REKTOR

Telekommunikációs és Informatikai Osztály	
Érk.: 2014.09.01.	
Ikt. sz.: 170.461/2014	
Tételsz.:	Ügyint.:

GMF14000234

15/2014. (VIII. 28.) számú Rektori Utasítás

A Budapesti Műszaki és Gazdaságtudományi Egyetem Informatikai Biztonsági Szabályzata

2014. augusztus 28.

Budapesti Műszaki és Gazdaságtudományi Egyetem
1111 Budapest, Műegyetem rkp. 3.
Postacím: 1521 Budapest

Rektori Kabinet • Központi Épület I. emelet 2.
Telefon: 463-2221, Fax: 463-2220
E-mail: rekikt@rektori.bme.hu

TARTALOMJEGYZÉK

Összefoglaló

Az Informatikai Biztonsági Szabályzat jelen változata a korábbi Rektori Utasítás szerinti szabályzatot néhány — az informatikai rendszerek besorolását nem változtató — esetben pontosítja. A szabályzatban hivatkozott MSZ ISO/IEC 27001:2006 szabvány is változott néhány ponton, a jelenlegi szabályzatban áttekintettük ezeket a változtatásokat, ezek nem igényeltek változtatást a szabályzatban.
Az Informatikai Biztonsági Szabályzat alkalmazása valamennyi olyan informatikai rendszerre alkalmazandó, amelyek a Budapesti Műszaki és Gazdaságtudományi Egyetem központi hálózati infrastruktúráját használja.
A szabályzat szerint kötelező a Telekommunikációs és Informatika Osztály (TIO) beleegyezését és véleményét kérni a következő esetekben:

- a 7.§ 17. pontja szerint új IT rendszer indítása esetében
- a 7.§ 20, 21 pontja szerint külső szervezet IT üzemeltetési megbízása esetében
- a 10.§ szerinti szolgáltatás indítási kérelmek felülvizsgálata a TIO által

A szabályzatban foglalt valamennyi kérdésben az Egyetem bármely szervezete konzultációt kérhet a TIO igazgatójától.

1. §
Általános rendelkezések

(1) Az Informatikai Biztonsági Szabályzat (a továbbiakban: IBSZ) célja, hogy a Budapesti Műszaki és Gazdaságtudományi Egyetem (a továbbiakban: az Egyetem) informatikai rendszerei, így hardver és szoftverállománya vonatkozásában meghatározza az informatikai biztonsággal (az informatikai rendszerekben tárolt információk védelmével és az informatikai rendszerek megbízható működésével) kapcsolatos feladat-, felelősségi és hatásköröket, valamint az Egyetem informatikai biztonságpolitikáját a MSZ ISO/IEC 27001:2006 elvei alapján.

(2) Az IBSZ személyi hatálya kiterjed az Egyetem összes hallgatójára és vele közalkalmazotti, vagy egyéb foglalkoztatásra irányuló jogviszonyban álló személyre (a továbbiakban: dolgozó), valamint mindenkire, aki az Egyetem számítógép-hálózatát vagy informatikai eszközeit, berendezéseit használja.

(3) Amennyiben az Egyetem képviseletében eljáró kötelezettségvállalásra jogosult vezető harmadik félnek is lehetőséget biztosít az Egyetem hálózati infrastruktúrájának használatára, a kötelezettségvállalás dokumentumában a harmadik külső harmadik személynek (szervezetnek) kötelezettséget kell vállalnia az IBSZ-ben foglaltak betartására.

2. §
Az IBSZ célja

Az IBSZ célja, hogy egységes és általános értelmezést adjon az informatikai rendszerekben kezelt adatok bizalmassága, hitelessége, sértetlensége, rendelkezésre állása és funkcionalitása biztosítása érdekében követendő irányelvekre. Az irányelvek figyelembevételével meghatározható az informatikai biztonsági szabályozás alapján minősített adatokat kezelő

informatikai rendszerek biztonsági osztályba sorolása. Kidolgozhatóak a konkrét, rendszer szintű informatikai biztonsági szabályozások, amelyek az informatikai rendszer teljes életciklusában meghatározzák a szabványos biztonsági funkciók tervezéséhez, megvalósításához, üzemeltetéséhez és megszüntetéséhez a szükséges alapelveket és követelményeket.

3. §
Értelmező rendelkezések

Az IBSZ alkalmazásában:

Adatvédelem: az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény hatálya alá eső adatkör védelme.

Biztonsági esemény: Az informatikai rendszer védelmi állapotában beállt illetéktelen nem kívánt változás, melynek hatására az informatikai rendszer által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül.

Felhasználó: az informatikai infrastruktúrát használó személy. Minden olyan személy, aki az Egyetem által rendelkezésére bocsátott informatikai infrastruktúrát (IT Rendszert) használja.

GMF: BME Gazdasági és Műszaki Főigazgatóság

Incidens: A szolgáltatás standard működésétől eltérő esemény, mely fennakadást vagy minőségcsökkenést okoz, vagy okozhat a szolgáltatásban.

Intranet: az Egyetemen belüli hálózat, az egyetemi hálózaton kívüli hálózatról nem érhető el.

ISO/OSI szabvány: A Nemzetközi Szabványosítási Szervezet (ISO) által kibocsátott a nyílt informatikai rendszerek összekapcsolását lehetővé tevő architektúrára vonatkozó ISO/OSI 7498-1 szabvány. Magyar megfelelője: MSZ OSI 7498-1. A nyílt rendszerek biztonsági architektúrájára az ISO/OSI 7498-2 szabvány vonatkozik. Magyar megfelelője: MSZ OSI 7498-1

IT: információ-technológiai (IT) rendszer [information technology (IT) system] információs rendszer (hardver és szoftver) nemzetközi szakkifejezése.

IT szolgáltatás: bármilyen, az Egyetemen használt vagy bevezetni szándékozott IT Rendszerrel összefüggő, azzal kapcsolatos szolgáltatás.

Kiszolgáló/ Szerver: minden olyan számítógép vagy funkció, amely szolgáltatást nyújt felhasználók vagy más számítógépek számára.

Kockázat: A fenyegetettség mértéke, amely valamely fenyegető tényezőből ered, és amelyet a kockázatelemzés során a fenyegető tényezők értékelése révén tárunk fel. A kockázatot a kárnagyság és a bekövetkezés gyakoriság szorzataként definiáljuk egy megadott időtávon.

Probléma: A probléma egy állapot, mely gyakran több hasonló tünetet produkáló incidens alapján ismerhető föl. A probléma azonosítható lehet egyetlen jelentős incidens alapján is, mely valamilyen hibára utal, melynek oka nem ismert, de hatása jelentős.

SLA: Service Level Agreement – Szolgáltatási szint megállapodás egy olyan írásos megállapodás, mely két fél között jön létre: a szolgáltató (az IBSZ alkalmazása során a szolgáltatásért felelős szervezeti egység) és a szolgáltatás felhasználója között. Az SLA meghatározza a két fél között nyújtandó szolgáltatás tartalmát és feltételeit, az egyes szolgáltatásokkal kapcsolatos információvagyon, jogosultságkezelési és használati szabályokat. Mindenfajta változtatás az SLA-k változtatási rendjének megfelelően végezhető. Az SLA-ra vonatkozó részletes szabályokat az Egyetem Informatikai Szabályzata tartalmazza.

TIO: GMF Telekommunikációs és Informatikai Osztály

Üzletmenet-folytonosság és katasztrófa-elhárítás tervezés: Az informatikai rendszer és a benne kezelt adatok, valamint a környezetüket képző összes rendszerelem csoportra vonatkozó védelmi intézkedések meghatározására irányuló tervezési tevékenység üzemzavarok és katasztrófa esetére. A védelmi intézkedések érvényesítésével az adatok védelme és/vagy visszaállíthatósága valósítható meg üzemzavar vagy katasztrófa események estén. Angol nyelvű elnevezése: Business Continuity Planning (rövidítése: BCP) és Disaster Recovery Planning (rövidítése: DRP).

4. §
IT Rendszerek biztonsági osztályai, besorolás

Az Egyetem Informatikai Szabályzatával összhangban:

(1) Az Egyetemen üzemeltetett IT rendszereket az alábbi négy kategória valamelyikébe kell besorolni. A besorolás fő szempontjai: az IT rendszer és az általa kezelt adatok milyen értéket képviselnek, tartalmaznak-e érzékeny, személyes adatokat, illetve mennyire kritikus a működésük az Egyetem egészét tekintve.

(2) ***Kritikus rendszerek:*** („A" osztály) Az Egyetem működése szempontjából kritikus rendszerek, amelyek érzékeny, illetve személyes adatokat tartalmaznak. Adatvédelmi szempontból kiemelt védelmet igényelnek, és az Egyetem működése szempontjából nélkülözhetetlen fontosságú rendszerek:

- Bér- és Munkaügyi Gazdálkodási rendszer: MGR (üzemeltető: GMF, TIO)
- Tanulmányi rendszer: Neptun (üzemeltető: KTH)
- Központi névtár, telefonkönyv (üzemeltető: TIO)
- Központi levelező kiszolgálók (üzemeltető: TIO)
- Központi tárhely-kiszolgálók (üzemeltető: TIO)
- Autentikációs rendszerek (üzemeltető: TIO)
    - Eduroam
    - Címtár

(3) ***Kiemelt rendszerek:*** („B" osztály) Az Egyetem működése szempontjából kiemelt fontosságú rendszerek, amelyek elsősorban technikai jellegűek, a rajtuk tárolt adatok elsősorban nem személyes jellegűek.

- Számítógép hálózat (TIO)
- Technológiai (environment, middleware) rendszerek (SLA szerinti szolgáltatásért felelős szervezeti egység)
- Egyetemi web szerver szolgáltatás (TIO)
- Telefonközpont és a hozzá tartozó kábelhálózat (TIO)

(4) ***Normál rendszerek:*** („C" osztály) Az Egyetem napi működése szempontjából nem kiemelt fontosságú rendszerek. Védendő, akár személyes adatokat is tartalmazhatnak.
- Kiszolgálók (szerverek) (SLA szerinti szolgáltatásért felelős szervezeti egység)
- Kutatói rendszerek
- Hallgatói laborok

(5) ***Egyéb rendszerek:*** („D" osztály) Működésük az Egyetem egészére nincs kihatással. Szűkebb csoport oktatási vagy kutatási munkáját segítik. Ide tartozik minden más, fenti kategóriákba be nem sorolt rendszer.

