A MISKOLCI EGYETEM

INFORMATIKAI BIZTONSÁGI SZABÁLYZATA

Miskolc, 2016.

7.11. sz. Egyetemi Szabályzat

A MISKOLCI EGYETEM
INFORMATIKAI BIZTONSÁGI SZABÁLYZATA

A MISKOLCI EGYETEM SZENÁTUSÁNAK
173/2016. SZ. HATÁROZATA

Készült **8** példányban
1. sorszámú, változás átvezetésére kötelezett példány.

Kiadásért felelős: A Miskolci Egyetem Rektora
Kiadja a Miskolci Egyetem
ME Sokszorosító Üzeme:
Nyomdaszám:Ka.20 -….. ME
Miskolc-Egyetemváros, 2016. …….
A szabályzat gondozásáért felelős: Informatikai Szolgáltató Központ igazgatója

Tartalomjegyzék

PREAMBULUM

(1) Az informatikai rendszerek üzemeltetése során a veszélyeket teljes mértékben megszüntetni nem lehet. A veszélyeztetettség kockázati tényező, amellyel számolnunk kell, de állandóan törekedni szükséges 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, folyamatos figyelés az időben történő észlelés érdekében és – bekövetkezés esetén – gyors és hatékony reakció/beavatkozás a kár minimalizálása érdekében.

(3) A megelőző kontrollok közé tartoznak azon technikák, melyekkel megpróbáljuk elkerülni egy adott veszélyhelyzet bekövetkezését. 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 előre megtervezett, hatékony cselekvés-sorozat követi.

Általános rendelkezések

1.§

(1) Az Informatikai Biztonsági Szabályzat (a továbbiakban: IBSZ) célja, hogy a Miskolci Egyetem (a továbbiakban: 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 az MSZ ISO/IEC 27001:2014 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 informatikai infrastruktúrájának használatára, a kötelezettségvállalás dokumentumában a külső harmadik személynek (szervezetnek) kötelezettséget kell vállalnia az IBSZ-ben foglaltak betartására.

Az IBSZ célja

2.§

(1) 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 figyelembe vételével 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.

IT rendszerek biztonsági osztályai, besorolás

3.§

(1) Az Egyetemen üzemeltetett IT rendszereket az alábbi öt 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) **„5." biztonsági osztályú rendszerek:** Az Egyetem működése szempontjából kritikus rendszerek, amelyek esetében kiemelkedően nagy káresemény következhet be, mivel különleges személyes adat kiemelten nagy mennyiségben sérülhet. Emberi életek kerülnek közvetlen veszélybe, személyi sérülések nagy számban következhetnek be. A nemzeti adatvagyon helyreállíthatatlanul megsérülhet. Az ország, a társadalom működőképességének fenntartását biztosító létfontosságú információs rendszer rendelkezésre állása nem biztosított. A lehetséges társadalmi-politikai hatás: súlyos bizalomvesztés az érintett szervezettel szemben, alapvető emberi, vagy a társadalom működése szempontjából kiemelt jogok sérülhetnek. Az érintett szervezet üzlet- vagy ügymenete szempontjából nagy értékű üzleti titkot, vagy kiemelten érzékeny folyamatokat kezelő elektronikus információs rendszer, vagy információt képező adat tömegesen vagy jelentősen sérülhet. A közvetlen és közvetett anyagi kár eléri az érintett szervezet költségvetésének 15%-át. Az Egyetem vonatkozásában az alábbi rendszerek:

a) Gazdálkodási rendszer (üzemeltető: Gazdasági Igazgatóság)

b) Neptun Egységes Tanulmányi rendszer (üzemeltető: Üzemeltetési Igazgatóság, Informatikai Szolgáltató Központ (a továbbiakban: ISZK)).

