati szolgáltatás megosztására alkalmas eszközt a hálózathoz illeszteni az Informatikai Osztály munkatársain kívül mindenki másnak tilos.
(5) A hálózatokat fizikai és logikai megoldásokkal is szegmentálni szükséges. Az Internet oldali hálózatot és a belső hálózatot tűzfallal kell elválasztani. Internet irányból csak az erre alkalmas tűzfalakon lehet belépni az Egyetem hálózatába. Törekedni kell a szolgáltatások kizárólag belső hálózatról való elérhetőségére, külső hálózatról VPN használatára, azon szolgáltatások esetében, ahol a felhasználás módja ezt lehetővé teszi.
(6) A belső hálózatokat szegmentálni szükséges VLAN-ok kialakításával. A VLAN-ok szervezeti egységek és funkciók szerint kerülnek kialakításra.
(7) Törekedni kell a MAC address alapú végpont azonosításra, port security korlátozások bevezetésére, ahol ez biztonsági szempontból fokozottan indokolt.
(8) A hálózati beállítások alapelve az „alapvetően minden tiltott, és csak a munkavégzéshez szükséges kivétel engedélyezett (a szükséges legkisebb jogosultság elve)”.
(9) Az alap hálózati infrastruktúrát magas rendelkezésre állással kell kialakítani. Az alapinfrastruktúra kiterjed a magas rendelkezésre állású szolgáltatásokat (LDAP, AD, SAP, ECM, FileShare, Zimbra…) kiszolgáló hálózati eszközökre (switch, router), tűzfalszolgáltatást biztosító eszközökre és azokon futó szolgáltatásokra. A magas rendelkezésre állás biztosítása céljából az Informatikai Osztály tartalékot köteles képezni az ésszerű erőforrás gazdálkodás irányelveinek betartásával.
(10) A WAN hálózat szintjén redundáns optikai körgyűrű kialakítása szükséges a budapesti telephelyek összekötésére. A Budapesten kívüli telephelyeken törekedni kell az optikai kapcsolat megszakadása esetére az alapvető működés biztosítására (lokális címtár kiszolgáló, Internet kapcsolat).
(11) A vezetéknélküli hálózat elemeinek egy központilag menedzselt infrastruktúrába kell illeszkedni. A központi menedzsmentet redundáns kialakítással kell megvalósítani. A WiFi controller és az AccessPoint-ok közötti forgalom titkosított. Az AccessPoint-ok jelszóval védettek, beállításuk a controller segítségével megváltoztatható a hálózatban. A hálózati aktív eszközök adatokat csak titkosított formában tárolhatnak.
(12) A hálózat menedzsmentje csak az Informatikai Osztály által kijelölt személyek számára engedélyezett. Hálózati menedzsment tevékenység csak hálózaton belülről, meghatározott IP címről kezdeményezhető, és az ilyen kommunikációt titkosítani kell.
(13) A hálózati forgalom lehallgatása, megfigyelése, szolgáltatások veszélyeztetése, vagy azokra utaló magatartás az informatikai rendszerekből történő azonnali kizárást eredményez. A hálózati forgalom megfigyelésére, naplózására, elemzésére kizárólag az Informatikai Osztály hálózati menedzsment feladatokat ellátó munkatársai jogosultak, de a megfigyelés ekkor sem terjedhet ki a személyes felhasználói kommunikáció tartalmára A megfigyelés kizárólag a hálózati szolgáltatás biztonságos, rendeltetetésszerű működésének biztosítását szolgálhatja.
(14) A távközlési szolgáltatókkal kötött szolgáltatói szerződésekben a rendundáns megoldásokra kell törekedni. Külső szolgáltatóval a szolgáltatási felelősségi határokat úgy kell meghatározni, hogy azok egyértelműen számon kérhetők legyenek, valamint ne eredményezzenek átfedésben lévő felelősségeket. A belső hálózatban külső szolgáltató nem kaphat lehetőséget felügyelet nélküli menedzsment tevékenységre, kizárólag az Informatikai Osztály munkatársának közreműködésével járhat el.
(15) A kommunikációs hálózathoz való csatlakozás feltétele a – csatlakozás módjától és a csatlakoztatott rendszertől függő – biztonsági előírások maradéktalan betartása.
(16) A hálózat felépítését, az egyes zónákat a hálózati infrastruktúra dokumentáció tartalmazza. A dokumentáció naprakészségének biztosítása az Informatikai Osztály feladata.