5. §
Az Egyetem informatikai biztonsági alapelvei

Az IBSZ alkalmazásában informatikai biztonság az az állapot, amikor az informatikai rendszer által kezelt adatok védelme — bizalmasság, hitelesség, sértetlenség, rendelkezésre állás és funkcionalitás szempontjából — zárt, teljes körű, a kockázatokkal arányos és folyamatos.

Információbiztonsági alapelvek

(1) Az Egyetem szolgáltatásért felelős szervezeti egységeinek az „A", „B" és „C" kategóriába sorolt rendszerek által kezelt adatok védelmét bizalmasság, hitelesség, sértetlenség, rendelkezésre állás és funkcionalitás szempontjából úgy kell megvalósítani, hogy az informatikai rendszernek és környezetének védelme folytonos, teljes körű, zárt és a kockázatokkal arányos legyen, valamint a megvalósuljon a zárt szabályozási ciklus, a következők szerint:

a) ***Teljes körű*** a védelem, ha a védelmi intézkedések *az informatikai rendszer összes elemére, az ISO/OSI szabvány szerinti összes rétegére*, valamint a *végpontok közötti összes elemre* kiterjednek.
A **teljes körűségre vonatkozó alapelvet** a fizikai, a logikai és az adminisztratív védelem területén kell érvényesíteni, úgymint:
- az összes információbiztonsági rendszerelem csoportra,
- az informatikai rendszer infrastrukturális környezetére,
- a hardver rendszerre,
- az alap- és felhasználói szoftver rendszerre,
- a kommunikációs és hálózati rendszerre,
- az adathordozókra,
- a dokumentumokra és feljegyzésekre,
- a belső üzemeltetőkre és a külső partnerekre,

- az MSZ OSI 7498-1. szabványban meghatározott nyílt rendszerek architektúrája minden rétegére, azaz mind a számítástechnikai infrastruktúra, mind az informatikai alkalmazások szintjén,
- mind a központi, mind a végponti informatikai eszközökre és környezetükre.

b) ***Zárt* a védelem**, ha *az összes releváns fenyegetés figyelembe lett véve* a védelmi intézkedések megtervezésénél és megvalósításánál. A **védelem zártsága** akkor biztosított, ha a valószínűsíthető fenyegetések elleni védelmi intézkedés megvalósul. A **zárt szabályozási ciklus** úgy érvényesíthető, hogy az adminisztratív védelemmel biztosítani kell a szabályozás, érvényesítés, ellenőrzés és a védelmi intézkedések/szankcionálás zárt folyamatát.

c) ***Kockázattal arányos*** a védelem, ha kellően nagy időintervallumban a védelem költségei arányosak a potenciális kárértékek összegével és a megvalósított védelmi intézkedések következtében a kockázatok elviselhető mértékűre mérséklődtek, azaz ha az informatikai rendszerek által kezelt adatok védelmének erőssége és költségei a felmért kockázatokkal arányban állnak. Célkitűzés a minimális védelmi költséggel elért szükséges maximális védelmi képesség.

d) ***Folyamatos* a védelem**, ha *az időben* változó körülmények és viszonyok ellenére is *megszakítás nélkül* valósul meg. A védelem **folytonosság**a úgy biztosítható, hogy az informatikai rendszerek fejlesztése és megvalósítása során kialakított védelmi képességeket az üzemből történő kivonásig folytonosan biztosítani kell az előírások betartatásának rendszeres ellenőrzésével és az ezt követő védelmi intézkedésekkel.

A fenti (1) bekezdés alkalmazásában:

Rendelkezésre állás: annak a valószínűsége, hogy egy definiált időintervallumon belül az alkalmazás a tervezéskor meghatározott funkcionalitási szintnek megfelelően a felhasználó által használható.

Funkcionalitás: az IT Rendszer megfelelő tervezésének és üzemeltetésének eredményeként az adat tartalmi és formai használhatóságának biztosítása a funkcionális használat követelményeinek megfelelően.

Az informatikai biztonság alapterületei

(2) ***Információvédelem***, amely alatt az IBSZ alkalmazásában az IT Rendszerek által kezelt adatok által hordozott információk védelmét kell érteni a bizalmasság, a hitelesség és a sértetlenség sérülése, elvesztése ellen.

(3) ***Megbízható működés,*** amely alatt az IBSZ alkalmazásában az IT Rendszerek által kezelt adatok által hordozott információk védelmét kell érteni a rendelkezésre állás, és a funkcionalitás sérülése, elvesztése ellen.

6.§
Az Egyetem informatikai biztonsági politikája

(1) Az Egyetem átfogó informatikai biztonságpolitikája minden felhasználó számára egységes értelmezésben azt határozza meg, hogy az IT Rendszerek által kezelt adok bizalmasságának, hitelességének, sértetlenségének, rendelkezésre állásának és funkcionalitásának megőrzésével kapcsolatosan milyen biztonsági struktúrát és elveket kell követni, illetve milyen követelményeket szükséges teljesíteni.

(2) Az Egyetem informatikai biztonságpolitikájának elsődleges célja a működőképesség fenntartása, ezért az olyan felhasználót, aki magatartásával más felhasználók munkáját veszélyezteti, az üzemeltető a szolgáltatásból haladéktalanul kizárja mindaddig, amíg a veszélyt okozó tevékenységét nem szünteti meg. A jelentős súlyú, és/vagy más IT Rendszereket és azok felhasználóit is veszélyeztető esetben a TIO jogosult az egyetemi hálózatból kitiltásra.

SLA: Service Level Agreement – Szolgáltatási szint megállapodás egy olyan írásos megállapodás, mely két fél között jön létre: a szolgáltató (az IBSZ alkalmazása során a szolgáltatásért felelős szervezeti egység) és a szolgáltatás felhasználója között. Az SLA meghatározza a két fél között nyújtandó szolgáltatás tartalmát és feltételeit, az egyes szolgáltatásokkal kapcsolatos információvagyon, jogosultságkezelési és használati szabályokat. Minden fajta változtatás az SLA-k változtatási rendjének megfelelően végezhető. Az SLA-ra vonatkozó részletes szabályokat az Egyetem Informatikai Szabályzata tartalmazza.

(3) Törekedni kell a kockázataink minimalizálására amellett, hogy minden vezetőben és munkatársban tudatosítani kell, hogy tökéletes védelem és biztonság nincsen, és ezzel összefüggésben a maradvány kockázatokat tudatosan vállaljuk.

(4) A felelősségeket az információbiztonság területén hangsúlyozottan meg kell határozni és az egyes informatikai szolgáltatásokban érintettekhez kötni az IBSZ-ben foglaltak szerint.

(5) Hangsúlyozottan törekedni kell a törvényi és jogszabályi megfelelőségre különös tekintettel a személyes adatok kiemelt védelmére. Ennek során az Adatvédelmi Országgyűlési Biztos[1] ez irányú állásfoglalásait figyelembe kell venni.

(6) Törekedni kell a mobilitás lehetősége és a biztonság közötti ellentét kiegyensúlyozott kezelésére.

(7) A védelem mellett biztosítani kell az oktatási és kutatási tevékenységhez szükséges szabad információáramlást.

(8) Elérendő cél, hogy a szolgáltató rendszerek üzemzavarait ne elsősorban a felhasználók, hanem automatikus szolgáltatásmonitorozó komponensek jelezzék.

[1] Az adatvédelmi biztos intézménye az Alaptörvény hatálybalépésével, 2012. január 1-jén megszűnt. Hatáskörét részben a Nemzeti Adatvédelmi és Információszabadság Hatóság gyakorolja.

(9) Vezetői elkötelezettség: Minden (átfogó) szervezeti egység vezetője személyesen felel az információbiztonság kultúrájának kialakításáért és fenntartásáért. A vezetők elkötelezettségüket személyes példamutatással (szabályozások betartása) és személyes felelősségvállalással demonstrálják. A belső és külső szolgáltatói megállapodások (SLA-k) figyelése, figyelembe vétele és a bennük megfogalmazott paraméterek mérése a vezetői elkötelezettség kinyilvánítása. Az információbiztonsági intézkedések megvalósításához szükséges erőforrások biztosítása szintén a vezetői elkötelezettséggel összhangban zajlik.

7.§
Feladat- és hatáskörök

(1) Az információbiztonsággal kapcsolatos felelősség megoszlik a TIO, az egyes szervezetek és a felhasználók között az alábbi általános elvek szerint.

Az Üzemeltető hatásköre és felelőssége

(2) Minden, az Egyetemen üzemeltetett IT Rendszer esetében az IBSZ-nek való megfelelés az adott rendszer Üzemeltetőjének felelőssége.

(3) Az Egyetem IT Rendszereinek az IBSZ-ben foglaltaknak való megfelelősége elsődlegesen az adott rendszer működtetéséért felelős átfogó szervezeti egység/szervezeti egység vezetőjének a hatáskörébe tartozik.

(4) Üzemeltetők a következők:
- az adott IT szolgáltatást nyújtó, azért felelős átfogó szervezeti egység/szervezeti egység (a továbbiakban: a szolgáltatásért felelős szervezeti egység),
- illetve az általa szerződéssel ezzel megbízott külső, az Egyetemmel munkavégzésre irányuló (megbízási, vállalkozási) jogviszonyban álló személy

(a továbbiakban együtt: az Üzemeltető).

(5) A szolgáltatásért felelős szervezeti egység harmadik személytől vásárolt szolgáltatásként is biztosíthatja az IT Rendszer üzemeltetését. Ez utóbbi esetben a szolgáltatásért felelős szervezeti egység azért felelős, hogy érvényesítse a szerződés útján üzemeltető harmadik személlyel szemben az IBSZ-ben az üzemeltetőre rótt kötelezettségeket.

(6) Abban az esetben, ha a szolgáltatásért felelős szervezeti egység az üzemeltetéssel külső harmadik személlyel, szervezettel köt szerződést, a szerződésben szerepeltetni kell a következőket:
- A külső harmadik személy kötelezettség- és felelősségvállalását az egyetemi tulajdonú IT rendszerek esetében a hatályos jogszabályoknak, az Egyetem mindenkori belső szabályozásainak – különösen az Informatikai Szabályzatnak és az IBSZ-nek – való megfelelésért, valamint a szerződésben rögzített műszaki feltételek betartásáért,
- Az Informatikai Szabályzat alapján megkötött SLA-nak megfelelő kötelezettségek vállalását a külső harmadik személy, szervezet részéről,

- Az Egyetem nevében eljáró átfogó szervezeti egység/szervezeti egység jogát ennek ellenőrzésére,
- Az egyetemre vonatkozó adatvédelmi és az információbiztonsági kérdéseket.

Amennyiben az itt meghatározottaktól a külső harmadik személy eltér, és ezt a szolgáltatásért felelős átfogó szervezeti egység/szervezeti egység észleli, a szükséges intézkedések megtétele a szolgáltatásért felelős szervezeti egység feladata és felelőssége.

