2. verzió

Az Óbudai Egyetem **Szervezeti és Működési Szabályzata**
1. melléklet **Szervezeti és Működési** Rend
22. függelék

AZ ÓBUDAI EGYETEM INFORMATIKAI BIZTONSÁGI SZABÁLYZATA

BUDAPEST, 2014. június

TARTALOMJEGYZÉK

PREAMBULUM

(1) Az informatikai rendszerek üzemeltetése során a veszélyeket teljes mértékben megszüntetni sohasem lehet. A veszélyeztetettség egy kockázati tényező, mellyel számolnunk kell, és állandóan törekednünk kell a kockázatok kezelhető mértékre történő leszorítására. Ez azt jelenti, hogy e tényezőket folyamatos kontroll alatt tartjuk.

(2) A szabályozás hármas feladatot lát el: megelőzés a kár elkerülése érdekében, folyamatos figyelés az időben történő észlelés érdekében és a bekövetkezés esetén gyors és hatékony reakció a kár minimalizálása érdekében. Az intézkedések és szabályok a biztonsági osztályba sorolásnak megfelelően három kiemelt területre fogalmaznak meg eljárásokat. Ezek az adminisztratív, a fizikai és logikai védelmi szabályrendszerek. Az adminisztratív védelem területére tartoznak azok a szabályok és eljárás rendek, amelyek általánosságban fogalmazzák meg az engedélyezett és tiltott tevékenységeket. A fizikai védelem a hardverek és szoftverek védelme az illetéktelen hozzáféréstől. A hardvereket és a szoftvereket elzárt helyiségekkel, a helyiségeket részben vagy egészben a belépő azonosítására alkalmas beléptető rendszerrel védjük. A logikai védelem magában foglalja mindazokat a tevékenységeket, amelyek a megelőzésére, a kár minimalizálására, a katasztrófa elhárítására irányulnak, pontosan meghatározva a szükséges feladatokat és a felelősségeket.

(3) A megelőző kontrollok közé tartoznak azok a technikák, amelyekkel megpróbáljuk elkerülni egy adott veszélyhelyzet bekövetkezését. Nagyrészt ide tartoznak a szabályozások is, hiszen alapvetően ezek is megelőző rendelkezéseket tartalmaznak. Az észlelő kontrollok lényege, hogy minél előbb felismerjék a nem kívánt esemény bekövetkezését, és így korlátozható legyen annak káros hatása. Ez azonban csak úgy lehetséges, ha a veszély felismerését azonnal előre megtervezett, hatékony cselekvés-sorozat követi.

(4) Jelen Informatikai Biztonsági Szabályzat arra hivatott, hogy az Óbudai Egyetemen működő informatikai rendszerekre specializálva a megelőző kontrollok definiálásával csökkentse az informatikai biztonsági kockázatok bekövetkezésének valószínűségét, az észlelő kontrollok meghatározásával, a legnagyobb biztonsággal tegye felderíthetővé a vészhelyzeteket és a reakció kontrollokon keresztül a lehető leghamarabb szüntesse meg a bekövetkezett káros esemény hatását.

I. rész
Általános rendelkezések
A szabályzat feladata, célja és hatálya
1. §

(1) Az Informatikai Biztonsági Szabályzat (a továbbiakban: IBSZ) egy olyan intézkedés együttes, amelynek az Óbudai Egyetem informatikai rendszerével kapcsolatos biztonsági intézkedéseit, előírásait kell tartalmaznia. A szabályzatnak az intézmény biztonságpolitikájában jelzett irányelveket kell követnie és a gyakorlatban megvalósítania. Amíg a biztonságpolitika egy magasabb szintű, főleg vezetői döntéseket és alapelveket megfogalmazó dokumentum, addig az Informatikai Biztonsági Szabályzat olyan alacsonyabb szintű szabálygyűjtemény, amely azokat a gyakorlati kérdéseket helyezi előtérbe, amelyek konkrét cselekvési mintákat határoznak meg. Itt kell megfogalmazni azokat a célokat, amelyek elérése érdekében a szabályzat létre lett hozva, és ami miatt az intézménynél az informatikai biztonsággal foglalkozni kell. Az IBSZ az Óbudai Egyetem belső használatra szóló dokumentuma. Az egyetemen kezelt adatok és eszközök biztonsági osztályba sorolását az Óbudai Egyetem Adatvédelmi Szabályzata fogalmazza meg.

(2) Az IBSZ feladata továbbá, hogy az informatikai rendszereket érintő veszélyforrásokat felderítse,

elvégezze a szükséges kockázatelemzést, és meghatározza a védelmi intézkedéseket. A kockázat nagyságát – bekövetkezés valószínűségét – és az esetlegesen okozott kár mértéket figyelembe véve 3 kockázati fokozat állapítható meg:

a) magas kockázati fokozat – az egyetem munkáját alapvetően befolyásoló kockázati tényezők, például a Neptun rendszer leállása, adatok megsemmisülése.
b) közepes kockázati fokozat – a központi szolgáltatások üzemeltetését befolyásoló kockázati tényezők, például a levelezés tartós kiesése.
c) alacsony kockázati fokozat – egyéb szolgáltatások üzemeltetését befolyásoló kockázati tényezők, például a WiFi hálózat rövid idejű meghibásodása.

(3) Az IBSZ feladata, hogy a kockázati fokozatokkal arányos védelem kialakításáról intézkedjen. Ennek a feladatának a biztonsági rendszer tervezésével tesz eleget. Az arányos védelem azt jelenti, hogy a védelemre fordítható anyagi lehetőségek, a védeni kívánt érték vagy információ fontosságának függvényében alakul ki.

(4) Az IBSZ az egyetem informatikai tevékenységének átfogó szabályozására készített dokumentum. Célja, hogy az informatikai rendszer használata során biztosítsa a használhatóság és a biztonság együttes követelményeinek érvényesülését, megakadályozza a jogosulatlan hozzáférést a rendszerekhez, minimálisra csökkentse a szándékos vagy vétlen károkozást. Az IBSZ célja, hogy a hallgatók és a dolgozók ismerjék az egyetem informatikai rendszerének használatát, a hálózat és a szolgáltatások használatából adódó kockázatokat, és elhárításuk rájuk vonatkozó részét.

(5) Az IBSZ célja, hogy az egyetem informatikai tevékenysége során kezelt eszközök, feldolgozott és továbbított adatok bizalmasságát, sértetlenségét biztosítsa, valamint a rendelkezésre állást fenyegető veszélyek elhárítására védelmi intézkedéseket fogalmazzon meg.

(6) Az IBSZ célja továbbá, hogy megfogalmazza és szabályozza:

a) a titok-, vagyon-, tűzvédelemre vonatkozó védelmi intézkedéseket,
b) az üzemeltetett informatikai rendszerek rendeltetésszerű használatát,
c) az üzembiztonságot szolgáló járulékos szolgáltatások körét (klíma, szünetmentes áramforrás, stb.),
d) az adatállományok biztonságos mentését,
e) a speciális feladatokat ellátó helyiségek behatolás elleni védelmét.

(7) A szabályzat személyi és tárgyi hatállyal is rendelkezik.

a) Személyi hatálya: A szabályzat személyi hatálya az egyetem minden – az informatikai rendszert használó – polgárára kiterjed. Az egyetem polgára valamennyi dolgozó és hallgató. Az IBSZ vonatkozik továbbá minden olyan személyre is, aki használja az Óbudai Egyetem informatikai infrastruktúráját.
b) Tárgyi hatálya: A tárgyi hatályba beletartozik a fizikai, infrastrukturális eszközökön kívül az adatok, szoftverek teljes köre is. Technológiai értelemben a szabályzat kiterjed a folyamatokra, vonatkozik valamennyi telephelyre és kiterjed a létesítményekre is.

(8) Az adatvédelem és adatbiztonság szabályozásával, valamint a számítógépek biztonsági minősítésével az Óbudai Egyetem Adatvédelmi Szabályzata foglalkozik.