(3) **„4." biztonsági osztályú rendszerek:** Az Egyetem működése szempontjából kiemelt fontosságú rendszerek, amelyek esetében nagy káresemény következhet be, mivel különleges személyes adat nagy mennyiségben sérülhet. Személyi sérülések esélye megnőhet (ideértve például a káresemény miatti ellátás elmaradását, a rendszer irányítatlansága miatti veszélyeket). Az érintett szervezet üzlet-, vagy ügymenete szempontjából nagy értékű, üzleti titkot, vagy különösen érzékeny folyamatokat kezelő elektronikus információs rendszer, vagy információt képező adat tömegesen, vagy jelentősen sérülhet. A káresemény lehetséges társadalmi-politikai hatásaként a jogszabályok betartása, vagy végrehajtása elmaradhat, bekövetkezhet a bizalomvesztés a szervezeten belül, az érintett szervezet felső vezetésében, vagy vezetésében személyi felelősségre vonást kell alkalmazni. A közvetlen és közvetett anyagi kár eléri az érintett szervezet költségvetésének 10%-át. Az Egyetem vonatkozásában az alábbi rendszerek:

a) Informatikai hálózat (üzemeltető: ISZK),

b) Telefonközpont és a hozzátartozó hálózat (üzemeltető: Üzemeltetési Igazgatóság, ISZK),

c) Központi levelező kiszolgálók (üzemeltető: ISZK),

d) Központi tárhely kiszolgálók (üzemeltető: ISZK),

e) Autentikációs rendszerek (üzemeltető: ISZK).

(4) **„3.” biztonsági osztályú rendszerek:** Az Egyetem napi működése szempontjából olyan rendszerek, amelyek esetében közepes káresemény következhet be, mivel különleges személyes adat sérülhet, személyes adatok nagy mennyiségben sérülhetnek. Az érintett szervezet üzlet-, vagy ügymenete szempontjából érzékeny folyamatokat kezelő elektronikus információs rendszer, információt képező adat, vagy egyéb, jogszabállyal (orvosi, ügyvédi, biztosítási, banktitok, stb.) védett adat sérülhet. A lehetséges társadalmi-politikai hatás: bizalomvesztés állhat elő az érintett szervezeten belül, vagy szervezeti szabályokban foglalt kötelezettségek sérülhetnek. A közvetlen és közvetett anyagi kár eléri az érintett szervezet költségvetésének 5%-át. Az Egyetem vonatkozásában az alábbi rendszerek:

a) Kiszolgálók (szerverek) (üzemeltető: szervezeti egységek),

b) Kutatói rendszerek (üzemeltető: szervezeti egységek),

c) Technológiai rendszerek (environment, middleware) (üzemeltető: szervezeti egységek),

d) Egyetemi web szerver szolgáltatás (üzemeltető: ISZK),

e) Központi névtár, telefonkönyv (üzemeltető: ISZK).

(5) **„2.” biztonsági osztályú rendszerek:** Csekély káresemény következhet be, mivel személyes adat sérülhet. Az érintett szervezet üzlet-, vagy ügymenete szempontjából csekély értékű, és/vagy csak belső (intézményi) szabályzóval védett adat, vagy elektronikus információs rendszer sérülhet. A lehetséges társadalmi-politikai hatás az érintett szervezeten belül kezelhető. A közvetlen és közvetett anyagi kár eléri az érintett szervezet költségvetésének 1%-át. Az Egyetem vonatkozásában az alábbi rendszerek:

a) Központi hallgatói laborok (üzemeltető: ISZK).

b) Kari laborok (üzemeltető: szervezeti egységek).

(6) **„1.” biztonsági osztályú rendszerek:** Az Egyetemen működő azon rendszerek, amelyek esetében csak jelentéktelen káresemény következhet be, mivel az elektronikus információs rendszer nem kezel jogszabályok által védett (pl.: személyes) adatot. Nincs bizalomvesztés, a probléma az érintett szervezeten belül marad, és azon belül meg is oldható. A közvetlen és közvetett anyagi kár az érintett szervezet költségvetéséhez képest jelentéktelen.