29. § (1) Minden alkalmazás fejlesztési tevékenységét a szolgáltató alkalmazáspéldánytól és annak adatbázisától elkülönítve kell végezni. Amennyiben a fejlesztési tevékenységhez védett intézményi adatok is szükségesek, akkor a fejlesztői rendszer is „B" osztályú rendszernek minősül és a hozzáférési jogosultságok ennek megfelelően adhatók ki.
(2) Intézményi fejlesztésű vagy vásárolt szolgáltató rendszer csak funkcionális teszt után vonható szolgáltató üzembe. A funkcionális tesztnek a szolgáltatási feltételekben rögzített minden paraméterre és funkcióra, valamint a tipikus felhasználási mintákra kell kiterjednie. A funkcionális tesztről írásos jegyzőkönyvnek kell készülnie, melynek az összes mért és ellenőrzött paramétert és funkciót tartalmaznia kell.
(3) Minden, a szolgáltatási felületen vagy a funkciókészletben különbséget tartalmazó alkalmazás verzió esetén a tesztelési eljárást újra el kell végezni. A tesztelési kötelezettség az operációs rendszerek, adatbázis kezelők és egyéb támogató alkalmazások (pl. web szerver) esetén is fennáll, de csak a használt funkciókra kell kiterjednie.
(4) Szolgáltató üzemben működő alkalmazáson csak sikeres tesztelési dokumentáció birtokában és az üzemeltető alkalmazás- vagy rendszergazda engedélyével végezhető változtatás, külső munkavégző cég esetében is. Ez alól csak a szolgáltatás helyreállítását célzó sürgős hibajavítás jelenthet kivételt, ami esetében a dokumentálást utólag kell elvégezni.
(5) A már működő rendszerek továbbfejlesztése, módosítása során a biztonsági követelmények nem változtathatók olyan irányba, hogy a rendszer biztonsági szintje csökkenjen, csak különösen indokolt esetben, megfelelő kockázatelemzés után.

30. § (1) Az Informatikai Osztály vezetője felelős azért, hogy az informatikai rendszerek teljes körű belső biztonsági felülvizsgálata dokumentált módon legalább háromévente megtörténjen, és legalább ötévente sor kerüljön külső – harmadik fél általi – felülvizsgálatra az „A" osztályú rendszerek esetében.
(2) Súlyos biztonsági incidens esetén rendkívüli biztonsági ellenőrzés és felülvizsgálat rendelhető el.
(3) A felülvizsgálatok eredményei alapján az Informatikai Osztály vezetője rendel el javító, helyesbítő és megelőző intézkedéseket, melyek teljesülését a soron következő belső vagy külső felülvizsgálat során dokumentált módon ellenőrizni kell.

V. rész
Felhasználói szabályzat

A felhasználók jogai és kötelezettségei

31. § (1) A felhasználónak joga van a saját jogosultsági szintjének megfelelően az Egyetem informatikai infrastruktúrájának és szolgáltatásainak használatára és a használathoz szükséges valamennyi információ megszerzésére.
(2) A felhasználó számára tilos saját jogosultságának átruházása mások számára. Tilos minden olyan jogosultság megszerzése vagy megszerzésére irányuló kísérlet, amely a felhasználó számára nem engedélyezett.
(3) A felhasználó köteles rendeltetésszerűen használni az Egyetem informatikai infrastruktúráját, és együttműködni az Informatikai Osztállyal a működési hibák, nem rendeltetésszerű vagy szabálytalan használat felderítésére indult vizsgálatban.
(4) A felhasználó az Egyetem informatikai infrastruktúráját csak úgy használhatja, hogy azzal mások munkáját ne zavarja vagy akadályozza.
(5) Az Egyetem informatikai struktúrájának használata során tilos minden olyan tevékenység, amely bármilyen formában anyagi, erkölcsi kárt okoz vagy okozhat az Egyetemnek, különösen a torrent szerverek használata, hacker tevékenység, etikátlan vagy törvénybe ütköző tartalmak megjelenítése, adatok biztonságának veszélyeztetése.