(7) Az „A", „B" és „C" osztályú rendszerek esetében az installálási időszakon kívül hozzáférést a szolgáltatásért felelős szervezeti egység vezetője engedélyezheti. A kérelemnek tartalmaznia kell a felhasználó adatait, a hozzáférés indokát, módját, paramétereit és tervezett időtartamát. Engedély nélküli hozzáférés biztosítása esetén az adott informatikai rendszer nem minősül IBSZ megfelelőnek. Harmadik személy vagy szervezet csak kivételesen indokolt esetben kaphat felhasználási jogot „A", „B" vagy „C" kategóriájú rendszerhez, és csak abban az esetben, ha az az általa ellátandó feladathoz elengedhetetlenül szükséges.

(8) A vonatkozó jogszabályokban előírt információbiztonsági adatszolgáltatási kötelezettség teljesítése az adott szolgáltatásért felelős (átfogó) szervezeti egység vezetőjének felelőssége.

A felhasználók felelőssége

(9) A felhasználó köteles az IBSZ-ben foglaltaknak megfelelően használni az IT Rendszert.

(10) Minden közalkalmazott, hallgató és külső, az Egyetemmel polgári jogviszonyban álló személy vagy szervezet csak a számára meghatározott jogosultsággal léphet be a különböző rendszerekbe. A jogosultság változását a közalkalmazottak esetében a munkairányítónál, harmadik személy vagy szervezet esetében a megbízó szervezeti egység vezetőjénél kell kezdeményezni, aki azt továbbítja a szolgáltatásért felelős (átfogó) szervezeti egységnek.

(11) A szolgáltatás felhasználója teljes felelősséggel tartozik az adott szolgáltatás SLA-jában általa vállalt kötelezettségek betartásáért, beleértve a korlátos erőforrások pazarlása miatt az üzemeltetőnél keletkező többletköltségeket is.

(12) Az „A" osztályú rendszerek felhasználója munkaköri kötelezettsége keretében kezelheti az intézményi adatokat, ezek bizalmas kezelése munkaköri kötelessége. Az egyetemi rendszert köteles csak a munkakörének megfelelően, erőforrás-kímélő módon, a kezelési utasításoknak megfelelően használni.

(13) Az IBSZ előírásainak szándékos és tudatos megsértése esetén a felhasználó a vonatkozó jogszabályoknak és az Egyetem vonatkozó előírásainak megfelelően szankcionálható.

(14) Az Egyetem informatikai rendszereit felhasználók a szakmai szervezetekben való részvételükkor is (pl. ISACA, IVSZ stb.) kötelesek az IBSZ vonatkoztatható előírásait betartani.

(15) Amennyiben a felhasználó magatartásával más felhasználók munkáját veszélyezteti, az Üzemeltető intézkedik a szolgáltatásból kitiltásáról, és jogosultságainak visszavonásáról.

A GMF, ezen belül a TIO feladatai és felelősségi körei

(16) Az Egyetem információbiztonsági vezetője a TIO igazgatója.

(17) Az Egyetem (a továbbiakban Egyetem) informatikai biztonságának szabályozását és koordinálását a Gazdasági Műszaki Főigazgatóság (GMF) Telekommunikációs és Informatikai Osztálya (TIO) végzi.

(18) A TIO engedélyezi új IT Rendszer indítását.

(19) A nyilvános, minden, az Egyetemmel közalkalmazotti (és foglalkoztatásra irányuló egyéb jogviszonyban) vagy hallgatói jogviszonyban álló személy által igénybe vehető IT szolgáltatások ezen szabályzatnak való megfelelőségének ellenőrzésére a TIO jogosult.

(20) A jelentős súlyú, és/vagy más IT Rendszereket és azok felhasználóit is veszélyeztető esetben a TIO jogosult az egyetemi hálózatból kitiltásra.

(21) A TIO munkatársai felkérésre segítséget nyújtanak a szolgáltatásért felelős szervezeti egység számára külső szervezettel IT Rendszer üzemeltetésére megkötésre kerülő szerződésben a szolgáltatás tartalmának és egyéb paramétereinek egyeztetésében, hogy az a vonatkozó SLA-nak megfeleljen, valamint az SLA betartásának ellenőrzési feltételeinek kialakításában.

(22) Az informatikai rendszerek jelen Szabályzatnak történő megfelelőségi vizsgálatát, illetőleg az ezzel kapcsolatos tanácsadást a TIO igazgatója, illetve az általa kijelölt személyek végzik. Az IBSZ-nek megfelelőségi vizsgálatot a TIO igazgatója vagy az Üzemeltető (a szolgáltatásért felelős szervezeti egység vezetője vagy az üzemeltető külső szervezet vezetője) kezdeményezheti.

(23) A TIO igazgatója felelős a kapcsolattartásért a különleges érdekközösségekkel, mint például a magyar non-profit Internet használók közössége (Hungarnet). Az előzőekben megfogalmazott hivatalos tagsági és kapcsolattartási kérdésben a TIO igazgatója dönt az Egyetem érdekeinek figyelembe vételével.

Egyetemi Informatikai Bizottság

(24) Az információbiztonsági kérdésekkel kapcsolatos legmagasabb fóruma az egyes információbiztonsági védelmi intézkedésekkel kapcsolatban az Egyetemi Informatikai Bizottság.

(25) Az Egyetemi Informatikai Bizottság hatáskörébe tartozik:

a. az Egyetem informatikai biztonságpolitikájának rendszeres áttekintése, a megtett intézkedések értékelése,

b. minden olyan kérdés, amelyben a szolgáltatásért felelős szervezeti egység és a TIO között felmerült, és melyet a két fél nem tudott megegyezés útján lezárni,
c. szükség szerinti javaslattétel a döntésre jogosult felé a további védelmi intézkedésekre.

(26) Az Egyetemi Informatikai Bizottság tagjait a gazdasági és műszaki főigazgató kéri fel oly módon, hogy minden kar és nem törzskari átfogó szervezeti egység képviselve legyen a bizottságban. A bizottság elnöke a TIO igazgatója.

(27) Az Egyetemi Informatikai Bizottság üléseit a szükség szerinti gyakorisággal tartja, de legalább évente egy alkalommal.

(28) Üléseinek rendjét az Egyetemi Informatikai Bizottság maga határozza meg.

8.§
Az IBSZ-ben foglaltak megszegésének szankciói

(1) Amennyiben az IBSZ bármely esetben a szolgáltatásért felelős szervezeti egységet határozza meg az adott feladat, kötelezettség felelőseként, az IBSZ-ben foglaltak betartásának megszegéséből, elmulasztásából bárkit ért kárért elsősorban a szolgáltatásért felelős szervezeti egység köteles helytállni. Másodsorban, amennyiben a szolgáltatásért felelős szervezeti egység nem az SzFMR szerinti[2] átfogó szervezeti egység, az átfogó szervezeti egység köteles helytállni az okozott, és a szolgáltatásért felelős szervezeti egység által meg nem térített károkért.

(2) A felhasználókat a szabályzatban leírtak megsértése esetén az alábbi szankciók sújthatják:
- szolgáltatás megtagadás (kizárás a szolgáltatásból), melyről a TIO igazgatója dönt,
- a felelősség megállapítása és az okozott kár megtérítése.

(3) A szolgáltatásokat igénybe vevők bármilyen szankcionálása akkor történhet, ha az Üzemeltető dokumentálja a szankció elrendelését kiváltó eseményt, incidenst, vagy ilyet a TIO közvetlenül észlelt.

(4) Az IBSZ-ben foglaltak megszegése, kötelezettség elmulasztása esetén a személyes felelősséget az azonnali intézkedések (jogosultság visszavonása, kizárás a hálózatból) kivételével a vonatkozó egyetemi szabályozások szerinti eljárások alkalmazásával kell megállapítani, és érvényesíteni az esetleges kárt.

---

[2] SZFMR **4. § A szervezeti egységek típusai**
(1) Az Egyetem
- oktatási, valamint tudományos kutatási (művészeti) és innovációs
- (a továbbiakban: oktatási és kutatási) feladatokat végző,
- oktatás és kutatás irányítását segítő törzskari (továbbiakban: törzskari),
- oktatást és kutatást szolgáltatásaikkal közvetlenül támogató,
- oktatást és kutatást rendszerfenntartó és rendszerellátó szolgáltatásokkal segítő

szervezeti egységekre tagozódik.
(2) Az (1) bekezdésben említett típusokba tartozó szervezetek és csak e szervezetek átfogó szervezeti egységek. Az átfogó szervezeti egységeket jelen Szervezeti Felépítés és Működési Rend sorolja fel.

(5) Az Egyetemmel polgári jogi jogviszonyban állók esetén a felelősségi és kártérítési kérdésekben a polgári jog szabályai alapján kell eljárni.

9. §
Fizikai és környezeti biztonság

(1) ***Fizikai biztonsági határvédelem:*** az „A" kategóriájú szolgáltató rendszer kritikus fizikai komponensei (szerver, tároló alrendszer, router, stb.) csak külön erre a célra kialakított, megfelelő biztonsági paraméterekkel rendelkező helyiségekben működtethetők. A helyiségeknek mechanikai nyitórendszerrel (biztonsági zár vagy beléptető kártyával működtethető mágneses zár) és beléptető rendszerrel kell rendelkezniük. A beléptető rendszer szükséges alapfunkciói: belépő személy azonosítása kód vagy kártya alapján, belépési jogosultság megállapítása, belépési időpont regisztrálása, jogosulatlan belépés jelzése a biztonsági személyzet felé.

(2) ***Fizikai belépési szabályozás:*** Az „A" kategóriájú rendszerek komponenseit tartalmazó szolgáltató helyiségekbe (géptermek, kábelrendezők) való belépési jogosultságot szolgáltatásért felelős szervezeti egység vezetője engedélyezi egyetemi dolgozónak vagy a külső szerződött partnernek a helyiségek és a végezhető tevékenységek felsorolásával. A belépési lehetőséggel rendelkezők jogosultságukat nem ruházhatják át másra. Jogosulatlan személy beengedéséből fakadó eseményekért a felelősség a beengedő személyt terheli. Az illegálisan szerzett belépési lehetőség használata bűncselekménynek minősül és jogi következményeket von maga után.