II. rész
Intézkedések
Felelősségi körök
2. §

(1) Az egyetemen dolgozó munkatársak, hallgatók, vendégek, egyéb felhasználók kötelesek betartani a jelen szabályzatban leírtakat, továbbá kötelesek jelenteni az informatikai osztályvezetőnek, ha biztonsági problémát okozó jelenséggel találkoznak (biztonsági incidens).

(2) Az egyetem informatikai rektorhelyettese felelős az Informatikai Biztonsági Politika, az Informatikai Biztonsági Szabályzat kidolgozásáért. Az Informatikai Biztonsági Politikának ki kell fejeznie a vezetés elkötelezettségét az általános biztonság és az informatikai biztonság megfelelő szintjének kialakítása és fenntartása mellett.

(3) Az egyetem intézményi szintű vezetése, illetve az egyetem további vezetői felelősek a saját területükön az IBSZ-ben foglaltak betartatásáért. Az egyetem vezetésének feladata, hogy a szabályzatban megfogalmazott IT biztonsági szereplők részére a munkavégzésükhöz szükséges hatáskört és erőforrásokat biztosítsa.

(4) Az Informatikai Osztály (továbbiakban: IO) információbiztonsági kérdésekben közvetlenül az informatikai rektorhelyettesnek tartozik beszámolási kötelezettséggel.

(5) Az IO feladata és felelőssége az információbiztonság szintjének folyamatos ellenőrzése, a biztonsági incidensek megelőzése, illetve a bekövetkező incidensek hatásának mérséklése, valamint az okok feltárása, a felelősök azonosítása, továbbá a későbbi beszerzések, az informatikai fejlesztések során a biztonsági követelmények érvényre juttatása.

(6) Az alább felsorolt feladatok támpontot adnak az IO információbiztonság terén végzendő munkájához:

a) az informatikai rendszereket fenyegető veszélyforrások miatt fellépő kockázatok meghatározása és csökkentése,
b) részvétel a védelmi rendszer tervezésében,
c) biztonsági szabályok meghatározása és betartatása,
d) védelmi rendszer működtetése az egyetem informatikai biztonsági követelményeinek összehangolása,
e) információbiztonság rendszeres felülvizsgálata,
f) az informatikai hálózat biztonságának folyamatos ellenőrzése,
g) informatikai rendszer változásainak nyomon követése, és ennek megfelelően módosítási javaslat kidolgozása,
h) adatvédelmi felelőssel egyeztetve és együttműködve részt vesz a biztonsággal összefüggő szakmai munkában,
i) bejelentés alapján kivizsgálja a biztonsági incidenseket, és javaslatot tesz további intézkedésekre,
j) évente legalább egyszer ellenőrzi az IBSZ előírásainak betartását,
k) az előírások ellen vétőkkel szemben felelősségre vonási eljárást kezdeményezhet.

(7) Az adatvédelmi felelős munkája során szorosan együttműködik az IO-val. Segíti az IO munkáját és szakmai kérdésekben iránymutatást nyújt az IO-nak. Az adatvédelmi felelős feladatait az Adatvédelmi Szabályzat határozza meg.

(8) Az Informatikai Osztály vezetőjének feladata, felelősség és hatásköre a munkaköri leírásban található részletesen. Az információbiztonság tekintetében az osztályvezető felelős:

a) az informatikai rendszer üzemeltetéséhez szükséges erőforrások biztosításáért,
b) az informatikai rendszer folyamatos működéséért,
c) az informatikai rendszer biztonságának folyamatos felülvizsgálatáért.

(9) A rendszergazdák feladata, felelősség és hatásköre a munkaköri leírásban található részletesen. A rendszergazda információbiztonság szempontjából felelős:

a) a rábízott hálózat és eszközök biztonsági kockázatának minimalizálásáért,
b) az üzemeltetési feladatokat veszélyeztető és akadályozó tényezők felismeréséért és jelentéséért,
c) az informatikai szabályok betartásáért.

(10) Az operátorok az egyetem informatikai rendszerének végberendezéseiért (számítógépek) felelősek biztonsági szempontból. Ezzel kapcsolatban felmerülő feladataik:

a) új eszközök informatikai biztonsági politikának megfelelő beállítása,
b) biztonsági javítócsomagok telepítése a hozzájuk rendelt IT eszközökön,
c) biztonsági beállítások helyességének sértetlenségének folyamatos biztosítása.

(11) A személyes használatban lévő számítógépek, laptopok felhasználói, biztonsági szempontból felelnek a rájuk bízott eszköz biztonságáért. Feladatuk:

a) biztonsági frissítések, javítócsomagok telepítése,
b) személyes jogosultság beállítása,
c) rábízott érzékeny adatok védelme.

Amennyiben a személyes használatú számítógép biztonságáról a felhasználó nem maga kíván gondoskodni, köteles ezt a feladatot az operátorra bízni.

Környezeti és fizikai biztonság

3. §

(1) Védett helyiségnek kell tekinteni azokat a helyiségeket, ahol a bizalmas adatok feldolgozására, tárolására alkalmazott informatikai erőforrások találhatók. A védett területek zárt területnek minősülnek, ezért védelmükről ennek megfelelően kell gondoskodni.

(2) Védett területnek minősül az egyetemen:

a) szerverszoba,
b) kari szerverszoba
c) telefonközpont,
d) központi szünetmentes áramforrás elhelyezésére szolgáló helyiség,
e) aktív hálózati elemek elhelyezésére szolgáló helyiség (rendező).

(3) Szerverszoba: az IBSZ, hasonlóan az Informatikai Szabályzathoz, nem a szervezeti struktúrát igyekszik minél tökéletesebben leképezni, ezért a telephelyeket tekinti önálló egységekként, és a helyi sajátosságokat figyelembe véve definiál egységes rendszert. Ennek megfelelően, a telephelyeken szerverfarmokat kell kialakítani. A szolgáltatásokat biztosító, szerver feladatokat ellátó eszközöket közös helyiségben, szerverszobában kell elhelyezni. A szerverszoba biztonsági szempontból fokozottan védett helyiségnek minősül, melyekbe kizárólag ellenőrzött módon, az arra kijelölt személyek juthatnak be. A szerverszobával szemben támasztott követelmények:

a) zárt helyiség, csak arra feljogosított személyek léphetnek be,
b) naplózott beléptetés, amely ellenőrizhetővé teszi a tevékenységet végzőket,

c) légkondicionálás, az üzembiztonság fenntartása érdekében,
d) szünetmentes áramforrás, az üzembiztonság fokozása érdekében,
e) füst-, és tűzérzékelő, a vagyonvédelem és az üzembiztonság érdekében.

(4) A szerverszobában végzendő munka szabályai:
a) a szerverszobába csak arra feljogosított személy léphet be,
b) szerverszobába munka csak feljogosított személy által vagy annak jelenlétében végezhető

(5) Kari szerverszoba: az egyetem a nagyobb, több épületet is összefogó telephelyein a szervezeti egységek szervereinek külön helyiséget biztosít. Biztonsági szempontból ezek a szerverszobák nem különböznek a központi feladatokat kiszolgáló eszközöket tartalmazó szerverszobáktól. E helyiségek esetében is biztosítani kell a légkondicionálást, a behatolás elleni védelmet, és a szünetmentes áramellátást. A helyiségben a biztonsági és munkavégzési előírások megegyeznek a szerverszobánál előírtakkal.

(6) Telefonközpont: az Óbudai Egyetem telephelyein, eltérő módon kialakított telefonközpontokban a védelem is eltérően lett kialakítva. A helyi sajátosságokat figyelembe véve az óbudai telephelyen személyi védelem biztosítja a telefonközpont és a szünetmentes áramforrás védelmét. A Tavaszmező utcai telephelyen kódzárral kombinált riasztó rendszer garantálja a telefonközpont és a szünetmentes áramforrás védelmét.