Az Egyetem informatikai biztonsági alapelvei

4.§

(1) 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 kockázattal arányos és folyamatos.

Információbiztonsági alapelvek

5.§

(1) Az Egyetem szolgáltatásért felelős szervezeti egységeinek az „5.”, „4.” és „3.” biztonsági osztályba 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 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 ISO 7498-1. szabványban meghatározott nyílt rendszerek architektúrája minden rétegére, azaz mind az informatikai 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 zár folyamatát.

c) **Kockázattal arányos** a védelem, ha kellően nagy időintervallumban a védelem költségei arányosak a potenciális kárérték 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 folytonossága úgy biztosítható, hogy az informatikai rendszerek fejlesztése és megvalósítása során kialakított védelmi képességeket az üzemből történő kivonásig folytonosan biztosítani kell az előírások betartásának rendszeres ellenőrzésével és az ezt követő védelmi intézkedésekkel.

Az informatikai biztonság alapterületei

6.§

(1) 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.

(2) 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.

Az Egyetem informatikai biztonsági politikája

7.§

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

(2) Az Egyetem informatikai biztonságpolitikájának elsődleges célja a működőképesség fenntartása, ezért 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 az ISZK jogosult az egyetemi hálózatból kitiltásra.

(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 kell kötni az IBSZ-ben foglaltak szerint.

(5) Hangsúlyozottan törekedni kell a törvényi és jogszabályi megfelelőségre, különös tekintettel a személyes adatok kiemelt védelmére.

(6) Törekedni kell a mobilitás lehetősége és a biztonság 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.

(9) Vezetői elkötelezettség: Minden szervezeti egység vezetője személyesen felel az információbiztonság kultúrájának kialakításáért és fenntartásáért. A vezetők elkötelezettségüket személyes példamutatással (szabályok betartása) és személyes felelősségvállalással demonstrálják. A belső és külső szolgáltatói megállapodások 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.

Feladat- és hatáskörök

8.§

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

Az Üzemeltető hatásköre és felelőssége

9.§

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

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

(3) Üzemeltetők a következők:

a) az adott IT szolgáltatást nyújtó, azért felelős szervezeti egység (a továbbiakban: a szolgáltatásért felelős szervezeti egység),
b) illetve az általa szerződéssel ezzel megbízott külső, az Egyetemmel munkavégzésre irányuló (megbízási, vállalkozási) jogviszonyban álló személy (a továbbiakban együtt: az Üzemeltető), az irányadó egyetemi szabályzatoknak megfelelően.

(4) 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.

(5) Abban az esetben, ha a szolgáltatásért felelős szervezeti egység az üzemeltetéssel külső harmadik személlyel, szervezettel köt szerződést, a szerződésben szerepeltetni kell a következőket:

a) A külső harmadik személy kötelezettség-és felelősségvállalását az egyetemi tulajdonú IT rendszerek esetében a hatályos jogszabályoknak, az Egyetem mindenkori belső szabályozásainak – különösen az IBSZ-nek – való megfelelésért, valamint a szerződésben rögzített műszaki feltételek betartásáért,

b) A megkötött szolgáltatási szerződésben a Szolgáltatási Szint Szerződés-nek (továbbiakban SLA) megfelelő kötelezettségek vállalását a külső harmadik személy, szervezet részéről,

c) Az Egyetem nevében eljáró szervezeti egység jogát ennek ellenőrzésére,

d) Az Egyetemre vonatkozó adatvédelmi és információbiztonsági kérdéseket.

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

(6) Az „5.”, „4.” és „3.” biztonsági 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 csak kivételesen indokolt esetben a Kancellártól kaphat felhasználási jogot „5.”, „4.” vagy „3.” biztonsági osztályú rendszerhez, és csak abban az esetben, ha az az általa ellátandó feladathoz elengedhetetlenül szükséges.

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

A felhasználók felelőssége

10.§

(1) A felhasználó köteles az IBSZ-ben foglaltaknak megfelelően használni az IT rendszert.