(3) ***Irodák, szobák és egyéb létesítmények fizikai biztonsága:***

- Az informatikai rendszerek működtetéséhez szükséges egyéb munkaterületek használatának módja megegyezik az általános egyetemi területek használati módjával. Kitüntetett hozzáférést vagy védett adatokat tartalmazó kiegészítő rendszerkomponensek (mentési berendezés, fejlesztői rendszer, felügyelő terminál, stb.) csak beléptető rendszerrel védett munkaszobában és irodában helyezhetők el.
- Az informatikai célú helyiségekkel kapcsolatos kérdésekben a technikus vagy a rendszergazda felelős a ki- és az átalakítás koordinációjáért, a szakmai a biztonsági szempontok betartásáért.

(4) ***Külső és környezeti károk elleni védelem:***

- Az „A" kategóriájú szolgáltató rendszer kritikus fizikai komponensei csak a hatályos szabályozásnak megfelelő tűz- és villámvédelmi rendszerrel felszerelt helyiségekben üzemeltethetők. Talajszinten vagy az alatt elhelyezkedő helyiségek esetében az ár- és belvízvédelmi szempontoknak is meg kell felelni.
- Egyedi esetben a szolgáltatásért felelős szervezeti egység vezetője egyéb előírásokat is megfogalmazhat.
- A tűzvédelmi rendelkezéseknek megfelelően az erősáramú ellátó rendszernek tartalmaznia kell olyan központi áramtalanítókapcsolót, ami tűzjelzés esetén a biztonságos oltás feltételeit megteremti.
- Minden fenti helyiség esetén biztosítani kell azt a hűtési kapacitást, ami a teljes termelt hőmennyiség biztonságos elvezetését automatikusan meg tudja oldani.

- Minden fenti helyiség esetén biztosítani kell azt az erősáramú ellátó kapacitást, ami a berendezések megtáplálását túlterhelésmentesen el tudja végezni. Az erősáramú ellátó rendszernek áramkör-szelektív megszakítóval kell rendelkeznie.

(5) ***Munkavégzés biztonsági zónákban:*** Az „A" kategóriájú rendszereket tartalmazó helyiségekben minden olyan, nem az üzemeltető által folytatott munkavégzés, ami az informatikai rendszereket vagy azok működését veszélyeztetheti, csak előzetes egyeztetés alapján, felügyelet mellett végezhető. Az egyeztetést a munkavégző cég és az üzemeltető szervezeti egység vezetője végzi, a TIO gépteremvezető technikusának szervezésében és lebonyolításával. A helyiség gépészeti berendezéseit veszélyeztető munkák csak a gépteremvezető technikus és az üzemeltető előzetes engedélyével folytathatók.

(6) ***Nyilvános hozzáférés, szállítási és töltési területek:*** Az „A" kategóriájú rendszereket tartalmazó helyiségekben minden szállítási tevékenység csak belépésre jogosult munkatárs felügyelete mellett végezhető.

(7) ***Eszközök elhelyezése, védelme:*** Minden „A" kategóriájú rendszerkomponens fizikai elhelyezésénél törekedni kell a gépterem / kábelrendező felépítési elveinek betartására (pl. rackben történő elhelyezésre, megfelelő ventillációs irányra, stb.) Ezen irányelveket új komponens beszerzése esetén a TIO előírhatja.

(8) ***Támogató közművek (szolgáltatások):*** A gépterem / kábelrendező helyiségekben üzembe állítandó új rendszerek (vagy nagyobb rendszerkonfiguráció módosítás) esetében az installálást végző szakembereknek előzetesen konzultálniuk kell az erősáramú és hűtési igény biztosításáról a TIO gépteremvezető technikusával. A szükséges gépészeti módosításokat az új rendszer üzembe állítása előtt el kell végezni.

(9) ***Kábelbiztonság:*** Az „A" és „B" kategóriájú rendszerek védett helyiségen kívül húzódó, összekötő komponenseit (telefon és gerinchálózati kábeleket) tartalmazó BME tulajdonú alépítmények, kábelaknák és védőcsövek a TIO által felügyelt területnek minősülnek. Azokban munkát végezni, vagy a megközelíthetőségüket korlátozni csak a rendszerkomponens üzemeltetőjének előzetes engedélyével lehet.

(10) ***Eszközkarbantartás:***

- Minden szolgáltató rendszer üzemeltetője köteles a hardver komponensek karbantartási igényét felmérni és ezeket úgy ütemezni, hogy a rendszer élettartama ne rövidüljön karbantartási hiányosságok miatt.
- A gépészet külön karbantartási tervvel rendelkezik.
- A karbantartás során a felmerült biztonsági sérülékenységeket megfelelően kell kezelni, illetve úgy kell a karbantartásokat elvégezni, hogy újabb biztonsági kockázatok ne merüljenek fel. Ennek felelőse az Üzemeltető.

(11) ***Telephelyen kívül használt eszközök biztonsági szabályai:*** A telephelyekről kivitt eszközök használata során bekövetkező károkért (adatvesztés, adatszivárgás) az a személy viseli a felelősséget, aki az eszközt kivitte, amennyiben a kár neki felróható okból keletkezett. A telephelyen kívüli használat során mindazon elvek és gyakorlat követendő, amelyeket az IBSZ egyes fejezetei leírnak.

(12) ***Eszközök biztonságos megsemmisítése vagy újrahasznosítása:*** A használt eszközök selejtezése az Egyetem hatályos szabályainak figyelembevételével történik. Speciális eszközök selejtezése esetén az üzemeltető gondoskodik a szakszerű elhelyezésről / elszállításról. Az „A", „B" és „C" kategóriás eszközök selejtezésénél gondoskodni kell az azon tárolt adatok selejtezés előtti fizikai megsemmisítéséről, az adatok szükség szerinti archiválását követően.

(13) ***IT eszközök (hardver, szoftver) kivitele telephelyről:*** Az eszközök ki/beszállítását szállítólevéllel kell kísérni, amin az eszköz(ök) egyedi azonosítóját (ha értelmezhető) fel kell tüntetni.

10. §
Kommunikáció és üzemelés menedzsment

(1) ***Működési folyamatok és felelősségek:***

- Amennyiben a(z) (átfogó)szervezeti egység szolgáltatás-indítási kérelemmel fordul a TIO igazgatójához, ezzel elismeri megfelelési szándékát az Informatikai Szabályzat és az IBSZ kritériumainak. A szolgáltatás-indítási kérelem csak adathiány és Informatikai Szabályzat vagy IBSZ sértés esetén utasítható el. Az elutasítást részletesen indokolnia kell a TIO igazgatójának, nem kizárva az esetleges módosított újbóli kérelem beadását.
- Minősített („A", „B" ill. „C" osztályú rendszerek) esetében az Informatikai Szabályzat és IBSZ megfelelést a TIO esetileg vizsgálhatja és az esetleges hiánypótlásra az Üzemeltetőt felszólíthatja. Amennyiben a vizsgált informatikai rendszer maga is más informatikai szolgáltatásokat használ, úgy a használt szolgáltatás SLA-ja is vonatkozik rá.
- Minden informatikai rendszer esetében a használatra vonatkozó igény bejelentése (hozzáférés vagy felhasználói azonosító igénylése) egyúttal az Informatikai Szabályzat és az IBSZ elfogadásának szándéknyilatkozatát is jelenti. A hozzáférés megadásával a hivatkozott két szabályzat a szolgáltatás nyújtója és igénybevevője között érvénybe lép.
- Az „A" és „B" osztályú rendszerek esetében az elvárt szolgáltatási és rendelkezésre állási paraméterek alulteljesítése miatt az Egyetemet anyagi és egyéb kár érheti. Ilyen esetekben a felelősség megállapítására és a szükséges lépések megtételére (rendszer-módosítás, szabályzat-módosítás) a szolgáltatásért felelős szervezeti egység vezetője eseti bizottságot nevezhet ki. Ezen bizottságnak mindig tagja a TIO igazgatója is.

(2) ***Harmadik fél által nyújtott szolgáltatások menedzsmentje:***

- A külső harmadik fél által nyújtott informatikai szolgáltatások is SLA kötelezettek, a kritikus paramétereket a külső harmadik féllel kötött szolgáltatási szerződésben is rögzíteni kell. A szerződésnek ki kell terjednie az információbiztonsági és adatbiztonsági kérdésekre is.
- Az „A" és a „B" kategóriájú IT szolgáltatások esetében az Egyetem egykapus ügyintézést és érdekképviseletet alkalmaz. Ezen szolgáltatók esetében az ügyfélkapcsolatra és szerződéskötésre jogosult a szolgáltatásért felelős szervezeti egység vezetője.

(3) ***Rendszertervezés és elfogadás:*** Az informatikai szolgáltató rendszerek esetében az Informatikai Szabályzat és IBSZ megfelelést már a tervezési szempontok között szerepeltetni kell. Az üzemeltetni tervezett „A", „B" és „C" osztályú rendszerek esetében az Informatikai Szabályzat és IBSZ megfelelés TIO általi igazolása a szolgáltatás indításának szükséges feltétele. Erről az Informatikai Biztonsági Szabályzat 5. melléklete szerinti formanyomtatványt kell kitölteni.

(4) ***Védekezés vírusok és egyéb kártékony kódok ellen:***

- Azon rendszerek esetében, ahol a kártékony és mobil kódok előfordulhatnak, a detektálásukat és elhárításukat végző komponensek installálása a szolgáltatási engedély kiadásának feltétele.
- Minden olyan rendszer esetében, ahol vírusfenyegetés fennáll és lehetséges installálni vírusvédelmi rendszert, valamint a kémprogram jelző komponenst, ott az a szolgáltatás üzembe helyezésének és üzemeltetésének feltétele.
- Publikus levelező rendszerek esetében az Egyetemen kívüli kapcsolat létesítésének feltétele a levelek informatikailag veszélyes tartalmának vizsgálati képessége illetőleg az „open relay" lehetőség kiküszöbölése. Károkozás esetén a TIO igazgatója jogosult, illetve köteles az ilyen levelező rendszernek a haladéktalan kitiltására illetve hálózati kapcsolatának megszüntetésére. A károkozás tényét a TIO igazgatója köteles dokumentálni. A hálózati szolgáltatásból kitiltott címekről a TIO honlapján információ található.
- Felhasználói tulajdonú adathordozók használata esetén az adott eszköz használata következtében okozott károkért az Egyetem rendszereiben felhasználóként belépett személy a felelős (pl. vírusos USB kulcs).