(7) A rendező helyiségek, amelyekben az aktív hálózati elemek helyezkednek el, zárt helyiségek, központi riasztóra kötött kódzáras beléptetővel. A zárt helyiséghez kulcsa, és a kódzár feloldásának kódja az IO dolgozóinak a birtokában van.

(8) A számítógép-használat általános alapelvei: az egyetemen működő számítógépek csak rendeltetésszerűen, munkavégzés céljából használhatók. Minden munkatárs csak a munkájának végzéséhez szükséges rendszerekhez kaphat jogosultságot. Számítógépek használata során fokozott figyelmet kell fordítani a tűz-, érintés-, és munkavédelmi szabályokra. A számítógépek és monitorok szellőzőnyílásait letakarni nem szabad, elektromos csatlakoztatások használata során kiemelt figyelmet kell fordítani az áramütés veszélyére. Informatikai hálózat csatlakoztatását megbontani nem szabad. Az egyetemen működő számítógépekre csak az érvényes szabályozás mellett telepíthetők szoftverek. A beosztástól függően, vagy a megbízott informatikai személy végzi a telepítést, vagy a személyes használatban lévő gép felhasználója. Azokban az esetekben, amikor a számítógép személyes használatban van, a felhasználó felelőssége, hogy gépére illetéktelen szoftver ne kerüljön fel, és az elemi biztonsági feltételeknek a számítógép megfeleljen.

(9) A felhasználóknak a munkaállomások használata során a következő általános szabályokat kell betartaniuk:
a) személyes használatban lévő számítógépen felhasználói jogokkal kell rendelkeznie,
b) felhasználói jogaihoz tartozó jelszóval védeni tudja számítógépe integritását,
c) illetéktelen személynek felhasználói jogát át nem adhatja,
d) közepes vagy magas biztonsági kockázattal járó feladatvégzésekor a számítógépét senkinek át nem engedheti, információbiztonsági kockázatot nem okozhat,
e) biztonsági frissítésről gondoskodnia kell,
f) vírusvédelmi szoftver telepítéséről és frissítéséről gondoskodnia kell,
g) működő számítógépet csak jelszóval védett képernyővédő használatával hagyhatja magára.

(10) A hálózat használatának szabályai: az Óbudai Egyetem telephelyein strukturált és menedzselt informatikai hálózat működik. Ez a hálózat aktív és passzív elemekből áll. Illetéktelen személy a

kialakított rendszeren nem változtathat, végpontot át nem helyezhet és aktív- vagy szerver feladatokat ellátó eszközt a hálózatra nem kapcsolhat rá. A hálózat bővítésére vagy átalakításra kizárólag az Informatikai Osztály jogosult.
A VLAN-ok biztonsági feladatot látnak el, mert elválasztják egymástól a részhálózatokat, ezzel biztosítva, hogy sérülés, vagy támadás esetén csak az adott részterületre korlátozódjék az esetleges kár. A VLAN-ok kialakítása az Informatikai Osztály hatásköre.

(11) Az Óbudai Egyetem hálózata nem használható az alábbi tevékenységekre (a NIIF Felhasználói Szabályzata szerint, kiemelve a legfontosabb részeket, a teljes lista megtalálható az Interneten):

a) a mindenkor hatályos magyar jogszabályokba ütköző cselekmények előkészítése vagy végrehajtása, így különösen mások személyiségi jogainak megsértése (pl. rágalmazás), tiltott haszonszerzésre irányuló tevékenység (pl. piramisjáték), szerzői jogok megsértése (pl. szoftver nem jogszerű terjesztése),
b) profitszerzést célzó, direkt üzleti célú tevékenység és reklám,
c) a hálózat, a kapcsolódó hálózatok, illetve ezek erőforrásainak rendeltetésszerű működését és biztonságát megzavaró, veszélyeztető tevékenység, ilyen információknak és programoknak a terjesztése,
d) a hálózatot, a kapcsolódó hálózatokat, illetve erőforrásaikat indokolatlanul, túlzott mértékben, pazarló módon igénybevevő tevékenység (pl. körlevelek, hálózati játékok, kéretlen reklámok),
e) a hálózat erőforrásaihoz, a hálózaton elérhető adatokhoz történő illetéktelen hozzáférés, azok illetéktelen használata, gépek/szolgáltatások - akár tesztelés céljából történő - túlzott mértékben való szisztematikus próbálgatása (pl. TCP port scan),
f) a hálózat erőforrásainak, a hálózaton elérhető adatoknak illetéktelen módosítására, megrongálására, megsemmisítésére vagy bármely károkozásra irányuló tevékenység,
g) másokra nézve sértő, vallási, etnikai, politikai vagy más jellegű érzékenységét bántó, zaklató tevékenység (pl. pornográf/pedofil anyagok tárolása, közzététele),
h) hálózati üzenetek, hálózati eszközök hamisítása: olyan látszat keltése, mintha egy üzenet más gépről vagy más felhasználótól származna (spoofing).

(12) A felhasználók kötelességei a hálózat használata során:

a) A felhasználók kötelessége a szabályzat megismerése és az abban foglaltak betartása, valamint együttműködni a hálózat üzemeltetőivel a szabályzat betartatása érdekében.
b) A felhasználó viseli a felelősséget minden műveletért, amely az adott felhasználóhoz tartozó azonosítóval kerül végrehajtásra.
c) A felhasználó kötelessége és felelőssége, hogy a munkaállomásán jogtiszta szoftvereket használjon.

(13) A felhasználók jogai a hálózat használat során:

a) A felhasználónak joga van a felhasználói fiókhoz való hozzáféréshez. Az egyetemen ez a központi szolgáltatás az oktatóknak az asztali számítógépeiken, a hallgatóknak pedig a kari laborokban, vagy a WiFi szolgáltatás segítségével válik lehetővé.
b) A felhasználó személyiségi jogait és a levéltitkot a hálózat üzemeltetői tiszteletben tartják, ettől eltérni csak a törvény által meghatározott esetekben lehet.
c) A rendszer technikai problémáiról (tervezett vagy rendkívüli eseményekről) tájékoztatni kell a felhasználókat.
d) A felhasználók számára elérhető módon közzé kell tenni a felhasználókra vonatkozó szabályok érvényes változatát.
e) A szervezeti egységek további hálózati szolgáltatásokat biztosíthatnak.

(14) Jogosultságok kezelése a hálózat használata során:

a) Az eszközök használatának módját a felhasználói jogosultság szabályozza. A felhasználók különböző jogosultságokkal rendelkezhetnek, melyeket jelen szabályzat alapján, a meghatározott jogosultsági szinteknek megfelelően kell meghatározni.
b) A publikus hozzáférés (labor használat, Internet használat, információs pultok, stb.) kivételével, a jelszavas védelemnek a szerverekre, a hálózaton üzemelő és az egyedi számítógépekre is ki kell terjednie. A felhasználói hálózatra érvényes jelszó nélkül senki nem kapcsolódhat. Gondoskodni kell a hozzáférések naplózásáról is, így regisztrálható a sikertelen hozzáférési kísérlet. Ha jogosulatlan hozzáférés történt, vagy a jogosulatlan hozzáférés gyanúja merül fel, a jelszót azonnal meg kell változtatni.
c) A hozzáférési jogosultságok meghatározásakor figyelembe kell venni az adatokat kezelő program, a biztonsági program vagy részrendszer biztonsági osztályba sorolását, az ellátandó feladatot és a feladatot végző személy felelősségi körét.
d) Alapelvként kell kezelni a jogosultság kiosztásakor, hogy minden funkcióhoz illetve feladathoz csak a feladat ellátásához szükséges és elégséges mértékű jogosultságok biztosíthatók.
e) A hozzáférés-védelemre vonatkozó szabályoknak tartalmazniuk kell a jelszó-hossz és bonyolultság meghatározását, az időszakos jelszócsere szabályozását, a felhasználók kitiltási előírásait, illetve a hozzáférés-védelmi eszközök gyártásának, tárolásának, szétosztásának, használatának és kivonásának előírásait.
f) Az alap jogosultsági szint mindenkit megillet, aki az intézménnyel hallgatói, vagy munkavállalói jogviszonyban áll, és aláírásával igazolta, hogy a szabályzat tartalmát megismerte, annak betartását vállalja. Az alap jogosultsági szint adható pl. tanfolyam esetén az intézménnyel jogviszonyban nem állók részére is. A további jogosultsági szinteket az alap szint kiegészítéseként kell értelmezni. Az egyedi igényeket az erre rendszeresített igénylőlapon kell kérni. A felhasználótól a jogosultsági szintjének megfelelő jogot megtagadni csak indokolt esetben lehet. A jogosultsági szintnek megfelelő szabályok betartása a hálózatba nem kötött eszközök használata esetén is kötelező.