(2) 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 szervezeti egységnek.

(3) A szolgáltatás felhasználója teljes felelősséggel tartozik az adott szolgáltatáshoz vállalt kötelezettségek betartásáért, beleértve a korlátos erőforrások pazarlása miatt az üzemeltetőnél keletkező többletköltségeket is.

(4) Az „5." biztonsági 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.

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

(6) Az Egyetem informatikai rendszereit felhasználók a szakmai szervezetekben való részvételükkor is kötelesek az IBSZ vonatkozó előírásait betartani.

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

Az ISZK feladatai és felelőssége

11.§

(1) Az Egyetem információbiztonsági vezetője az ISZK igazgatója.

(2) Az Egyetem informatikai biztonságának szabályozását és koordinálását az ISZK végzi.

(3) Az ISZK engedélyezi új, egyetemi szintű IT rendszer indítását.

(4) 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 az ISZK jogosult.

(5) A jelentős súlyú és/vagy más IT rendszereket és azok felhasználóit is veszélyeztető esetben az ISZK jogosult az egyetemi hálózatból való kitiltásra.

(6) Az ISZK 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.

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

(8) Az ISZK igazgatója felelős a kapcsolattartásért a különleges érdekközösségekkel, mint például a magyar non-profit Internet használók közössége (Hungarnet). Az előzőekben

megfogalmazott hivatalos tagsági és kapcsolattartási kérdésekben a Kancellár az ISZK igazgatójának előterjesztése alapján dönt az Egyetem érdekeinek figyelembe vételével.

Az IBSZ-ben foglaltak megszegésének szankciói

12.§

(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.

(2) A felhasználókat a szabályzatban leírtak esetében az alábbi szankciók sújthatják:

a) szolgáltatás megtagadás (kizárás a szolgáltatásból), melyről a Kancellár az ISZK igazgatójának előterjesztése alapján dönt,

b) 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 az ISZK 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.

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

Környezeti és fizikai biztonság

13.§

(1) **Fizikai biztonsági határvédelem:** az „5.” biztonsági osztályú 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.

(2) **Fizikai belépés szabályozás:** Az „5.” biztonsági osztályú rendszerek komponenseit tartalmazó szolgáltató helyiségekbe (gépterem, kábelrendezők stb.) való belépési jogosultságot a szolgáltatásért felelős szervezeti egység vezetője engedélyezi egyetemi dolgozónak vagy a külső szerződött partnernek a helyiségek és a végezhető tevékenységek felsorolásával. A belépési lehetőséggel rendelkezők a 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:**

a) 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, felügyelő terminál stb.) csak beléptető rendszerrel védett munkaszobában és irodában helyezhetők el.

b) 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:**

a) Az „5." biztonsági osztályú 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.

b) Egyedi esetben a szolgáltatásért felelős szervezeti egység vezetője egyéb előírásokat is megfogalmazhat.

c) A tűzvédelmi rendelkezéseknek megfelelően az erősáramú ellátó rendszernek tartalmaznia kell olyan központi áramtalanítókapcsolót, ami tűzjelzés esetén a biztonságos oltás feltételeit megteremti.

d) Minden fenti helyiség esetén biztosítani kell azt a hűtési kapacitást, ami a teljes termelt hőmennyiség biztonságos elvezetését automatikusan meg tudja oldani.

e) 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 „5." biztonsági osztályú rendszereket tartalmazó helyiségekben minden olyan, nem az üzemeltető által folytatott munkavégzés, ami az informatikai rendszereket vagy azok működését veszélyezteti, csak előzetes egyeztetés alapján, felügyelet mellett végezhető. Az egyeztetést a munkavégző cég és az üzemeltető szervezeti egység vezetője, vagy az általa kijelölt munkatárs végzi. A helyiség gépészeti berendezéseit veszélyeztető munkák csak az üzemeltető előzetes engedélyével folytathatók.