(5) ***Biztonsági mentések:***

- Minden „A", „B" és „C" osztályú szolgáltató rendszer üzemeltetési leírásának tartalmaznia kell az alkalmazások és adatok mentési rendjét (a mentendő adatok körét, a mentés módját és gyakoriságát, a mentéséért felelős személyt, a mentés tárolási rendjét).
- „A" és „B" osztályú rendszerek esetén külső tárolású (off-site) mentésekkel is kell rendelkezni, C és D osztályú rendszerek esetén on-site mentések is elfogadhatóak.
- A mentési rendnek az alkalmazásra vonatkozó részét úgy kell megállapítani, hogy a rendszer működőképessége tetszőleges komponens meghibásodása vagy adatvesztése esetén helyreállítható legyen (új hardware biztosítása esetén). Ennek érdekében az alkalmazás futó kódját legalább minden verzióváltás előtt és után menteni kell, a mentést minimum 3 verzióra vagy egy évre visszamenőleg meg kell őrizni.
- Az alkalmazások és rendszerek konfigurációs beállításait minden változás esetén, de legfeljebb naponta kell menteni. A mentési eljárásnak lehetővé kell tennie egy adott konfigurációs állapot célirányos visszaállítását. A konfigurációs mentéseknek 10 előző állapotra ill. minimum az előző 30 szolgáltatási napra ki kell terjedniük.
- Az „A" osztályú rendszerek esetében az alkalmazásokban tárolt intézményi adatokat minden munkanap végén teljes egészében menteni kell. A mentési módnak lehetővé kell tennie ezen adatok tesztrendszerbe történő betöltését. A „C" osztályú rendszerek esetében a személyi adatok inkrementális mentése is megengedett eljárás. A teljes adatpark mentése 30 naponta javasolt. Az alkalmazás üzemeltető rendszergazdája belátása szerint bármikor jogosult eseti mentés indítására.

- Minden „A", „B" és „C" osztályú rendszer esetében évente minimum egy alkalommal visszatöltési gyakorlatot (tesztelés) kell tartani, ami a mentések felhasználhatóságát ellenőrzi. A visszatöltési gyakorlat a szolgáltató rendszerrel funkcionálisan egyező tesztrendszeren is teljesíthető. A mentések meglétét és a visszatöltési gyakorlatot a TIO ellenőrizheti.

(6) ***Hálózatbiztonság menedzsmentje:*** Az Egyetem teljes területére kiterjedő alapinfrastruktúra (számítógépes és telefonhálózat) védelme egységes koncepció és megvalósítás mellett történik. Az irányelvek és módszerek meghatározását és a szükséges operatív beavatkozásokat a telekommunikációs hálózat üzemeltetésével megbízott TIO szervezeti egység végzi. A kommunikációs hálózathoz való csatlakozás feltétele a (csatlakozás módjától és a csatlakoztatott rendszertől függő) biztonsági előírások maradéktalan betartása. Ezen előírások a csatlakozásnak, mint szolgáltatásnak az igénybevételi feltételei között tekinthetők meg (lásd IT Szabályzat).

(7) ***Média-kezelés:***
- Az „A" „B" és „C" osztályú rendszerek adatterületeinek mentései jogvédelem alá eső intézményi és személyes adatokat tartalmazhatnak. Ezen adathordozókat olyan körültekintéssel kell tárolni és kezelni, mint magát az adatot tároló rendszert.
- A mentések tárolása: Az „A" és „B" osztályú rendszerek mentéseinek tárolása a TIO által kijelölt és jóváhagyott védett helyiségben történik. A médiáról az üzemeletetésért felelős szervezeti egységnek nyilvántartást kell vezetni.
- Mentések adathordozóinak használatból való kivonása és megsemmisítése (pl. demagnetizálás) a szolgáltatást üzemeltető feladata. A média megsemmisítésről jegyzőkönyvet kell felvenni.

(8) ***Információcsere:***
- Az Egyetem „A", „B" és „C" osztályú rendszerei esetében az automatikus adatcserét lehetővé tevő kapcsolatok létesítéséhez TIO igazgatói engedély és az érintett szolgáltatásért felelős szervezeti egység vezetőjének hozzájárulása szükséges. A kérelemben az alkalmazások üzemeltetőinek részletezniük kell az elérendő adatkezelési célt és az alkalmazott informatikai megoldást, különös tekintettel a jogosulatlan adatcserét kizáró biztonsági megoldásokra.
- Az adatcsere környezetét, technológiai megvalósítását dokumentálnia kell az adatcserét kezdeményező alkalmazásüzemeltetőnek.

(9) ***Elektronikus kereskedelem:***
- Az elektronikus kereskedelmet lehetővé tévő alkalmazások esetében a biztonsági feltételek megteremtése érdekében a TIO igazgatójának engedélye szükséges a rendszer működtetéséhez.
- Az alkalmazás tervezésébe és megvalósításába be kell vonni a TIO igazgatóját vagy annak kijelölt képviselőjét.

(10) ***Monitorozás:*** Az „A" és „B" osztályú rendszerek esetében az üzemeltetők felelőssége az automatikus szolgáltatás monitorozó komponensek bevezetési lehetőségének vizsgálata és a monitorozás megvalósítása.

11. §
Emberi erőforrással kapcsolatos biztonsági kérdések

(1) ***Alkalmazás előtti tennivalók:*** Erkölcsi bizonyítvány szükséges az „A" és „B" osztályba sorolt rendszerek üzemeltetői és fejlesztői esetében.

(2) ***Az alkalmazás alatti tennivalók:***

- Az „A", „B" és „C" kategóriájú rendszerek esetében minden üzemeltető vagy felhasználó csak a munkakörének ellátásához elengedhetetlenül szükséges jogosultságokat birtokolhatja. (Azon fejlesztői rendszerek, amelyek személyes vagy intézményi adatokat nem tartalmaznak, nem minősülnek kategorizált rendszernek.)
- Az „A" és „B" osztályú rendszerek bizonyos szolgáltatásainak igénybevételéhez (pl. gazdálkodási rendszer) a szolgáltatásért felelős szervezeti egység vezetője tanfolyam és/vagy vizsga teljesítését írhatja elő. A kritériumok teljesítésének költsége a felhasználót foglalkoztató szervezeti egységet terheli.

(3) ***A jogviszony megszűnése vagy munkakör-változás:***

- A dolgozó jogviszonyának megszűnése vagy az informatikai biztonsággal kapcsolatos feladatait érintő munkakör változása esetén minden „A", „B" és „C" kategóriájú rendszer esetében az üzemeltetői, fejlesztői és felhasználói jogosultságot, ilyen tevékenységet lehetővé tevő belépési kódokat azonnal vissza kell vonni.
- A volt dolgozó vagy hallgató a „C" és „D" kategóriájú rendszerekben a (kizárólag) személyes adatainak elérésére szolgáló belépési kódjait a szolgáltatásért felelős szervezeti egység vezetőjének eseti engedélye alapján megtarthatja.

A jogviszony megszűnésekor vagy munkakör változása esetén a közalkalmazott közvetlen felettesének kötelessége azt ellenőrizni, hogy közalkalmazotti jogviszonyánál fogva az adott közalkalmazott rendelkezik-e bármilyen szintű jogosultsággal IT Rendszerrel kapcsolatban, és amennyiben igen, úgy a jogosultság változással érintett IT Rendszer vonatkozásában a szolgáltatásért felelős szervezeti egységet a közalkalmazotti jogviszonyt érintő változásról értesíteni kell. Amennyiben a szolgáltatásért felelős szervezeti egység és az üzemeltető eltér, a szolgáltatásért felelős szervezeti egység köteles az üzemeltetőt értesíteni az IT Rendszerrel kapcsolatos jogosultságban bekövetkező változás lebonyolítása érdekében.

12. §
Hozzáférés és jogosultság szabályozás

(1) ***Általánosan betartandó szabályok:***
Az azonosítás és hitelesítési funkció során az „A" biztonsági kategóriába eső rendszerek esetében:

- az egyedi felhasználókat és a felhasználó csoportokat jelszóval kell azonosítani,
- a jelszavakat egyirányúan titkosítva kell tárolni,
- a jelszó "öregítési" mechanizmust alkalmazni kell,
- meg kell határozni a jelszavak minimális hosszát,

- a jelszóadást és változtatást csak az erre a feladatra kijelölt rendszeradminisztrátor végezheti el,
- rendszeradminisztrátor csak felhatalmazott személy lehet, magas prioritású jogokkal,
- nehezen megfejthető jelszóalkotás támogatását biztosítani kell,
- adott számú téves bejelentkezési kísérlet után az adott felhasználói jogosultsági rendszert bénítani kell, a téves bejelentkezés ténye rögzítendő és kivizsgálandó,
- az adott rendszerhez hozzáférést és a hozzátartozó jogosultságot a szolgáltatás üzemeltetéséért felelős szervezeti egység vezetője vagy felhatalmazottja adhat ki.

Az elszámoltathatóság és auditálhatóság biztosítása érdekében olyan regisztrálási és naplózási rendszert (biztonsági napló) kell kialakítani, hogy utólag meg lehessen állapítani az informatikai rendszerben bekövetkezett fontosabb eseményeket, különös tekintettel azokra, amelyek a rendszer biztonságát érintik. Ezáltal ellenőrizni lehessen a hozzáférések jogosultságát, meg lehessen állapítani a felelősséget, valamint illetéktelen hozzáférés megtörténtét.

A rendszernek képesnek kell lennie minden egyes felhasználó vagy felhasználó csoport által végzett művelet szelektív regisztrálására.

A minimálisan regisztrálandó események a következők:

- rendszerindítások, leállások, leállítások,
- rendszeróra állítások,
- be/kijelentkezések,
- program leállások,
- az azonosítási és hitelesítési mechanizmus használata,
- hozzáférési jog érvényesítése azonosítóval ellátott erőforráshoz,
- azonosítóval ellátott erőforrás létrehozása vagy törlése,
- felhatalmazott személyek műveletei, amelyek a rendszer biztonságát érintik.

(2) ***Hozzáférési politika:***

- Minden olyan informatikai rendszer esetében, ami az Egyetem működéséhez szükséges, illetőleg bármilyen védett (intézményi, magán, kutatási, jogvédett, stb.) információt tartalmaz, meg kell határozni a hozzáférésre jogosultak körét és hozzáférési kísérlet esetén a jogosultságot ellenőrizni kell.
- Informatikai rendszerhez való, módosítást és védett adatok lekérdezését lehetővé tevő hozzáférésre kizárólag másik rendszer vagy természetes személy lehet jogosult, amennyiben a hozzáférés biztosítása nem ütközik adatvédelmi szabályokba. Természetes személyek egy csoportja (szervezeti egység dolgozói, cégek, stb.) közös használatú hozzáférési lehetőséget kizárólag publikus adatok lekérdezésére birtokolhat.
- A jogosultság kezelést az üzemeltetőnek napra készen kell tartani és dokumentálni.