(6) A felhasználó köteles kellő gondossággal eljárni, hogy a kezelésében álló vagyontárgyak, különös tekintettel az információvagyonra, az Egyetem tulajdonában, elvárható állapotban maradjanak, valamint képesek legyenek a feladatuk ellátására.
(7) A szolgáltatások felhasználása közben tapasztalt biztonsági gyengeségek vagy műszaki hibák jelentése – a rendszer működőképességének fenntarthatósága érdekében – minden felhasználónak kötelessége.
(8) Nem az Informatikai Osztály által üzemeltetett infrastruktúrán megvalósuló informatikai oktatási, kutatási tevékenység csak az Egyetem informatikai infrastruktúrájától elválasztott és zárt környezetben történhet, biztonságosan elhatárolva az Egyetem más rendszereitől.
(9) Az Egyetem nevében az Egyetem informatikai infrastruktúráján kívül lévő szolgáltatást csak a rektor engedélyével, az Informatikai Osztály vezetőjének tájékoztatásával lehetséges indítani és üzemeltetni.
(10) Minden felhasználó köteles a licence használati feltételeket betartani, annak jogi felelősségével. Minden felhasználó köteles törekedni az ésszerű és költséghatékony licence gazdálkodásra.
(11) A felhasználók az egyetemi infrastruktúrát jogosultak olyan módon és mértékben magán célra használni, hogy az a munkavégzési tevékenységet, az infrastruktúrát, vagy bármilyen egyéb módon az Egyetem érdekeit ne veszélyeztesse. A magán célú használatból származó minden kárért a felelősség a felhasználót terheli. Az egyetemi infrastruktúra üzletszerűen vagy haszonszerzési céllal nem használható.
(12) A felhasználók az egyetemi infrastruktúrán, vagy eszközökön saját szoftvereket nem telepíthetnek, csak az Informatikai Osztály előzetes engedélyével. A felhasználó által engedély nélkül telepített szoftver jogtisztaságáért, vagy az infrastruktúrájában okozott kárért a felhasználó felelős.
(13) A felhasználók kezelésében álló eszközök fizikai karbantartása a felhasználó feladata (pl. notebook, monitor, telefon, billentyűzet portalanítás) az elvárható hozzáértés mértékéig. Amennyiben a felhasználó bizonytalan a karbantartási tevékenység megfelelőségét, biztonságos megvalósíthatóságát illetően, szakmai tanácsot kérhet az Informatikai Osztály munkatársaitól. A felhasználó kizárólag a baleset-, egészség-, tűzvédelmi és vagyonvédelmi szabályok betartásával végezheti a karbantartást. A helytelen karbantartásra, rendellenes eszköz használattal, elhelyezéssel kapcsolatos károkra visszavezethető károk a felhasználót terhelik.
(14) A felhasználói eszközök szoftveres karbantartása az Informatikai Osztály feladata. A szoftveres karbantartási tevékenység (pl. frissítés, telepítés) támogatására központi menedzsment eszközök használat ajánlott.
(15) Az Informatikai Osztály központi, kötelezően alkalmazott kártékony kód elleni védelmi szolgáltatást biztosít felhasználói munkaállomásokra, amelyek frissítését az Informatikai Osztály végzi, központi terjesztéssel. Az Informatikai Osztály határvédelmi megoldással is támogatja a rosszindulatú tevékenységek elleni védelmet.
(16) Felhasználó támogatási céllal távfelügyeleti megoldás (monitor és konzol átvétel) alkalmazása lehetséges, de kizárólag a felhasználó adott alkalomra vonatkozó hozzájárulásával.
(17) Takarítási tevékenység során az eszközök hálózati vagy áram ellátásának, ki-be kapcsolt állapotának változtatása tilos.

32. § A jelen szabályzat rendelkezéseinek megsértése esetén, ha a felhasználó magatartása az Egyetem informatikai rendszerének biztonságát vagy egyéb módon az Egyetem érdekeit veszélyezteti, úgy a felhasználó – az Informatikai Osztály vezetőjének döntése alapján – az adott informatikai szolgáltatásból ideiglenes intézkedéssel kizárható, a megfelelő vizsgálati eljárás kezdeményezésével egyidejűleg.

Hozzáférésmenedzsment

33. § (1) A felhasználók által igénybe vehető informatikai szolgáltatásokat a szolgáltatás katalógus tartalmazza, amit az Informatikai Osztály honlapján tesz közzé.
(2) A szolgáltatás katalógus bizonyos elemei automatikusan rendelkezésére áll a felhasználóknak, a jogviszony létrejöttét követően, míg más szolgáltatások igénylés útján elérhetők csak.
(3) Az Egyetem által nyújtott informatikai szolgáltatásokat az igénylők három csoportja veheti igénybe:

a) hallgatói jogviszonnyal bíró természetes személyek,
b) egyetemi dolgozók, akik az oktatási, kutatási és adminisztratív feladatok végrehajtásában érintettek,
c) vendégek, akik nem egyetemi polgárok, de részt vesznek az Egyetem oktatási, kutatási és az ezt kiszolgáló folyamataiban.