(6) **Nyilvános hozzáférés, szállítási területek:** Az „5." biztonsági osztályú rendszereket tartalmazó helyiségekben minden szállítási tevékenység csak belépésre jogosult munkatárs felügyelete mellett végezhető.

(7) **Eszközök elhelyezése, védelme:** Minden „5." biztonsági osztályú rendszerkomponens fizikai elhelyezésénél törekedni kell a gépterem/kábelrendező felépítési elveinek betartására. Ezen irányelveket új komponens beszerzése esetén az ISZK előírhatja.

(8) **Támogató közművek (szolgáltatások):** A gépterem/kábelrendező helyiségekben üzembe állítandó új rendszerek esetében az installálást végző szakembereknek előzetesen konzultálnia kell az erősáramú és hűtési igény biztosításáról az ISZK illetékes munkatársaival. A szükséges gépészeti módosításokat az új rendszer üzembe állítása előtt el kell végezni.

(9) **Kábelbiztonság:** Az „5." és „4." biztonsági osztályú rendszerek védett helyiségen kívül húzódó, összekötő komponenseit tartalmazó alépítmények, kábelaknák védőcsövek az ISZK által felügyelt területnek minősülnek. Azokban munkát végezni, vagy a

megközelíthetőségüket korlátozni csak a rendszerkomponens üzemeltetőjének előzetes engedélyével lehet.

(10) **Eszközkarbantartás:**

a) Minden szolgáltató rendszer üzemeltetője köteles a hardver komponensek karbantartási igényét felmérni és ezeket úgy ütemezni, hogy a rendszer élettartama ne rövidüljön karbantartási hiányosságok miatt.

b) A gépészet külön karbantartási tervvel rendelkezik.

c) 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 telephelyről kivitt eszközök használata során bekövetkezett 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. Az eszközök ki/beszállítását szállítólevéllel kell kísérni, amin az eszköz(ök) egyedi azonosítóját (ha értelmezhető) fel kell tüntetni.

(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 „5.”, „4.” és „3.” biztonsági osztályú eszközök selejtezésénél gondoskodni kell az azon tárolt adatok selejtezés előtti fizikai megsemmisítéséről, az adatok szükség szerinti archiválását követően.

Kommunikáció és üzemelés menedzsment

14.§

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

a) Amennyiben a szervezeti egység szolgáltatás indítási kérelemmel fordul az ISZK igazgatójához, ezzel elismeri megfelelési szándékát az IBSZ kritériumainak. A szolgáltatás indítási kérelem csak adathiány vagy IBSZ sértés esetén utasítható el. Az elutasítást részletesen indokolnia kell az ISZK igazgatójának, nem kizárva az esetleges módosított újbóli kérelem beadását.

b) „5.”, „4.” és „3.” biztonsági osztályú rendszerek esetében az IBSZ megfelelést az ISZK 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.

c) Minden informatikai rendszer esetében a használatra vonatkozó igény bejelentése egyúttal az IBSZ elfogadásának szándéknyilatkozatát is jelenti. A hozzáférés megadásával a hivatkozott szabályzat a szolgáltatás nyújtója és igénybevevője között érvénybe lép.

d) Az „5.” és „4.” biztonsági 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 a szolgáltatásért felelős szervezeti egység vezetője eseti bizottságot nevezhet ki. Ezen bizottságnak mindig tagja az ISZK igazgatója is.

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

a) 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.

b) Az „5." és a „4." biztonsági kategóriájú IT szolgáltatások esetében az Egyetem egykapus ügyintézést és érdekképviseletet alkalmaz. Ezen szolgáltatók esetében az ügyfélkapcsolatra jogosult a szolgáltatásért felelős szervezeti egység vezetője.

(3) **Rendszertervezés és elfogadás:** Az informatikai szolgáltató rendszerek esetében az IBSZ megfelelést már a tervezési szempontok között szerepeltetni kell. Az üzemeltetni tervezett „5.", „4." és „3." biztonsági osztályú rendszerek esetében az IBSZ megfelelés az ISZK általi igazolása a szolgáltatás indításának szükséges feltétele.