(3) ***Felhasználói hozzáférés menedzsmentje:***

- Az adott informatikai rendszerhez történő hozzáférés módját (igénybe vételre jogosultak köre, igénylés módja, igénylés elbírálása) a rendszeren működő szolgáltatások SLA-i tartalmazzák. Az igénybevétel során a természetes személynek azonosítania kell magát egyedi adatával vagy adat-párjával. (pl. tanulmányi rendszer azonosító). Amennyiben az Egyetem az informatikai rendszerek felhasználóinak azonosítását és jogosultság-elbírálását központilag

valósítja meg, erre a célra szolgáló rendszerekkel (pl. LDAP, Kerberos) és a felhasználói adatbázis kezelése egységesen és konzisztensen történik, akkor az „A", „B" és „C" kategóriájú rendszereknek ehhez csatlakozási képességgel kell rendelkeznie. Kivételt azok a már meglévő és működő rendszerek képeznek, melyek nem képesek központi jogosultságkezelést megvalósítani.

- A szolgáltatási SLA felhasználó általi megszegése esetén a felhasználó az adott szolgáltatásból kizárható. Kizárás esetén a felhasználót ennek tényéről, a kizárás időtartamáról, a problémát okozó tevékenységről és a követendő magatartásról tájékoztatni kell. Ha a felhasználó tevékenysége által okozott kár csekély, akkor törekedni kell az előzetes figyelmeztetésre vagy a letiltás előtti tájékoztatásra.
- Az „A" és „B" osztályú rendszerek esetében az üzemeltető a hozzáférésre jogosultak esetében is előírhat engedélyezési eljárást (pl. a kérelmező munkáltatója által) a hozzáférés megadásához. Az engedélyt az üzemeltetőnek írásban, a kért jogosultságokat feltüntetve kell eljuttatnia kérelmező részére. Minden „A", „B" és „C" osztályú rendszer esetében az üzemeltető feladata, hogy a kiadott hozzáférések adatait (név, alkalmazás, jogosultsági szint, kiadás dátuma, indoka) naprakészen nyilvántartsa.
- A hozzáférés indokának megszűnése esetén az üzemeltetőnek a hozzáférést haladéktalanul vissza kell vonnia az SLA-ban dokumentált módon.

(4) ***Hálózati hozzáférés:***

- A számítógépes hálózatra történő fizikai csatlakozás csak az üzemeltető által elfogadott igénylés után, az abban megadott paraméterekkel lehetséges. A jogosulatlan csatlakozást az üzemeltető a rendszer integritásának védelmében azonnal megszüntetheti. A csatlakozási lehetőségeket és az igénylés módját a hálózati szolgáltatások SLA-i tartalmazzák.
- A hálózati szolgáltatások SLA-iban szereplő feltételrendszer az üzembiztonság, nyomon követhetőség és központi kezelhetőség szempontjai szerint van kialakítva, ezért az SLA be nem tartása a rendszer egészét, a többi felhasználó szolgáltatási környezetét veszélyezteti. Emiatt az SLA-t megszegő felhasználó a hálózati szolgáltatásokból utólagos figyelmeztetés mellett is kizárható.
- Az Internet bármely komponenséhez történő hozzáférés esetén a felhasználó köteles az egyetem Internet-szolgáltatójának szabályzatát is betartani.

(5) ***Operációs rendszer hozzáférés:*** Az „A", „B" és „C" osztályú szolgáltatások operációs rendszereiben adminisztrátori beavatkozást kizárólag csak az adott szolgáltatásért felelős szervezeti egység vezetője által kijelölt személy végezhet. A hozzáférés tényét, időtartamát és forrását a rendszernek visszakereshető módon naplóznia kell az SLA-ban meghatározottak szerint, illetve minimum 1 hónapig.

(6) ***Alkalmazásokhoz és információhoz való hozzáférés szabályozása:***

- Az intézményi adatokhoz való hozzáférést lehetővé tevő alkalmazások jogosultsági köreit olyan módon kell kialakítani, hogy a közalkalmazottak csak a munkakörükkel kapcsolatos adatokhoz férhessenek hozzá, illetve kezelhessék. A bizalmas intézményi adatokhoz történő hozzáférést, ezen adatok módosítását alkalmazás szinten is – visszakereshető módon - naplózni kell minimum 1 hónapra visszamenőleg.
- Minden „A", „B" és „C" osztályú rendszer esetén a személyes adatokhoz kizárólag az férhet hozzá, akinek a munkaköre ellátásához az adatra feltétlenül szüksége van, illetve az adattal rendelkező természetes személy férhet hozzá. Ez

alól csak a rendszer üzemeltetését ellátó és a mentéseket készítő azonosított személyek jelentenek kivételt. Az adatot birtokló természetes személynek ezen adatok publikálásához tevőlegesen meg kell változtatnia a publikálandó adatok hozzáférési jogosultságát.

(7) ***Mobil számítógép használat és telefonos munkavégzés:***

- Az „A", „B" és „C" osztályú rendszerekhez történő menedzsment hozzáférés kizárólag az egyetemi belső hálózatból (intranet, VPN) lehetséges. Minden egyéb hozzáférési kísérlet incidensnek minősül és informatikai megoldásokkal is akadályozandó az üzemeltetők részéről.
- Speciális hálózati szolgáltatásokkal (pl. VPN) az intranet az Egyetem fizikai hálózatán kívülre is meghosszabbítható, ezáltal a munkahelyen kívüli munkavégzés lehetséges. Ezen megoldások önerős megvalósítása kizárólag a TIO jóváhagyásával megengedett vagy a TIO ilyen tartalmú szolgáltatásai vehetők igénybe. Az intranet védelmi szintjének megsértése a hálózati hozzáférés nem megfelelő használatával (pl. saját átjáró, külső hálózati kapcsolat, stb.) felhasználó általi létesítése súlyos SLA sértésnek minősül.

(8) ***Központi autentikáció:***
A GMF TIO központi autentikációs rendszert üzemeltet, melyhez a szervezeti egységek a saját rendszereiket csatlakoztathatják. Ehhez engedélyt a TIO igazgatója ad ki, a rendszer használatára vonatkozó technikai ismeretek és szabályok tudomásul vétele után. A TIO a rendszer használatához technikai segítséget biztosít.

13. §
Titoktartási nyilatkozatok

(1) Az információbiztonsági szabályok betartásával és betartatásával kapcsolatban a **2.** számú mellékletben részletezett titoktartási nyilatkozatot írnak alá az „A" és „B" osztályú rendszerek üzemeltetői, illetve a felhasználók is, „C" és „D" osztályú rendszerek esetén bizalmassági nyilatkozatot kell tenni, amennyiben erről az adott rendszer SLA-ja külön rendelkezik. Titoktartási nyilatkozatot kötelesek tenni továbbá az Egyetemmel IT Rendszer üzemeltetésére szerződött külső személyek, szervezetek is, illetve mindazok, akik az IT Rendszerhez hozzáférési jogosultsággal bírnak. is a 4. számú mellékletben részletezett titoktartási nyilatkozat kitöltésével és aláírásával.

(2) Az IT rendszer üzemeltetői a rendszer üzemeltetése során különféle személyes, illetőleg bizalmas adatokhoz férnek hozzá, ezért az ilyen rendszerek üzemeltetőinek titoktartási nyilatkozatot kell tenniük.

(3) A munkavégzés során a munkavégzők részére átadott, illetve tudomásukra jutott adatvédelmi szempontból szenzitív információkat védeni kell, ezért ők is titoktartási nyilatkozatra kötelezettek.

(4) Minden bizalmassági kérdésben érintett szereplővel titoktartási nyilatkozatot kell kitöltetnie a szolgáltatás üzemeltetőjének, melynek aláírásával vállalja, hogy a birtokában levő információval nem él vissza, azt jogosulatlanul nyilvánosságra nem hozza, vagy arra nem jogosult harmadik személy számára nem teszi hozzáférhetővé.

14. §
Megfelelőség

(1) ***Jogszabályi megfelelőség:***

- Az adott szolgáltatásért felelős szervezeti egység vezetőjének felelőssége a mindenkori jogszabályi megfelelőség biztosítása a nyújtott szolgáltatások vonatkozásában.
- Az adott szolgáltatásért felelős szervezeti egység vezetője nem felel a felhasználók által elkövetett jogsértésekért (pl. jogosulatlan adatkezelés, szerzői jogokkal való visszaélés stb.), és hatósági megkeresés esetén a jogszabályban előírt adatokat az adott felhasználóval kapcsolatban kiadhatja/köteles kiadni, illetve a szükséges szabálytalanság-kezelési eljárásokat – amennyiben azok indokoltak – lefolytatni.
- Az információbiztonság témakörében érvényes legfontosabb jogszabályok jegyzékét a **3.** számú melléklet tartalmazza.

(2) ***Megfelelés biztonsági politikának, szabványoknak és műszaki előírásoknak:***

- Az adott szolgáltatásért felelős szervezeti egység vezetőjének felelőssége a mindenkori biztonsági politikának, szabványoknak és műszaki előírásoknak való megfelelőség biztosítása, szervezése a nyújtott szolgáltatások vonatkozásában.
- Az információbiztonság témakörében érvényes legfontosabb szabványoknak és műszaki leírásoknak a jegyzékét a 3. számú melléklet tartalmazza.

(3) ***Információs rendszerek felülvizsgálatával kapcsolatos megfontolások:***

- Az Informatikai Szabályzattal összhangban az adott szolgáltatást nyújtó szervezet vezetője felelős azért, hogy az IT-rendszerek teljes körű belső biztonsági felülvizsgálata dokumentált módon (belső felülvizsgálati jelentés) legalább háromévente megtörténjen, és legalább háromévente sor kerüljön külső, harmadik fél általi felülvizsgálatra az „A" osztályú rendszerek esetében. Ezt a TIO igazgatója jogosult ellenőrizni. A felülvizsgálat költségei az üzemeltetőt terhelik.
- Súlyos SLA sértés gyanúja esetén a TIO igazgatója külön rendkívüli biztonsági ellenőrzést és felülvizsgálatot rendelhet el.
- A felülvizsgálatok eredményei alapján a TIO igazgatója rendel el javító, helyesbítő és megelőző intézkedéseket, melyeket mindig a soron következő belső vagy külső, harmadik fél általi felülvizsgálat során kell dokumentált módon ellenőrizni.