(4) A hallgatói jogviszony alapján a hallgató az alábbi alapszolgáltatásokat kapja:

a) Neptun hozzáférés,
b) e-mail szolgáltatás (Zimbra) x.y@hallgato.ppke.hu,
c) 500 MB tárhely,
d) MS EDU szoftvercsomag,
e) Eduroam hozzáférés,
f) hozzáférés a PPKE weblap belépés köteles oldalaihoz.

(5) A hallgató az alapszolgáltatásokhoz kényszerített jelszóváltást követően juthat hozzá. A belépéshez szükséges technikai információk az Ügyfélszolgálati rendszerében érhetők el.
(6) Az Egyetem munkavállalói az alábbi alapszolgáltatásokat kapják:

a) Neptun hozzáférés,
b) e-mail szolgáltatás (Zimbra) x.y@ppke.hu, x.y@szervezetiegyseg.ppke.hu,
c) 5 GB tárhely,
d) MS EDU szoftvercsomag
e) Eduroam hozzáférés,
f) hozzáférés a PPKE weblap belépés köteles oldalaihoz,
g) Nexon (HR rendszer) hozzáférés.

(7) A munkavállaló az alapszolgáltatásokhoz kényszerített jelszóváltást követően juthat hozzá. A belépéshez szükséges technikai információk az Ügyfélszolgálati rendszerében érhetők el.
(8) A munkavégzéshez szükséges informatikai eszközöket a munkavállalók számára a foglalkoztató szervezeti egység biztosítja. Az eszközön található szoftverkörnyezetet és azok beállításait kötelezően az Informatikai Osztály alakítja ki.
(9) A munkavállaló egyéb jogosultságait és alkalmazás-hozzáféréseit, kapcsolódó informatikai munkakörnyezet kialakítását a munkavállaló szervezeti egységének vezetője igényli az Informatikai Osztálytól az ügyfélszolgálati rendszeren keresztül.
(10) Az Egyetemmel más jogviszonyban álló személyek által igénybe vehető informatikai szolgáltatásokat az adott személlyel fennálló jogviszony határozza meg. A jogosultságokat a jogviszony szempontjából illetékes szervezeti egység vezetője igényli meg az ügyfélszolgálati rendszeren.
(11) Az Egyetem vendégei az egyes rendezvényekhez kötötten jogosultak ideiglenes jelszóval a rendezvényen nyújtott szolgáltatásokat (pl. WiFi) igénybe venni. Ez a jogosultság a rendezvény végeztével automatikusan megszűnik és a szolgáltatás technikai feltételei is megszűnnek az eszközök leszerelésével vagy kikapcsolásával, illetve a hozzáférések megszüntetésével.

34. § (1) Hozzáférés, jogosultság csak a jogviszonyban meghatározott feladat elvégzéséhez szükséges és elégséges mértékben igényelhető, adható, és minden érintett jogosultsága azokra az információkra korlátozódik, melyek szükségesek a munkája megfelelő végzéséhez.
(2) A jogosultságok változtatásának igénylése az ügyfélszolgálati rendszeren keresztül történik.