(15) A felhasználói jogosultságok szintjei:

Szint:	Jogosultak:	Jogok:
Alap	Az intézmény bármely hallgatója vagy dolgozója	Általános azonosítás, mely lehetővé teszi az oktatáshoz, munkához szükséges adatok valamint az internet elérését
Tanulmányi csoport	Tanulmányi osztály dolgozói	Egyéni azonosító, Internet használat, saját könyvtár a szerveren, teljeskörű hozzáférés a Neptun rendszer adminisztratív moduljaihoz.
Oktató	Az intézmény oktatói	Alap + hozzáférés az oktatói könyvtárakhoz, és a hallgatókkal kapcsolatos adminisztrációs adatokhoz
Adminisztrátor	Adminisztrációval kapcsolatos munkakörök	Alap + hozzáférés az adminisztrációs adatokat tartalmazó könyvtárakhoz
Gazdasági	A gazdasági irodák dolgozói	Alap + hozzáférés a gazdálkodással és a dolgozókkal kapcsolatos adatokat tartalmazó könyvtárakhoz

Operátor	Az adott feladatra kijelölt személy	Speciális jogok, pl. a levelező rendszer, vagy a Web oldalak karbantartásával kapcsolatos feladatok ellátásához
Rendszergazda	Az intézmény rendszergazdája	Korlátlan jog

(16) A speciális feladatok (pl. telepítések elvégzése), illetve az azokhoz tartozó jogok alapértelmezésben a rendszergazdát illetik meg. Ezek egy-egy jól elhatárolható hálózati adminisztrációs feladat elvégzéséhez rendelhetők, s a rendszergazda beleegyezésével, külön megállapodás alapján más személynek átadhatók. A speciális jogok, illetve az ezekhez tartozó azonosítók magán célra nem használhatók fel. Ezek használata csak a szükséges rendszeradminisztráció erejéig történhet. Az ehhez szükséges kiemelt jogokat a rendszergazda biztosítja. Amennyiben a rendszergazda úgy ítéli meg, hogy a speciális feladatokat ellátó személy a rendszer biztonságát veszélyezteti, úgy joga van a kiemelt jogok használatának lehetőségét felfüggeszteni. Erről, és a felfüggesztés okáról köteles haladéktalanul beszámolni a szervezeti egység vezetőjének.

Adminisztratív biztonság

Az elektronikus informatikai biztonsággal kapcsolatos engedélyezési eljárás során az új vagy módosított elektronikus adatkezelő rendszerek vagy szolgáltatások információ biztonsági szempontból vizsgálat alá kerülnek. A vizsgálat lehet műszaki ellenőrzés üzemeltetés közben, lehet teszt futtatása, lehet dokumentumok ellenőrzése és az alkalmazásba vétel jóváhagyása. Az új vagy módosított elektronikus adatkezelő rendszer engedélyezésre az informatikai rektorhelyettes elé kerül, aki szükség esetén az RT elé terjeszti az engedélyezésre váró rendszert, vagy saját hatáskörben dönt annak engedélyezéséről. A jóváhagyást írásban megküldi az IO osztályvezetőnek, aki az engedély birtokában beüzemeli a rendszert.

Személyekkel kapcsolatos biztonság

4. §

(1) Az egyetem biztonsági szabályozásában szereplő információbiztonsági irányelveknek meg kell jelenniük a munkaköri leírásokban. A munkaköri leírások biztonsággal kapcsolatos részeinek kidolgozása során mérlegelni kell az adott munkatárs érintettségét.

(2) Minden munkatársnak és az egyetemmel kapcsolatba kerülő, az informatikai rendszert használó külső személy titoktartási nyilatkozatot kell aláírnia, melyben nyilatkozik, hogy a munkája során tudomására jutott, az egyetem számára értéket jelentő információt, sem a munkavégzése alatt, sem annak befejezése után nem hozza harmadik fél tudomására.

(3) Amennyiben a felhasználók bármilyen biztonsági incidensre, biztonsági hiányosságra vagy szoftver, illetve hardver hibára utaló jelet tapasztalnak, azt haladéktalanul jelenteniük kell az informatikai osztályvezetőnek.

(4) A felhasználó azonosítása – hitelesítése – minden informatikai rendszer biztonságának alapja. Az Óbudai Egyetem központi informatikai szolgáltatásait különböző szintű, a veszélyeztetettséggel és az általa kezelt adatok érzékenységével arányos hitelesítési rendszerrel kell ellátni. A felhasználói neveket és jelszavakat az ügyfél és a szolgáltatást nyújtó szerver között titkosítva kell továbbítani. Ennek

technikai feltételeit az Informatikai Osztály biztosítja. Az Óbudai Egyetem dolgozói belépésükkel egyidőben felhasználói azonosítót szereznek a központi szolgáltatásokhoz. Ezzel a felhasználói azonosítóval az alapjogok birtokosa lesz, vagyis használhatja az Óbudai Egyetem hálózatát, eléri az Internetet, levelezni tud a központi levelező szerveren, és lehetővé válik az oktatáshoz, munkához szükséges adatok elérése. Az Óbudai Egyetem hallgatója a beiratkozáskor megkapja a Neptun kódját, amellyel tanulmányai befejezéséig rendelkezik a számára szükséges alapjogokkal. Az alapjogokhoz használt jelszó feleljen meg a következő szabályoknak: a jelszó hossza nem lehet rövidebb 8 (nyolc) karakternél, tartalmaznia kell legalább egy számot és egy nagybetűt. Az alapjogok birtokosa, jelszavát saját elhatározásból korlátozás nélkül cserélheti.

(5) A Neptun adminisztrátorok különleges jogokkal rendelkeznek. Figyelembe véve, hogy a kezelt adatok személyiségi jogokat érintenek, valamint hogy a Neptun rendszer kiemelten védett központi szolgáltatás, indokolt a speciális felhasználók különleges jogokkal történő ellátása. A Neptun rendszerben adminisztratív tevékenységet folytató munkatársak azonosítása RSA Token segítségével valósul meg. A hitelesítő rendszer segítségével egy folyamatosan változó kódkombináció biztosítja a kezelő bejutását a rendszerbe, titkosított, biztonságos csatornán keresztül. A bejutást a hitelesítő rendszer és a Neptun rendszer is naplózza, valamennyi tevékenység tárolódik, és visszakereshető. RSA Tokent munkakört váltó vagy kilépő dolgozó nem adhat át másnak, személyesen kell leadnia az IO vezetőjének.

(6) A gazdasági adminisztrátorok különleges jogokkal rendelkeznek. Figyelembe véve, hogy a kezelt adatok személyiségi jogokat érintenek, valamint hogy a gazdasági rendszer kiemelten védett központi szolgáltatás, indokolt a speciális felhasználók különleges jogokkal történő ellátása. A gazdasági rendszer külön tűzfallal védett, az Óbudai Egyetem hálózatában. A hitelesítő rendszer egyedi jogokat biztosít a különböző feladatok végrehajtóinak.