(4) Azon informatikai rendszerek esetében, amelyeknek nem volt sikeres az IBSZ szerinti megfelelőségi vizsgálata (IBSZ vizsgálat), minden incidens felelőssége a szolgáltatásért felelős szervezeti egység vezetőjét terheli. Azon rendszerek esetében, ahol az IBSZ vizsgálat sikeres volt (illetőleg a vizsgálat során készült és elfogadott hiánylistát az Üzemeltető pótolta) az incidensek felelőseit és okait egyedi vizsgálat alapján kell megállapítani és értékelni. Az IBSZ (és a rendszerre vonatkozó mellékleteinek) betartása esetén az üzemeltető jóhiszeműnek minősül. A TIO igazgatója felelős az információbiztonsági események, incidensek tanulságai és a pozitív példák megjelenítéséért a TIO szokásos információs csatornáin.

15. §
Az információvagyon menedzsmentje

(1) Az információs vagyon az Informatikai Szabályzat alapján készített üzemeltetési dokumentációkban leírtak alapján meghatározott. Az „A", „B" és „C" kategóriájú rendszereinek nyilvántartását és az általuk biztosított szolgáltatások paramétereinek nyilvántartását (mint információs vagyonleltárt) az adott szolgáltatásért felelős szervezeti egység vezetője által kijelölt személy végzi. Az ehhez szükséges adatszolgáltatás a rendszerek külső üzemeltetőinek is kötelezettsége.

(2) Az információs vagyon tulajdonjoga: Az „A", „B" és „C" kategóriájú rendszerek intézmény-specifikus konfigurációs adatai és beállításai (minden olyan konfigurációs komponens, ami az eredeti telepített rendszer alapbeállítása szerinti állapottól eltér) az Egyetem tulajdonát képezi. Ugyanezen rendszerekben tárolt minden intézményi adat (és annak minden felhasználási joga) az Egyetem tulajdonát képezi.

(3) Az információvédelem területén történő osztályozás az adatok minősítési szintjével növekvő mértékű, a bizalmasság, hitelesség és a sértetlenség sérüléséből vagy elvesztéséből származó kárszinteken alapul.
- Információvédelmi alapbiztonsági osztály: Személyes adatok, üzleti titkok, pénzügyi adatok, illetve az Egyetem belső szabályozásában hozzáférés-korlátozás alá eső (pl. egyes feladatok végrehajtása érdekében bizalmas) adat feldolgozására, tárolására alkalmas rendszer biztonsági osztálya.
- Információvédelmi fokozott biztonsági osztály: A szolgálati titok, valamint a nem minősített adatok közül a különleges személyes adatok, nagy tömegű személyes adatok, közepes értékű üzleti titkok feldolgozására, tárolására is alkalmas rendszer biztonsági osztálya.
- Információvédelmi kiemelt biztonsági osztály: Az államtitok, a katonai szolgálati titok, valamint a nem minősített adatok közül a nagy tömegű különleges személyes adatok és nagy értékű üzleti titkok feldolgozására, tárolására alkalmas rendszer biztonsági osztálya.

(4) Az információs vagyonelemek besorolása, jelölése az Informatikai Szabályzat szerint (lásd Informatikai Szabályzat 5.4 fejezet) történik és a végrehajtásáért az Üzemeltető felelős.

16. §
Informatikai rendszerek beszerzése, fejlesztése és karbantartása

(1) ***Alkalmazások helyes használata:***
- Az „A" osztályú alkalmazásokhoz kizárólag azon felhasználók férhetnek hozzá, akiknek az Egyetemi feladat-és/vagy hatáskörük (munkakörük, illetve vezetői feladataik ellátása) ezt megkívánja, és legfeljebb olyan jogosultsággal, amit a munkakörük maradéktalan ellátása megkíván. Nevesítve:
  - a rendszer üzemeltetői (üzemeltetői jogosultsággal)
  - a rendszer felhasználói (a munkakörükhöz, szerepükhöz szükséges lekérdező és módosító jogosultságokkal)

- A rendszer fejlesztői a szolgáltató alkalmazáson nem rendelkezhetnek üzemeltetői jogosultságokkal, mivel ez az ő munkakörük ellátáshoz nem szükséges (éles üzemű szolgáltató rendszerben fejlesztés nem történhet).

(2) ***Kriptográfiai szabályozások:***

- Az „A" és „B" osztályú rendszerekbe történő, módosítási jogosultságot is lehetővé tevő bejelentkezés csak titkosított kommunikációval (pl. SSH, SSL, IPsec) engedélyezett, kivéve azon bejelentkezési területeket, ahol a felhasználó munkahelye és a szolgáltató rendszer közötti csatorna külső fél általi lehallgatása technikailag nem lehetséges (pl. fizikai védelem miatt).
- A hozzáférési jogosultságok elbírálását végző komponensek bármely rendszer esetében a felhasználói jelszavakat csak titkosítva tárolhatják.
- Egyéb kriptográfiai szabályozások az adott szolgáltatás SLA-jában találhatóak.

(3) ***Rendszer fájlok biztonsága:***

- A szolgáltató rendszerek működését biztosító rendszer fájlokhoz a felhasználók csak olyan mértékben férhetnek hozzá, amit a szolgáltatás használata feltétlenül megkövetel. A szolgáltatás szempontjából kritikus rendszerfájlokat a felhasználók nem módosíthatják.
- A rendszerfájlok védelme, az üzembiztos konfiguráció megőrzése és helyreállíthatóságának biztosítása az üzemeltető által erre kijelölt vagy megbízott személy (jellemzően a rendszergazda) kötelessége.

(4) ***Fejlesztési és támogatási folyamatok biztonsága:***

- Minden „A" és „B" osztályú alkalmazás fejlesztési tevékenységét a szolgáltató alkalmazás-példánytól és annak adatbázisától elkülönülten kell végezni. Amennyiben a fejlesztési tevékenységhez védett intézményi adatok is szükségesek, akkor a fejlesztői rendszer is „A" és „B" osztályú rendszernek minősül és a hozzáférési jogosultságok ennek megfelelően adhatók ki.
- Egyetemi fejlesztésű vagy vásárolt illetve ajándékba kapott szolgáltató rendszer csak funkcionális teszt után vonható szolgáltató üzembe. A funkcionális tesztnek az SLA-ban 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.
- 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.
- „A" osztályú alkalmazáson csak a teszt rendszeren végzett teszt sikeres tesztelési jegyzőkönyve birtokában és a felelős vezető által erre kijelölt vagy megbízott személy (jellemzően a rendszergazda) engedélyével végezhető változtatás (külső munkavégző esetében is). Ezen előírás alól csak a szolgáltatás helyreállítását célzó sürgős hibajavítás jelent kivételt. Ilyenkor a dokumentálást utólag kell elvégezni.

(5) ***Műszaki sérülékenység menedzsment:*** Az adott alkalmazás üzemeltetőjének felelőssége a publikált technikai sérülékenységek elleni védekezés megvalósítása. A publikált sérülékenységek elleni védekező intézkedés (pl. kiadott hibajavítások

telepítése, a sérülékenység elkerülésére irányuló konfigurációs beállítások) legkésőbb az észlelést követő első munkanapon végrehajtandó.

17.§
Új információ-feldolgozó rendszerek elfogadási eljárása

Új informatikai szolgáltatás TIO-hoz benyújtásra kerülő indítási kérelméhez az Informatikai Szabályzat szerint csatolni kell a rendszer vázlatos leírását és a tervezett SLA-t. Ezen anyagok alapján a TIO igazgatója a szolgáltatás engedélyezése előtt javaslatot kérhet az IBSZ mellékletek aktualizálására, az új szolgáltatás IBSZ paramétereinek megállapítására. A szolgáltatás indítási kérelem automatikusan az Informatikai Szabályzat és az IBSZ elfogadási szándéknyilatkozatának is tekintendő.

18. §
Működés-folytonosság biztosítása

A működés-folytonosság információbiztonsági vetülete: Az Egyetem működése szempontjából kritikus, „A" és „B" osztályú rendszerek működés-folytonosságának biztosítása az üzemeltető feladata. Ez kiterjed az IT Szabályzatban foglaltak maradéktalan betartására, a felelős incidenskezelésre, a szükséges funkcionális és biztonsági javítások telepítésére és az IBSZ betartására, valamint a rendszer fejlesztési terveinek erőforrás-kalkuláción alapuló körültekintő elkészítésére.

19. §
Információbiztonsági események menedzsmentje

(1) ***Biztonsági események és gyengeségek jelentése:***

- „A", „B" és „C" osztályú szolgáltató rendszer esetében a szolgáltatás üzemeltetője köteles incidens bejelentési lehetőséget biztosítani a felhasználóknak, és a bejelentés módjáról az SLA-ban kell rendelkezni. A bejelentett incidenseket az üzemeltetők a szolgáltató rendszer integritásának és a kezelt adatok védelmében kötelesek lehetőség szerint rövid reakcióidővel elbírálni és a szükséges lépéseket (pl. hozzáférés korlátozás, biztonsági komponensek beállításainak módosítása) megtenni. Az üzemeltető köteles a bejelentőt tájékoztatni a biztonsági esemény következményeiről és a megtett intézkedésekről. Tömeges érintettség esetén lehetőség van a TIO központi tájékoztató csatornáinak használatára is.
- Biztonsági esemény vagy gyengeség bejelentése esetén a bejelentő köteles csatolni mindazon adatokat, amik az esemény megítéléséhez legjobb tudása szerint szükségesek (pl. időpont, tapasztalt jelenség, naplóbejegyzés, stb.)
- Az informatikai szolgáltatások igénybevétele közben tapasztalt biztonsági gyengeségek jelentése (a rendszer működőképességének fenntarthatósága érdekében) minden felhasználónak kötelessége. Ennek elmulasztása vagy a gyengeség kihasználása biztonsági eseménynek minősül.

(2) ***Információbiztonsági események és fejlesztések menedzsmentje:***

- Az informatikai szolgáltató rendszerek esetében egyenszilárdságú biztonsági megoldásokat kell kialakítani. Rendszerenként egységes tervezés és megvalósítás

alapján kell a biztonsági megoldásokat kezelni. Amennyiben egy informatikai rendszer egy másik szolgáltatását igénybe veszi, akkor az SLA biztonsági követelményei az igénybevevő rendszer egészére vonatkoznak.

- A megvalósítandó vagy üzemben álló szolgáltató rendszer rendszertervének a felhasználók számára előírt biztonsági megoldásokat is tartalmaznia kell. Amennyiben ezek a változó követelmények miatt nem bizonyulnak elegendőnek, a rendszer fejlesztési tervében szerepeltetni kell az új biztonsági rendszer tervezett megoldásait.

20. §
Az információbiztonság független felülvizsgálata

A TIO igazgatója kéri fel, vagy jelöli ki a felülvizsgálatot végző szervezetet vagy személyt. A független audit szükségességére és módjára esetileg a TIO igazgatója tesz javaslatot az adott IT szolgáltatásért felelős szervezeti egység vezetőjének. Az „A" osztályú rendszerek esetén a felülvizsgálat 3 évente javasolt. Az információbiztonsági vizsgálat eredményeit meg kell küldeni a belső ellenőrzési csoportnak.