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

a) Azon rendszerek esetében, ahol a kártékony és mobil kódok előfordulhatnak, a detektálásukat és elhárításukat végző komponensek installálása a szolgáltatási engedély kiadásának feltétele.

b) 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.

c) 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 az ISZK igazgatója jogosult, illetve köteles az ilyen levelező rendszernek a haladéktalan kitiltására illetve hálózati kapcsolatának megszüntetésére. A károkozás tényét az ISZK igazgatója köteles dokumentálni.

f) Felhasználói tulajdonú adathordozók használata esetén az adott eszköz használata következtében okozott károkért az Egyetem rendszereibe felhasználóként belépett személy a felelős (pl. vírusos USB kulcs).

(5) **Biztonsági mentések:**

a) Minden „5.", „4." és „3." biztonsági osztályú szolgáltató rendszer üzemeltetési leírásának tartalmaznia kell az alkalmazások és adatok mentési rendjét (a mentendő adatok körét, a mentés módját és gyakoriságát, a mentésért felelős személyt, a mentés tárolási rendjét).

b) „5." és „4." biztonsági osztályú rendszerek esetén külső tárolású mentésekkel is kell rendelkezni, „3." és „2." biztonsági osztályú rendszerek esetén on-site mentések is elfogadhatóak.

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

d) 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, illetve minimum az előző 30 szolgáltatási napra ki kell terjedniük.

e) Az „5." biztonsági 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 „3." biztonsági 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.

f) Minden „5.", „4." és „3." biztonsági 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 az ISZK 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 az ISZK végzi. A kommunikációs hálózathoz való csatlakozás feltétele a biztonsági előírások maradéktalan betartása.

(7) **Média kezelés:**

a) Az „5.", „4." és „3." biztonsági 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.

b) A mentések tárolása: Az „5." és „4." biztonsági osztályú rendszerek mentéseinek tárolása az ISZK által kijelölt és jóváhagyott védett helyiségben történik. A médiáról az üzemeltetésért felelős szervezeti egységnek nyilvántartást kell vezetni.

c) Mentések adathordozóinak használatból való kivonása és megsemmisítése a szolgáltatást üzemeltető feladata. A média megsemmisítéséről jegyzőkönyvet kell felvenni.

(8) **Információcsere:**

a) Az Egyetem „5.", „4." és „3." biztonsági osztályú rendszerei esetében az automatikus adatcserét lehetővé tevő kapcsolatok létesítéséhez ISZK 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.

b) Az adatcsere környezetét, technológiai megvalósítását dokumentálni kell az adatcserét kezdeményező alkalmazásüzemeltetőnek.

(9) **Elektronikus kereskedelem:**

a) Az elektronikus kereskedelmet lehetővé tevő alkalmazások esetében a biztonsági feltételek megteremtése érdekében az ISZK igazgatójának engedélye szüksége a rendszer működtetéséhez.

b) Az alkalmazás tervezésébe és megvalósításába be kell vonni az ISZK igazgatóját vagy annak kijelölt képviselőjét.

(10) **Monitorozás:** Az „5." és „4." biztonsági osztályú rendszerek esetében az üzemeltetők felelőssége az automatikus szolgáltatás monitorozó komponensek bevezetési lehetőségének vizsgálata és a monitorozás megvalósítása.

Emberi erőforrással kapcsolatos biztonsági kérdések

15.§

(1) **Alkalmazás előtti tennivalók:** Az „5." és „4." biztonsági osztályba sorolt rendszerek üzemeltetői és fejlesztői esetében, a rendszer üzemeltetéséért felelős szervezeti egység vezetőjének kötelessége az IBSZ betartására a figyelmet felhívni.