(7) Az Informatikai Osztály munkatársai az alapjogokon felül, üzemeltetési feladataiknak megfelelően többletjogokkal rendelkeznek. Az egyetem központi szolgáltatásait biztosító szerverekhez egyedi azonosítóval férhetnek hozzá, amelyeket a rendszer naplózza. A központi szolgáltatásokat végző szerverek adminisztrátori jelszavait zárt borítékban páncélkazettában kell őrizni. A páncélkazettához csak az IO osztályvezetőnek, és az informatikai rektorhelyettesnek lehet kulcsa.

Eszközökkel kapcsolatos biztonság
5. §

(1) Az eszközök elhelyezésénél figyelembe kell venni a biztonsági követelményeket, hogy a természeti hatásokból, fizikai környezet változásaiból eredő kockázatok minimálisak legyenek. Megfelelő fizikai környezet megakadályozza a jogosulatlan hozzáférést is az informatikai eszközökhöz.

(2) Az eszközöket a strukturált hálózat szabályainak és helyi sajátosságok figyelembe vett adottságának megfelelően kell elhelyezni. Fokozottan védett adatokkal dolgozó rendszerek elhelyezésére különös figyelmet kell fordítani.

(3) A különböző fizikai, környezeti hatások, egyéb események, amelyek az Óbudai Egyetem informatikai rendszerére hatással lehetnek:

a) lopás,
b) tűz,
c) robbanás,
d) füst,
e) vízbetörés,

f) áramellátás zavara, megszakadása,
g) por,
h) telephelyek közelében végzett földmunkák.

Védett helyiségekben is, ahogy az egyetem egész területén, tilos a dohányzás, továbbá tilos enni, inni.

(4) Az informatikai eszközöket védeni kell az áramellátás zavaraiból, megszakadásából származó meghibásodás, és/vagy hibás működés ellen. Az alkalmazott áramellátás kialakításánál tekintetbe kell venni az eszköz gyártójának előírásait, a szükséges rendelkezésre állás mértékét, és az anyagi lehetőségeket.

(5) Az informatikai eszközöket, a gyártó által előírt környezeti paramétereket biztosító helyiségben kell elhelyezni, ennek érdekében a védett helyiségekben légkondicionáló berendezéssel biztosítani kell az előírt hőmérsékletet és páratartalmat.

(6) A strukturált kábelezés biztosítja, hogy az Óbudai Egyetem telephelyein, a telekommunikációs és áramellátó vezetékezést külön tálcában, egymástól elválasztottan vezessék. A nem strukturált hálózatok építésekor, javításakor figyelemmel kell lenni arra, hogy a szétválasztás lehetőség szerint megtörténjen. A kábeleket csatornán kívül vezetni nem szabad, még ideiglenes megoldásként sem.

(7) A számítógépes hálózat végződéseit (fali aljzatait) az aktív hálózati elemeken adminisztrálni kell, a használaton kívüli végződéseket az aktív eszközökön, szoftveres módon tiltani kell, hogy illetéktelenek ne férhessenek hozzá.

(8) A biztonsági követelmények (rendelkezésre állás, sértetlenség) teljesítése érdekében az eszközök rendszeres karbantartásáról gondoskodni kell.

a) A gyártó ajánlásainak figyelembe vételével, illetve a szoftver frissítés szempontjainak figyelembe vételével kell a karbantartást végezni.
b) Csak arra felhatalmazott személy végezheti a karbantartást, és a szükséges javítási munkákat.
c) Az ütemezett karbantartási munkákat előzetesen be kell jelenteni, amennyiben a karbantartás idejére szolgáltatás kimaradása várható.
d) A hibákat és rendszerleállásokat és a tervezett karbantartási munkákat dokumentálni kell.

(9) A személyes használatban lévő munkaállomások, laptopok karbantartását végezheti a felhasználó saját maga, ha ehhez a szükséges ismeretek birtokában van, vagy a karbantartással megbízott informatikai szaktudással rendelkező dolgozó. Az adathordozón tárolt adatok biztonságáért, minden esetben a felhasználó felel.

(10) Otthoni munkavégzés során is be kell tartani a biztonsági szabályokat. Alapvető szabály, hogy a távoli hozzáférés esetében a minimális biztonsági követelmény, hogy a hitelesítés során használt jelszó, a hálózaton titkosított formában haladjon, amennyiben ez lehetséges, akkor az adatforgalmat is titkosítani kell (VPN használata).

Üzemeltetés biztonsági vonatkozásai

6. §

(1) Az Óbudai Egyetem informatikai infrastruktúrájának és központi szolgáltatásainak üzemeltetését részben papíron, részben elektronikus formában dokumentálni kell. A dokumentálásnak ki kell terjednie a következőkre:

a) konfigurációkezelésre,
b) ügyeleti rendszer biztosítására,

c) telefonszámok, elérhetőségek váratlan események kezelésére,
d) rendszerleállások, újraindítások kezelésére,
e) külső üzemeltetőkkel történő kapcsolattartásra.

(2) Kapacitás felügyelet: az informatikai eszközök kapacitását folyamatosan felügyelni kell. A jövőbeli kapacitásigényeket a jelenlegi helyzetnek és az elvárásoknak megfelelően kell megtervezni.
Valamennyi központi szolgáltatás igénybe vételekor, a felhasználó tudomására kell hozni, hogy a közös tárolókapacitásokból mekkora rész jut rá, és tájékoztatni kell arról is, hogy kapacitáshiány esetén miképpen tud helyet felszabadítani. Külön kérésre az IO többletkapacitást biztosíthat a munka folytatásához.

(3) Javítások, frissítések: a rendszerek javítása, frissítése kiemelten fontos feladat, melyet a központi szolgáltatásokat ellátó rendszerek esetében az Informatikai Osztály lát el. A szervezeti egységeknél üzemelő számítógépek karbantartását, a szoftver telepítések javítását és a frissítések elvégzését a telephelyi operátor támogatásával a szervezeti egység saját – informatikai feladatokkal megbízott – munkatársa végzi.

(4) Vírusvédelem: meg kell tenni minden lehetséges lépést a veszélyes programok által okozott incidensek kiküszöbölésére. Ennek érdekében hatékony vírusellenőrző alkalmazásokat kell telepíteni mind a munkaállomásokra, mind pedig a szerverekre és határvédelmi eszközökre.

a) A felhasználóknak be kell tartaniuk a vírusvédelemre vonatkozó elemi szabályokat, és az egyéb intézkedéseket. Tisztában kell lenniük azzal, hogy vírusfertőzést kapni csak egy a biztonsági kockázatok közül. Előfordulhat, hogy a felhasználó maga válik vírusgazdává, ezzel veszélyeztetve a környeztében dolgozó munkatársait, és a hálózat többi felhasználóját, illetve az Internetre kikerülve ismeretlen felhasználókat is.
b) Az egyetem Informatikai Osztálya minden évben biztosítja valamennyi dolgozója számára a legfrissebb vírusvédelmi szoftver legális használatát, a munkahelyi és egy otthoni munkaállomáson egyaránt. A munkahelyi munkaállomáson az Informatikai Osztály által javasolt vírusvédelmi rendszert kötelező használni. A laborokban elhelyezett számítógépek vírusvédelméről a laborfelelősöknek kell gondoskodni. A vírusvédelmi szoftver frissítéséről és a védelmi adatbázis aktualizálásáról a felhasználónak kell gondoskodnia.
c) Az egyetem központi rendszereit külön vírusszűrő szoftverek védik. Az Informatikai Osztály feladata, hogy a védelmi szoftverek automatikusan frissüljenek.
d) Nem ellenőrzött forrásból származó állományokat használat előtt ellenőrizni kell.
e) Az IO dolgozóinak (rendszergazdáknak) tájékoztatnia kell a felhasználókat a vírusok felbukkanásáról, a velük szemben követendő magatartásról, illetve az időnként terjedő hamis vírusfenyegetettségről.
f) A felhasználónak TILOS lánclevelet, hamis vírusriasztásokat (hoax) küldeniük a központi levelező rendszeren keresztül.
g) Vírusfertőzésről, mint biztonsági incidensről, az Informatikai Osztályt értesíteni kell abban az esetben is, ha a vírus terjedését sikerült helyben megakadályozni.