(3) Az informatikai rendszereket és eszközöket használó munkavállalók belépés előtti előzetes biztonsági megfelelési vizsgálatát az Informatikai Osztály nem végzi. A titoktartással és a biztonsági intézkedések betartásával kapcsolatban a munkaszerződések rendelkeznek.
(4) A hallgatói jogviszony létesítése előtt biztonsági megfelelőség vizsgálat nem történik. A képzési szerződés aláírásával és a beiratkozással a hallgatók tudomásul veszik a vonatkozó szabályok betartási kötelezettségét.
(5) A harmadik személyekkel kapcsolatos információbiztonsági kockázatokat a jogviszony létrehozását kezdeményező köteles mérlegelni mielőtt az érintettek jogosultságait és hozzáférési szintjét az Informatikai Osztályhoz eljuttatná kérelmében. Az érintettektől szükséges írásos nyilatkozatok (pl. titoktartási nyilatkozat, stb.) beszerzése, illetve az informatikai rendszerek használatával kapcsolatos megfelelő szintű tájékoztatás biztosítása szintén a jogviszony létrehozását kezdeményező feladata.
(6) A felhasználó azonosítás címtárakban (AD, LDAP) történik. A felhasználó azonosítás során az egykapus és biztonságos azonosítási eljárások alkalmazására törekszünk a rendszerek elérhetőségének biztosítására.
(7) A bizalmas információkat tároló és kezelő rendszerek (pl. SAP, ECM, Nexon-HEGO felület) elérhetősége csak belső egyetemi hálózatról engedélyezett a felhasználók számára.
(8) Külső együttműködő, szolgáltató számára a rendszerekhez való hozzáférést az Egyetem VPN segítségével biztosít vagy egyedi megállapodás szerint, ideiglenes jelleggel (pl. SSH). A hozzáférések megadását az Informatikai Osztály vezetője engedélyezheti. A hozzáférés mértéke nem haladhatja meg a szerződött feladat elvégzéséhez szükséges és elégséges szintet.
(9) Hozzáférési kulcs csak időkorlát alkalmazásával adható ki, annak időtartamát az Informatikai Osztály vezetője határozza meg.
(10) Hozzáférési kulcs átadása felhasználónak csak személyesen történhet, vagy indokolt esetben titkosított formában lehetséges kiküldeni, amely feloldásához szükséges információt csak a kiküldési csatornától eltérő biztonságos csatornán (javasolt SMS-ben) lehetséges továbbítani az Informatikai Osztály vezetőjének hozzájárulásával.
(11) Távoli rendszerüzemeltetés csak titkosított kommunikáció használatával lehetséges. Az „A” és „B” osztályú rendszerekbe történő, változtatási jogosultságot is lehetővé tevő bejelentkezés csak védett, titkosított kommunikációval (pl. SSH, VPN) engedélyezett az Egyetem hálózatán kívülről.
(12) VPN hozzáférést kezdeményezni kizárólag egyetemi eszközről lehetséges.
(13) Nem az Informatikai Osztály üzemeltetésében álló eszköz a belső hálózathoz nem csatlakoztatható.
(14) Minden hozzáférés kizárólag személyes azonosításra alkalmas módon történhet az informatikai rendszerhez. Nem nevesített felhasználóval tevékenység sem végezhető. A hozzáférés birtokosa köteles gondoskodni a hozzáférés biztonságos kezeléséről.
(15) Az Informatikai Osztály jogosult minden üzemeltetésében álló eszköz esetében hozzáférést szabályzó, biztonságos működést, adatvédelmet célzó beállításokat, korlátozásokat alkalmazni.
(16) A hozzáféréseket (belépéseket és kilépéseket) az Informatikai Osztály jogosult naplózni és biztosítja, hogy ezek az adatok a szakterületi igényektől/kötelezettségektől függő időtartamig visszakereshetők, lekérdezhetők legyenek.
(17) Az Egyetem Internetes hálózati kapcsolatait az Informatikai Osztály vezetőjének engedélyével lehetséges használni egyedi megállapodások alapján a nem az egyetemi Informatikai Osztály üzemeltetésében álló eszközökkel is, jellemzően kutatói tevékenység esetében, és a belső erőforrásoktól határvédelemmel elszigetelt módon. Az ilyen megoldás kialakítását megelőzően biztonsági kockázatelemzés szükséges. Az érintett eszközökkel az egyetemi belő hálózathoz csatlakozni, hozzáférés lehetőségét kialakítani tilos. A nem az Informatikai Osztály által üzemeltetett eszközökkel járó minden üzemeltetési, jogi, erkölcsi, gazdasági felelősség az üzemeltetést végző szervezeti egység vezetőjét terheli.