21. §
Egyetemen kívülre irányuló adatszolgáltatás, adatátadás

(1) A külső felekkel, partnerekkel való kapcsolattartás szabályai:

- Személyes vagy egyetemi adatok kiadása csak a hatályos jogszabályoknak és az egyetemi belső szabályozásokban foglalt felhatalmazásoknak megfelelően történhet, és kizárólag az arra jogosult által.
- Az átadott adatoknak a hatályos jogszabályok által előírt védelméért az adatot megkapó tartozik felelősséggel.
- Az adatszolgáltató, adatátadó az adatátadást megelőzően véleményt, tájékoztatást kérhet a TIO igazgatójától adatvédelmi és információbiztonsági kérdésekben.

(2) Adatok kiadása az „A" és „B" biztonsági osztályba sorolt rendszerekből az adott szervezeti egység vezetőjének engedélyével lehetséges, kivételt ez alól az olyan eset képez, amikor az adatcserét, adatátadást – jogszabály felhatalmazása alapján – jogszabály vagy szerződés rögzíti. Utóbbi esetben a szerződésnek tartalmaznia kell az adatkezelésre vonatkozó szabályokat.

22.§
Az IBSZ felülvizsgálata, módosítása

(1) A szabályzat felülvizsgálatára az alábbiak szerint kerül sor: háromévente egy alkalommal (az esedékes következő felülvizsgálati időpontot a dokumentum lezárásakor kell kijelölni) illetve minden olyan esetben, amikor a szabályzatban leírtakhoz képest jelentős jogszabályi és egyéb változás(ok) történnek.

(2) A jelen szabályzat mellékletei GMF Főigazgatói Körlevél alapján módosíthatóak.

(3) Az Informatikai Biztonsági Szabályzattal kapcsolatos észrevételeket, változtatási javaslatokat a TIO igazgatójának címzett, az 1. mellékletben található változáskezelési lapon lehet benyújtani.

23. §
Záró rendelkezések

(1) A szabályzat mellékleteinek módosítását a gazdasági és műszaki főigazgató saját hatáskörben végzi. A mellékletek GMF főigazgatói utasítások formájában készülnek és módosulnak.

(2) Jelen szabályzat a kiadás napján lép hatályba.

Budapest, 2014. augusztus 28.

Dr. Péceli Gábor
rektor

Mellékletek

1. számú melléklet

IBSZ változáskezelési lap

Benyújtó neve:

Beosztása:

Szervezeti egysége:

e-mail:

telefon:

Benyújtás dátuma:

Aláírás:

A változtatni kívánt IBSZ bekezdés száma, megnevezése:

A változtatási javaslat rövid indoklása:

A javasolt új szövegrész:

TIO tölti ki

Beérkezés időpontja:

Átvevő:

Az igény vizsgálatával kapcsolatos megjegyzések:

Az igény elbírálása: Bekerül a dokumentumba a változtatás

NEM kerül be a dokumentumba a változtatás

Indoklás:

Aláírás:

2. számú melléklet

Felhasználói nyilatkozat

Alulírott, mint a Budapesti Műszaki és Gazdaságtudományi Egyetem és annak szervezeti egységei (a továbbiakban: Egyetem) által nyújtott IT szolgáltatások felhasználója kijelentem, hogy az Egyetem informatikai rendszereinek Informatikai Szabályzatát és Informatikai Biztonsági Szabályzatát megismertem, az azokban foglaltakat betartom, és az azokban meghatározottaknak megfelelően fogok eljárni.

Kötelezettséget vállalok, hogy az informatikai rendszerek használata során az Egyetemről tudomásomra jutott információkat, adatokat időbeli korlátozás nélkül

a. üzleti titokként kezelem,

b. azokat jogosulatlan személy részére nem szolgáltatom ki, illetve nem teszem egyéb módon hozzáférhetővé,

c. azokat csak a munkakörömben foglalt feladatok teljesítéséhez, az ehhez szükséges mértékben használom fel, és csak az annak megismerésére jogosult számára teszem hozzáférhetővé,

d. azzal egyéb módon nem élek vissza.

Az IT rendszerekben tárolt, általam megismert személyes adatokra a fentieket megfelelően alkalmazva, azok tekintetében is titoktartási kötelezettséget vállalok.

Az alábbiakat nyomtatott betűkkel kell kitölteni!

Név:

Lakcím:

Dátum:

Aláírás:

A nyilatkozatot átvettem:

Név:

Szervezeti egység:

Dátum:

(Aláírás)

3. számú melléklet

Az információbiztonság témaköréhez kapcsolódó legfontosabb törvények, szabványok és műszaki leírások

Az információbiztonsághoz legszorosabban kapcsolódó fontos törvények, jogszabályok Magyarországon:

- az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény.
- 2012. évi I. tv. a Munka Törvénykönyvéről
- 2012. évi C. tv. a Büntető Törvénykönyvről
- 1996. évi LVII. tv. a tisztességtelen piaci magatartás és a versenykorlátozás tilalmáról.

Biztonságtechnikai, tűzvédelemi szabványok, előírások:

- 2/(II. 27.) ÉVM rendelet az Országos Építési Szabályzat Átadásáról.
- MSZ 595/1-9 Építmények tűzvédelme.
- MSZ EN 3/1-5 Tűzoltó készülékek.
- MSZ 9785/1-2 Tűzjelző berendezés.
- MSZ IEC 839-1 Riasztórendszerek.
- MSZ 274 Villámvédelem.
- MSZ EN 60950 Adatfeldolgozó berendezések és irodagépek biztonsági előírásai.

Egyéb szabványok, ajánlások:

- MSZ EN 60950 Adatfeldolgozó berendezések és irodagépek biztonsági előírásai.
- MeH ITB 12. ajánlása: az informatikai rendszerek fizikai, logikai és adminisztratív védelmi követelményeit és az ezek alapján foganatosítandó védelmi intézkedéseket írja le
- ITSEC = Information Technology Security Evaluation Criteria (Információtechnológia Biztonsági Értékelési Kritériumok) az Európai Közösség ajánlása az informatikai rendszerek biztonságának funkcionális és minősítési követelményeire
- TCSEC = Trusted Computer System Evaluation Criteria (Biztonságos Számítógépes Rendszerek Értékelési Kritériumai), az Egyesült Államok Védelmi Minisztériuma által kiadott informatikai biztonsági ajánlás
- MeH ITB 8. ajánlásán alapuló kockázatkezelési módszertan
- ISO/OSI 7498-2 szabvány a nyílt rendszerek biztonsági architektúrájára vonatkozik. Magyar megfelelője: MSZ OSI 7498-1

4. számú melléklet

Titoktartási nyilatkozat (üzleti partnerek részére)

Cégnév/Név: .....

Cégjegyzékszám/Nyilvántartási szám/Vállalkozói igazolvány száma: .....

Székhely: .....

Cégszerű aláírásra jogosult képviselő(k): .....,

(A továbbiakban: a .....)

Alulírott(ak), a fent megnevezett képviseletében kijelentjük és kötelezettséget vállalunk arra, hogy a Budapesti Műszaki és Gazdaságtudományi Egyetemmel .....-án megkötött ..... szerződés (a továbbiakban: a szerződés) teljesítése során a Budapesti Műszaki és Gazdaságtudományi Egyetemről (a továbbiakban: BME) a szerződéssel kapcsolatosan, azzal összefüggésben a ..... tudomására jutott információkat, adatokat, így különösen a személyes adatokat, valamint a BME tulajdonát, vagyonkezelését képező, vagy a tevékenységével, gazdálkodásával, működésével, pénzügyi és jogi helyzetével kapcsolatos információkat (amelyeket a szerződéskötés, vagy annak teljesítése érdekében a BME előtte felfed, illetőleg amelynek a szerződéssel összefüggésben váltak számára ismertté vagy egyébként hozzáférhetővé)

a. üzleti titokként kezeli,

b. azt jogosulatlan személy részére nem szolgáltatja ki, illetve nem teszi egyéb módon hozzáférhetővé,

c. azt csak az együttműködés teljesítéséhez, az ehhez szükséges mértékben használja fel, és csak a teljesítésben közvetlenül részt vevő alkalmazottai, illetve alvállalkozói számára teszi hozzáférhetővé, és

d. azzal egyéb módon nem él vissza.

A ..... képviseletében kijelentem (kijelentjük), hogy a ..... az ilyen bizalmas, üzleti titkot képező információkat kizárólag indokolt esetben és kizárólag a BME előzetes, írásbeli hozzájárulásának birtokában használhatja fel a szerződés teljesítésének érdekében kívül eső céllal összefüggésben. A jelen nyilatkozatban vállalt titoktartási kötelezettség nem vonatkozik az olyan információra

a. amely köztudomású;

b. amelyet nem a szerződés vagy a jelen nyilatkozat megsértésével hozunk nyilvánosságra;

c. amely nyilvánosságra hozatali korlátozás nélkül a ..... birtokában volt már azelőtt, hogy a BME-től megkapta volna;

d. amelyet a ..... olyan harmadik Féltől kapott, aki jogszerűen szerezte meg, és jogszerűen továbbította, vagy hozta létre azt, és akit nem köt a titoktartási kötelezettség;

e. amelyet a ..... a BME bizalmas információjának felhasználása nélkül maga hozott létre; vagy

f. amelyet a .....-nak – jogszabályban meghatározott – kötelessége átadni az illetékes hatóság számára.

A jelen nyilatkozatban vállalt kötelezettségek a szerződés megszűnését követően határozatlan ideig hatályban maradnak, kivéve, ha a kérdéses információ hozzáférhetővé tételének megakadályozása – jogszabályváltozás, vagy egyéb körülmények beálltának következtében – kétséget kizáró módon nem áll többé a BME érdekében, illetve ha az információ nem került egyébként is nyilvánosságra.

Tudomással bírunk arról, hogy a jelen nyilatkozatban foglaltak megsértését a BME súlyos szerződésszegésként tekinti.

A ..... vállalja, hogy a jelen nyilatkozatban meghatározott bármely információ megszerzésével érintett munkatársaival, a szerződés teljesítésében közreműködőkkel titoktartási nyilatkozatot irat alá, mely titoktartási nyilatkozat legalább a jelen nyilatkozatban meghatározott megkötéseket tartalmazza, és ennek teljesítését a BME felhívására megfelelően igazolja.

Budapest, ...

.....

(cégszerű aláírás)