(5) Kéretlen levelek, reklámok **szűr**ése (Spam): a kéretlen levelek központi szűréséről az Informatikai Osztály üzemeltetésében álló szerverek gondoskodnak. A levelek kéretlennek minősítése egy folyamatos valószínűségi skálán történik, amely pontszám alapján 3 csoportba sorolja a leveleket:

a) nem gyanús: változatlanul továbbítjuk a címzettnek,
b) gyanús: megjelölve továbbítjuk a címzettnek,
c) nagy biztonsággal spam: karanténba kerülnek, és a címzett tájékoztatást kap a visszatartott levélről, melyet a karanténban megtekinthet. A levél egy hónap múlva törlődik.

Hálózat menedzsment
7.§

(1) Óbudai Egyetem Intranet üzemeltetése: az Óbudai Egyetem belső hálózatán használt központi szolgáltatások, telephelytől függetlenül kliens-szerver alapúak, amelyek nagymértékben függenek a hálózat működési paramétereitől, ezért a hálózat védelme és folyamatos működése, valamint annak felügyelete az egyetem alapvető érdeke. Ezeknek az elvárásoknak a kielégítése érdekében a belső hálózat menedzselését meg kell oldani. Azokon a telephelyeken, ahol a strukturált hálózat kialakítása megtörtént egy Web alapú SNMP protokollt használó, saját fejlesztésű menedzsment szoftver került alkalmazásra. A többi telephelyen hagyományos módon, egyedi ellenőrzésekkel kell a feladatot mindaddig ellátni, amíg az adott telephely hálózata nem biztosítja a szoftver használatát.

(2) Az Óbudai Egyetem Intranet ellenőrzése során végzendő feladatok:

a) a hálózat működőképességének folyamatos felügyelete és a meghibásodás naplózása,
b) a hálózat meghibásodása esetén a hibaelhárítás haladéktalan megkezdése,
c) aktív hálózati elem meghibásodása esetén a csereeszközről kell gondoskodni,
d) folyamatos statisztika készítése a forgalmi adatokról.

(3) Határvédelmi eszközök üzemeltetése: az Óbudai Egyetem telephelyeinek hálózatait az Internettől és a többi telephelytől tűzfal funkciójú eszközök választják el. A tűzfalak szabályrendszereinek kialakítása a telephelyi adottságok figyelembevételével, a tűzfalak beállításainak folyamatos karbantartása, a naplók elemzése, a szükséges intézkedések megtétele az Informatikai Osztály feladata:

a) határvédelmi eszközök üzembiztonságáért az IO felel,
b) valamennyi telephelyen, a lehetőség szerint törekedni kell a határvédelmi eszközök azonos beállításáról, a naplózás rendjének betartásáról,
c) gondoskodni kell a betörési kísérletek kiszűréséről,
d) garantálni kell a hálózati szegmensek integritását.

(4) Biztonsági mentések: az üzembiztonság fenntartása, az adatok védelme érdekében a központi informatikai szolgáltatásokat ellátó rendszerek biztonsági mentéséről az Informatikai Osztálynak folyamatosan gondoskodnia kell. A biztonsági mentésnek ki kell terjednie az alábbi aktív- vagy szerver feladatokat ellátó eszközökre:

a) hálózati switch-ek, routerek és vezeték nélküli hozzáférési pontok (aktív eszközök),
b) tűzfal szabálylistája,
c) névkiszolgálók adatbázisa (DNS),
d) Neptun adatbázis,
e) központi levelezés,
f) központi címtár,
g) központi weboldalak,
h) pénzügyi szoftverek.

A biztonsági mentések adathordozóit az adatok keletkezési helyétől eltérő helyen kell tárolni, amiről az Adatvédelmi Szabályzat rendelkezik.

(5) A mentések végrehajtásának menete: a biztonsági mentések során olyan eljárást kell alkalmazni, amely egyértelműen biztosítja, hogy a tároló médiára az adatok sértetlenül és visszaolvashatóan felírásra kerüljenek. Fokozott figyelmet kell fordítani a vezetői levelező szerver mentésére, valamit fokozott figyelemmel kell gondoskodni a Neptun hallgatói nyilvántartó rendszer adatbázisáról. A gazdasági rendszer napi mentéséről a szerverre telepített backup szoftver gondoskodik, a pénzügyi-számviteli szerver minden munkanapon automatikusan mentődik az erre a feladatra dedikált gépen.

(6) Archiválás: a mentések során el kell különíteni azokat az adatokat, amelyek a törvényi előírásnak megfelelően meghatározott ideig (de mindenképpen hosszabb pl. 5-10 év) kötelezően megőrzendőek. Ezeket az adatokat tekintjük archiváltnak. A napi vagy heti, de mindenképpen ismétlődő és meghatározott idő elteltével felülíródó adatoktól elkülönítve kell tárolni az archíválásra kijelölt adatokat. Külön gondot kell fordítani a gazdasági és személyi adatokat tartalmazó mentésekre, illetve archiválásokra. Ezért az egyetem külön archiváló adattárolót üzemeltet, amely kifejezetten a hosszútávú megőrzésre szánt adatok tárolását végzi.

Elektronikus levelezéssel kapcsolatos biztonsági szabályok
8. §

(1) Az egyetem valamennyi munkatársa jogosult felhasználói jogosultságot igényelni az elektronikus levelezéshez, vagyis a dolgozó munkába lépésekor a szükséges formanyomtatvány kitöltésével és aláírásával a központi levelezési rendszer tagjává válik. A formanyomtatványon és a mellékelt használati utasításon minden szükséges információt megkap, ami a levelező rendszer biztonságos használatához szükséges.

(2) Az elektronikus levelezés szolgáltatás használata során az alábbi szabályokat kell betartani:

a) A felhasználó tudomásul veszi, hogy a központi levelezés során a felhasználó levelezési forgalma naplózásra kerül.
b) A levelezési szolgáltatás mind a munkatársak közötti, mind az egyetemen kívüli kapcsolattartásra felhasználható.
c) Az elektronikus levélhez fájl csatolható, amelynek mérete korlátozott.
d) Az elektronikus levélhez csatolt fájl nem lehet futtatható állomány, nem lehet tömörített csomagban futtatható állomány, nem lehet továbbított reklám.
e) A felhasználó tudomásul veszi, hogy a levélcím kötött, és nem változtathatja meg.
f) A levelezési rendszeren tilos biztonsági szempontból érzékeny anyagot, egyetemi titkot, vagy üzleti titkot kijuttatni az Internetre.
g) Tilos a levelezési rendszeren keresztül olyan tartalmú levelet küldeni, amely bármilyen más személy, csoport vagy társaság személyes, illetve üzleti érdekeit sértheti.
h) Az elektronikus levelezési jogosultsággal rendelkező felhasználó csak saját nevében küldhet levelet, kivéve, ha erre felelős vezető utasítja.
i) Az egyetem teljes címtára felhasználásával egyetemi szintű körlevelet csak az Informatikai Osztályvezető küldhet, a levélmintát neki kell eljuttatni.
j) Tilos rasszista, szemérmet és jó ízlést sértő, valamint szélsőséges politikai nézeteket képviselő tartalmú levelet küldeni.