35. § (1) Az informatikai szolgáltatás igénybe vételére való jogosultság megszűnik az annak alapjául szolgáló jogviszony megszűnésével. Az Informatikai Osztály által üzemeltetett rendszerekben a jogosultságok megvonását a kiléptetés során a Humánerőforrás Gazdálkodás bejelentése alapján az Informatikai Osztály végzi.
(2) A hallgatói jogviszony megszűnése után az alapszolgáltatások közül a hallgató a Neptun hozzáférésre marad csak jogosult a saját személyes adatai vonatkozásában. Hallgatók esetében, a jogszabályokban előírtakon túl, az Informatikai Osztály nem archiválja az adatokat.
(3) A munkaviszony megszűnését követően a munkavállaló az alapszolgálatások közül jogosult marad a saját személyes adatai vonatkozásában Neptun és Nexon hozzáférésre. A munkahelyi vezető kérheti a kilépő személy által kezelt intézményi adatok mentését, postafiókjának archiválását, és az ezekhez szükséges hozzáféréseket. A fenn nem tartott informatikai jogosultságok megszüntetését a kiléptetési eljárásban az Informatikai Osztály igazolja.
(4) Szerződéses partnerek és vendégek (pl. vendégoktatók) esetében a vendéglátó vagy szerződéses Egyetemi kapcsolattartó igénylése alapján jár el az Informatikai Osztály az archiválási és jogosultsági igények ügyében. A kilépő lapon vagy más dokumentált módon nem igényelt adatok archiválásáért, illetve indokolatlanul fennmaradó jogosultságokért a vendéglátó vagy a szerződéses Egyetemi kapcsolattartó jogosultság igénylő a felelős.
(5) A jogosultság kiadását kezdeményező annak megvonását kezdeményezheti rendkívüli eljárás keretében is, adott határidővel vagy azonnali hatállyal, telefonon és párhuzamosan dokumentált formában (ügyfélszolgálati rendszer bejelentés, e-mail, levél, SMS) az az Informatikai Osztály vezetőjétől.
(6) Amennyiben a jogosultság, hozzáférés tulajdonosa a jogosultságok és hozzáférések mennyiségében, minőségében eltérést tapasztal a neki célszerűen meghatározotthoz képest, vagy bármely gyanús eseményt tapasztal, azt haladéktalanuk jelenteni köteles a munkahelyi vezetője számára, aki köteles indokolt esetben az Informatikai Osztályhoz fordulni a problémával.

Jelszóhasználat

36. § (1) Az Informatikai Osztály törekszik az egy jelszó használatára (Single Sign On, SSO), de néhány szolgáltatáshoz való hozzáférés ettől eltérő jelszó használatot feltételez:

a) A Shibboleth rendszer egy egyetemi környezetben elterjedt felhasználó azonosítási megoldás, amely biztonságosabb felhasználó azonosítást tesz lehetővé a rendszerhez csatlakozó felsőoktatási intézményeknél.
b) A gazdasági rendszerek, tartományi eszközök vagy egyedi eszközök Active Directory külön jelszót használnak
c) A Neptun tanulmányi rendszer, és ahhoz kapcsolódó egyéb központi rendszerek szintén külön jelszóval védettek.

(2) A három jelszó csoport jelszavainak megváltoztatása az ügyfélszolgálati rendszerben a „Jelszóbeállítás” menüpont alatt vagy az közvetlen hozzáféréssel az alábbiak szerint lehetséges:

a) Shibboleth (pl. Zimbra levelező, belső weboldalak, WiFi) jelszó: https://info.ppke.hu/cgi-bin/password-changer
b) Active Directory jelszó-változtatás: https://pwd.ad.ppke.hu/rdweb/pages/hu-HU/password.aspx A "Tartomány\felhasználónév:" AD\sajátazonosító (pl. AD\QWE6TR)
c) Neptun Tanulmányi Rendszer:
    1) Oktatóknak: https://neptun3.ppke.hu/Oktato/login.aspx
    2) Hallgatóknak: https://neptun3.ppke.hu/Hallgato/login.aspx

(3) A biztonságos jelszóhasználat érdekében a jelszó formátuma meghatározott. A jelszó rendszeres megváltoztatása ajánlott, de nem kikényszerített, kivétel az első belépés alkalmával. További tájékoztatás a jelszó változtatás igénylő felületén közvetlenül is elérhető.
(4) A jelszóhasználat szabályozására egyebekben az Informatikai Osztály vezetője jogosult.

VI. rész
Záró rendelkezések

37. § (1) A jelen szabályzat rendelkezései – a (2)–(4) bekezdésekben foglalt kivételektől eltekintve – a kihirdetését követő napon lépnek hatályba.
(2) A jelen szabályzat 10. § (1) bekezdése, 17. § (6) bekezdése, 28. § (10)–(11), bekezdései, valamint 33. § (1) bekezdése 2020. január 1-jén lép hatályba.
(3) A jelen szabályzat 6. § (2) és (4) bekezdései, 8. §-a, 16. § (4)–(6) bekezdései, 24. § (2) bekezdése, 25. § (3)–(8) bekezdései, 26. §-a, valamint 28. § (16) bekezdése 2021. január 1-jén lép hatályba.
(4) A jelen szabályzat 7. § (7) bekezdése, 10. § (2) és (6) bekezdései, 12. §-a, 19. § (1) bekezdése, valamint 30. § (1) bekezdése 2022. január 1-jén lép hatályba.