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

a) Az „5.", „4." és „3." biztonsági osztályú rendszerek esetében minden üzemeltető vagy felhasználó csak a munkakörének ellátásához elengedhetetlenül szükséges jogosultságokat birtokolhatja.

b) Az „5." és „4." biztonsági osztályú rendszerek bizonyos szolgáltatásinak igénybevételéhez 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 munkakörváltozás:**

a) A dolgozó jogviszonyának megszűnése vagy az informatikai biztonsággal kapcsolatos feladatait érintő munkakör változása esetén minden „5.", „4." és „3." biztonsági osztályú rendszer esetében az üzemeltetői, fejlesztői és felhasználói jogosultságot, ilyen tevékenységet lehetővé tevő belépési kódokat azonnal vissza kell vonni.

b) A volt dolgozó vagy hallgató a „3." és „2." biztonsági osztályú rendszerekben a 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 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 felelő 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.

Hozzáférés és jogosultság szabályozás

16.§

(1) **Általánosan betartandó szabályok:** Az azonosítás és hitelesítés funkció során az „5." biztonsági osztályú rendszerek esetében:

a) az egyedi felhasználókat és a felhasználó csoportokat jelszóval kell azonosítani,

b) a jelszavakat egyirányúan titkosítva kell tárolni,

c) a jelszó „öregítési" mechanizmust alkalmazni kell,

d) meg kell határozni a jelszavak minimális hosszát,

e) a jelszóadást és változtatást csak az erre a feladatra kijelölt rendszeradminisztrátor végezheti el,

f) rendszeradminisztrátor csak felhatalmazott személy lehet, magas prioritású jogokkal,

g) nehezen megfejthető jelszóalkotás támogatását biztosítani kell.

h) adott számú téves bejelentkezési kísérlet után az adott felhasználói jogosultsági rendszert bénítani kell, a téves bejelentkezés ténye rögzítendő és kivizsgálandó,

i) az adott rendszerhez hozzáférést és a hozzátartozó jogosultságot a szolgáltatás üzemeltetéséért felelős szervezeti egység vezetője vagy felhatalmazottja adhat ki.

Az elszámolhatóság és auditálhatóság biztosítása érdekében olyan regisztrálási és naplózási rendszert 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:

a) rendszerindítások, leállások, leállítások,

b) rendszeróra állítások,

c) be/kijelentkezések

d) program leállások,

e) az azonosítási és hitelesítési mechanizmus használata,

f) hozzáférési jog érvényesítése azonosítóval ellátott erőforráshoz,

g) azonosítóval ellátott erőforrás létrehozása vagy törlése,

h) felhatalmazott személyek műveletei, amelyek a rendszer biztonságát érintik.

(2) **Hozzáférési politika:**

a) Minden olyan informatikai rendszer esetében, ami az Egyetem működéséhez szükséges, illetőleg bármilyen védett információt tartalmaz, meg kell határozni a hozzáférésre jogosultak körét és hozzáférési kísérlet esetén a jogosultságot ellenőrizni kell.

b) 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 közös használatú hozzáférési lehetőséget kizárólag publikus adatok lekérdezésére birtokolhat.

c) A jogosultság kezelést az üzemeltetőnek napra készen kell tartani és dokumentálni.

(3) **Felhasználói hozzáférés menedzsmentje:**

a) Az adott informatikai rendszerhez történő hozzáférés módját a rendszeren működő szolgáltatások SLA-i tartalmazzák. Az igénybevétel során a természetes személynek azonosítania kell magát egyedi adatával vagy adat-párjával. Amennyiben az Egyetem az informatikai rendszerek felhasználóinak azonosítását és jogosultság-elbírálását központilag valósítja meg, erre a célra szolgáló rendszerekkel (pl. LDAP) és a felhasználói adatbázis kezelése egységesen és konzisztensen történik, akkor az „5.”, „4.” és „3.” biztonsági osztályú rendszereknek ehhez csatlakozási képességgel kell rendelkeznie. Kivételt azok a már meglévő és működő rendszerek képeznek, melyek nem képesek központi jogosultságkezelést megvalósítani.