(3) Az Internet használattal kapcsolatos szabályok: az egyetem belső hálózatába működő munkaállomások alaphelyzetben Internet eléréssel rendelkeznek. Kivétel alá esnek, és így az Internetet nem érhetik el, a gazdasági szoftvereket használó, és különösen érzékeny adatokkal dolgozó munkaállomások.
Felhasználói jogosultsággal azok a munkatársak rendelkeznek, akik valamilyen központi szolgáltatást használnak munkájuk során. Ilyenek például a Tanulmányi Osztály dolgozói, akik napi munkájuk döntő részében a Neptun Egységes Tanulmányi Rendszer bejelentkezett felhasználói.
Az Internet használata során az egyetem fenntartja a jogot arra, hogy a felhasználók Internet forgalmát figyelemmel kísérje, és naplózza.
A felhasználónak tisztában kell lennie azzal, hogy az Internet használata biztonsági kockázattal jár, ami nem csak a személyes használatában lévő munkaállomást veszélyeztetheti, hanem a hálózat egyéb

eszközeit is. A felhasználónak tisztában kell lennie azzal is, hogy nem használhatja az Internet elérés lehetőségét törvények és szabályok tudatos vagy szándékos megsértésére.
Az Internetről letöltött szoftver vagy fájl jogtisztaságáért az egyetem, mint jogi személy felel, ezért fenntartja jogot, hogy a szabályok megsértőivel szemben szankciókat alkalmazzon. Illegális tevékenység céljára használt Internet elérés fegyelmi eljárást eredményezhet.

(4) Az Internet használata során elvárható magatartás:

a) A felhasználó nem titkolja el személyazonosságát az Internet használat közben.
b) Az egyetem dolgozói nem nyilváníthatnak véleményt az egyetem tevékenységével, szolgáltatásaival kapcsolatban jóváhagyás nélkül.
c) A felhasználók tudomásul veszik, hogy a szabadalmakra és egyéb szellemi tulajdonra vonatkozó szabályok alkalmazása az Internetre is vonatkozik.
d) A szellemi tulajdon védelme az Internetre is kiterjed.
e) Az egyetem laboratóriumaiban az éppen órát tartó tanár döntheti el, - hogy egy erre a feladatra készített speciális szoftver segítségével, - engedélyezi, vagy tiltja a laborban működő munkaállomások Internet elérését.
f) Az egyetem WiFi hálózata biztonsági megfontolásból többszörös védelemmel rendelkezik, de alapvetően engedélyezi az Internet elérését.

Hozzáférés ellenőrzése
9. §

(1) Felhasználók regisztrálása: az egyetem dolgozóinak döntő többsége napi munkája során hálózatba kötött munkaállomáson végzi el a feladatait. Ezért a munkaállomásokon központosított felhasználó regisztrálás nem történik. Minden személyes használatban lévő munkaállomáson szabadon választható a regisztráció.

(2) A központi szolgáltatások esetében a regisztráció kötelező, és a feladatok függvényében a jogosultságok hierarchiája valósul meg. Minden felhasználó csak annyi jogot kap, amennyi a feladata elvégzéséhez szükséges. Különösen védett adatok esetében a személyes regisztráción felül, a titkosított csatorna használatához is szükséges azonosítót alkalmazni.

(3) A felhasználói jelszavak generálásának, átadásának bizalmasan kell történnie, a kezdeti jelszót a felhasználó szabadon megváltoztathatja, aminek gyakoriságát a rendszer nem szabályozza. A jelszavak kiválasztásánál a következő alapvető szabályokat kell betartani:

a) Tilos könnyen kitalálható jelszavakat választani!
b) Tilos a LOGIN nevet jelszóként használni!
c) Tilos a vezetéknevet és a keresztnevet jelszóként használni!
d) Tilos azonos számokból, vagy betűkből álló jelszót használni!
e) Tilos a jelszót nyilvános helyen kiírva tartani (monitorra ragasztva)!
f) Ajánlott a számok és betűk keverése jelszavak használatakor.
g) Ajánlott a kis és nagybetűk keverése jelszavak használatakor.

(4) A Neptun Egységes Tanulmányi rendszer kitüntetett felhasználóinak (TO dolgozói, Neptun adminisztrátorok) RSA token használata kötelező. Az RSA token használatához szükséges jelszó az RSA szerveren tárolódik és azonosítja a token használóját. Amennyiben illetéktelen felhasználó három alkalommal hibás jelszóval próbál bejelentkezni, a rendszer automatikusan letiltja a tokent, és a bejelentkezés meghiúsul. Ilyen letiltott tokent csak a rendszergazda tud újraszinkronizálni, az esemény naplózódik.

(5) A központi levelező szerver felhasználói azonosítása az LDAP adatbázisban tárolt adatok alapján történik. Az alkalmazott szabály értelmében a jelszónak legalább 8 karakter hosszúnak kell lennie, tartalmaznia kell legalább egy nagybetűt, és egy számjegyet.

(6) Az egyetem WiFi (vezeték nélküli) hálózatában a felhasználók két nagyobb csoportra lettek osztva. Az egyik csoportba tartoznak az egyetem dolgozói, mindazok a felhasználók, akiknek LDAP azonosítójuk van. A másik csoportba tartoznak a hallgatók, akinek Neptun kódjuk van. Különleges alkalmi csoportot alkothatnak a vendégek, akinek a WiFi hálózat használatához ideiglenes regisztrációt generál az IO.

(7) A rendszergazda a szervereket nem hagyhatja magára, és a feladata elvégzése után ki kell jelentkeznie a rendszerből.

Távoli elérés
10. §

Külső elektronikus rendszerek

Külső, azaz nem egyetemi, elektronikus rendszerek üzemeltetése során a távoli elérést biztosító eszköz működéséhez az egyetem biztosít IP címet. Az eszköz a külső elektronikus rendszert működtető cég tulajdonában van, és egyben működtetésének felelőssége is a céget terheli. Kötelezően elvárt biztonsági beállítás, hogy az eszköz default jelszavát az üzemeltető változtassa meg.

(1) Virtuális privát hálózati szolgáltatás (VPN): nyílt hálózaton, például Interneten keresztül történő kapcsolatfelvétel esetén virtuális magánhálózat alkalmazása szükséges. Telefonos kapcsolatfelvételt az egyetem hálózata nem támogat. Távoli bejelentkezés esetében is ugyanazokat a biztonsági szabályokat kell betartani, mint a munkahelyen használt egyéb számítógépek esetén.

(2) A biztonság fokozása érdekében az Óbudai Egyetem informatikai hálózatának távoli, használatakor VPN-t kell alkalmazni. Az egyetemen kétféle VPN szolgáltatást kell működtetni:

a) A Neptun biztonságát szolgáló VPN: Minden felhasználójának saját RSA token-t és felhasználói nevet kell igényelnie, amelynek kiadásáról és ellenőrzéséről az Informatikai Osztály gondoskodik.
b) Általános célú VPN szolgáltatás: Minden felhasználónak saját SSL tanúsítványt, és kapcsolódási profilt kell igényelnie. A kapcsolódáshoz szükséges felhasználói név és jelszó a Központi Címtárban tárolódik.

Rendszerhasználat felügyelete (monitoring)
11. §

Az egyetem rendszer és kommunikáció védelmi eljárásrendje összhangban van a hatályos törvényekkel, vezetői döntésekkel, direktívákkal, szabályzatokkal, rendelkezésekkel, szabványokkal és útmutatókkal. A rendszer és kommunikáció védelmi szabályzat részét képezi a szervezet általános informatikai biztonsági szabályzatának. A rendszer és kommunikáció védelmi eljárásrendet ki kell fejleszteni általánosan, és egy bizonyos informatikai rendszerhez is, ha szükséges. (lásd Neptun)

A rendszer és kommunikáció védelem megköveteli az egyetemi rendszerek folyamatos elektronikus ellenőrzését, a naplózást.

(1) A naplózást az egyetem minden központi szolgáltatást futtató eszközén, valamint a határvédelmi eszközökön alaphelyzetben engedélyezni kell. A szerverek, hálózati eszközök, valamint a biztonsági rendszer eleminek naplóállományait rendszeresen ellenőrizni kell, és a biztonsági megfontolásokat figyelembe véve meghatározott ideig tárolásáról gondoskodni kell.

(2) A naplózási funkciónak rögzítenie kell legalább a következőket:
a) a rendszer leállását és újraindulását,
b) a rendszerben fellépő hibákat,
c) felhasználó bejelentkezést, vagy sikertelen bejelentkezési kísérleteket,
d) tranzakció végrehajtását,
e) új felhasználó felvételét, törlését,
f) a naplóállományok törlését.

(3) A központi szolgáltatások, és a határvédelmi eszközök, valamint kritikus informatikai eszközök egy riasztórendszerhez kapcsolódnak. A riasztórendszer automatikus SMS küldéssel reagál a rendszerhibákra, és minden olyan eseményre, ami a normális működéstől eltér. Az SMS-ek a felügyelettel megbízott rendszergazdák mobiltelefonjára érkeznek munkaidőben és munkaidőn kívül is. Az SMS-ek érkezése után a rendszergazdának haladéktalanul meg kell kezdenie a hiba felderítését, és elhárítását.

(4) Az Óbudai Egyetem informatikai rendszerinek esetleges hosszabb idejű működésképtelensége esetén az egyetem Katasztrófa-elhárítási Terve szerint kell eljárni. Ennek megfelelően kell mindent megtenni a rendszer minél gyorsabb helyreállítása és a folyamatos üzemmenet biztosítás érdekében. A Katasztrófa-elhárítási Terv tartalmazza azokat a külső szerződő partnereket, akiknek katasztrófa esetén adott idő áll rendelkezésére, hogy a szerződésben szereplő eszközöket, vagy egyéb informatikai berendezéseket a megadott időn belül kijavítsa, vagy helyettesítésükről gondoskodjon.
Katasztrófa, vagy kritikus helyzet minél gyorsabb megoldása érdekében, a portaszolgálatoknak tudomására kell hozni azoknak a munkatársaknak a névsorát, akik bármikor, vagyis akár a lezárt épületekbe is bejuthatnak. Ez vonatkozik a munkaszüneti napokra, ünnepekre, és a munkaidőn kívüli időre (éjszaka) is.

(5) A szabályzat megsértésének gyanúja esetén az esetet ki kell vizsgálni, és a kijelölt felelősnek meg kell tennie a szükséges intézkedéseket, amelyre a következők az irányadók:
a) A szabályzat előírásainak nem ismerete nem mentesít a következmények vállalásának kötelessége alól.
b) A szabályzat gondatlan megszegése esetén az elkövetőt figyelmeztetésben kell részesíteni.
c) A szabályzatnak egy figyelmeztetést követő ismételt megsértése szándékos elkövetésnek minősül.
d) A szabályzat szándékos megsértése esetén az elkövető a hálózat használatából ideiglenesen vagy véglegesen kizárható, és az eset súlyosságától függően fegyelmi eljárás folytatható le ellene.
e) A szándékos elkövető köteles megtéríteni az általa okozott károkat a Polgári Törvénykönyv előírásai szerint.
f) Ha az elkövetett cselekedet kimeríti valamely hatályos magyar törvény tényállását, akkor a felelősnek kötelessége megtenni a megfelelő törvényi lépéseket.
g) A felelősnek kötelessége tájékoztatni az Informatikai Osztályt és az adott szervezeti egység vezetőjét a szabályzat súlyos megszegéséről.

(6) A szabályzat elkészülte és bevezetése után gondoskodni kell annak folyamatos, a változásokat követő fejlesztéséről. Legalább évente felül kell vizsgálni, hogy a benne foglaltak időszerűek, érvényesek-e, és a felmerülő új kihívásokra új válaszokat kell adni a szabályzatban.

III. rész

Hatályba léptető és záró rendelkezések

12. §

(1) Az Óbudai Egyetem Informatikai biztonsági szabályzatát a Szenátus 2014. június 16-ai ülésén megtárgyalta és elfogadta. Jelen 2. verziószámú szabályzat 2014. július 1-jén lép hatályba.

(2) Az Óbudai Egyetem Informatikai Biztonsági szabályzatát az egyetem honlapján nyilvánosságra kell hozni, és hozzáférhetővé kell tenni.

Budapest, 2014. június 17.

Prof. Dr. Fodor János
rektor

Fogalmak

- Aktív hálózati eszköz: kapcsolók (switch-ek), forgalomirányítók (router-ek), vezeték nélküli hozzáférési pontok és egyéb eszközök, amelyek segítségével a hálózat üzemvitele biztosítható.
- Csomópont: szerver feladatokat ellátó eszközök és aktív eszközök csoportja, az informatikai szolgáltatások ellátására.
- DNS: az internet neveket és címeket egymáshoz rendelő adatbázis, amely általában külön kiszolgáló gépen fut.
- Felhasználó: az a természetes személy, aki az Informatikai Infrastruktúrát használja.
- Felhasználói azonosító: az intézményi címtárban tárolt egyedi azonosításra szolgáló rövid karaktersorozat, amely általában a felhasználó nevéből képződik.
- Felhasználói kód: az Egységes Tanulmányi Nyilvántartó Rendszerben (NEPTUN) létező, betűkből és számokból álló 6 karakter hosszúságú kód.
- Hálózat: felhasználói számítógépek és/vagy szerverek közötti adatátvitelt biztosító passzív és aktív eszközökből álló infrastruktúra.
- **Informatikai erőforrások**: a hardver, szoftver eszközök összessége.
- Internet: a világháló.
- Intranet: az intézményen belüli hálózat és annak szolgáltatásai.
- IP telefónia: olyan számítógép-hálózati alkalmazás, amely dedikált eszközök (készülék és központ) segítségével telefonszolgáltatást tesz lehetővé. Ez a hagyományos telefonközpontokat felváltó számítógépes rendszer.
- Központi címtár: az egyetem dolgozóinak felhasználói adatit tároló LDAP adatbázis.
- Központi szolgáltatások: levelezés, címtár, fájl kiszolgálás, Web szolgáltatás, névszolgáltatás, stb.
- LDAP (Light Weight Directory Access Protocol): nyílt szabványú címtár struktúra leíró nyelv.
- NIIF (Nemzeti Információs Infrastruktúra Fejlesztési Iroda): az iroda a teljes magyarországi kutatási, felsőoktatási és közgyűjteményi közösség számára biztosít integrált országos számítógép-hálózati infrastruktúrát, valamint erre épülő kommunikációs, információs és kooperációs szolgáltatásokat, élvonalbeli alkalmazási környezetet, és tartalom-generálási ill. tartalom-elérési hátteret.
- Passzív eszközök: hálózati kábelezés és csatlakozók.
- Számítógép: olyan informatikai eszköz, amelyet a felhasználó a napi munkája során használ, és amellyel igénybe veheti a hálózat szolgáltatásait.
- Szerver feladatokat ellátó eszköz: olyan számítógépek, szoftverek, vagy speciális eszközök, amelyek különböző szolgáltatásokat biztosítanak más számítógépek számára.
- Szerverszoba: fokozottan védett, naplózott bejutású, klimatizált, zárt helyiség, ahol a folyamatos működés feltételei az informatikai erőforrások számára biztosítottak.
- **Tűzfal**: olyan kiszolgáló eszköz (számítógép vagy program), amelyet a helyi és a külső hálózat közé, a csatlakozási pontra telepítenek, annak érdekében, hogy az illetéktelen behatolásoknak ezzel is elejét vegyék. Emellett lehetővé teszi a kifelé irányuló forgalom ellenőrzését is.
- VLAN: a hálózat egy meghatározott, a feladatoknak megfelelően logikai csoportba szervezett része.
- VPN szolgáltatás: speciális hálózati elérés, amely az egyetem hálózatához titkosított, és hitelesített kapcsolatot tesz lehetővé a világ bármely részéről.
- WiFi (Wireless Fidelity): olyan szabványos vezeték nélküli adatátviteli technika, amely a 11-108 Mbps-os tartományban működik. A szabad frekvenciatartományt használó rendszer átviteli sebessége nagymértékben függ a rádióhullámok terjedési környezetétől (akadályok, távolság). Legtöbb notebook, laptop számítógép és okostelefon gyárilag rendelkezik ilyen kapcsolódási lehetőséggel.