b) 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.

c) Az „5.” és „4.” biztonsági osztályú rendszerek esetében az üzemeltető a hozzáférésre jogosultak esetében is előírhat engedélyezési eljárást a hozzáférés megadásához. Az engedélyt az üzemeltetőnek írásban, a kért jogosultságokat feltüntetve kell eljuttatnia a kérelmező részére. Minden „5.”, „4.” és „3.” biztonsági osztályú rendszer esetében az üzemeltető feladata, hogy a kiadott hozzáférések adatait naprakészen nyilvántartsa.

d) A hozzáférés indokának megszűnése esetén az üzemeltetőnek a hozzáférést haladéktalanul vissza kell vonnia.

(4) **Hálózati hozzáférés:**

a) 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 integritása védelmében azonnal megszüntetheti.

b) A hálózati szolgáltatások az üzembiztonság, nyomon követhetőség és a központi kezelhetőség szempontjai szerint vannak kialakítva.

a) Az internet bármely komponenséhez történő hozzáférés esetén a felhasználó köteles az Egyetem internet szolgáltatójának szabályzatát is betartani.

(5) **Operációs rendszer hozzáférés:** Az „5.”, „4.” és „3.” biztonsági 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 naplózni kell.

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

a) 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.

b) Minden „5.”, „4.” és „3.” biztonsági 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:**

a) Az „5.", „4." és „3." biztonsági 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.

b) 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 az ISZK jóváhagyásával megengedett vagy az ISZK 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:** Az ISZK központi autentikációs rendszert üzemeltet, melyhez a szervezeti egységek a saját rendszereiket csatlakoztathatják. Ehhez engedélyt az ISZK igazgatója ad ki, a rendszer használatára vonatkozó technikai ismeretek és szabályok tudomásul vétele után. Az ISZK a rendszer használatához technikai segítséget biztosít.

Titoktartási nyilatkozatok

17.§

(1) Az információbiztonsági szabályok betartásával és betartatásával kapcsolatban a 2. számú mellékletben részletezett titoktartási nyilatkozatot írnak alá az „5." és „4." biztonsági osztályú rendszerek üzemeltetői, illetve a felhasználók is, „3." és „2." biztonsági osztályú rendszerek esetén bizalmassági nyilatkozatot kell tenni. 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. A titoktartási nyilatkozatok aláírását, a rendszer üzemeltetéséért felelős szervezeti egység vezetője kezdeményezi.

(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 kitöltenie a szolgáltatás üzemeltetőjének, melynek aláírásával vállalja, hogy a birtokában lévő információval nem él vissza, azt jogosulatlanul nyilvánosságra nem hozza, vagy arra nem jogosult harmadik személy számára nem teszi hozzáférhetővé.

Megfelelőség

18.§

(1) **Jogszabályi megfelelőség:**

a) Az adott szolgáltatásért felelős szervezeti egység vezetőjének felelőssége a mindenkori jogszabályi megfelelőség biztosítása a nyújtott szolgáltatások vonatkozásában.

b) Az adott szolgáltatásért felelős szervezeti egység vezetője nem felel a felhasználók által elkövetett jogsértésekért (p. 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.

c) Az információbiztonság témakörében érvényes legfontosabb jogszabályok jegyzékét a 3. számú melléklet tartalmazza

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

a) Az adott szolgáltatásért felelős szervezeti egység vezetőjének felelőssége a mindenkori biztonsági politikának, szabványoknak és műszaki előírásoknak való megfelelőség biztosítása, szervezése a nyújtott szolgáltatások vonatkozásában.

b) Az információbiztonság témakörében érvényes legfontosabb szabványoknak és műszaki leírásoknak a jegyzékét a 3. számú melléklet tartalmazza.

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

a) 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 „5.” biztonsági osztályú rendszerek esetében. Ezt az ISZK igazgatója jogosult ellenőrizni. A felülvizsgálat költségei az üzemeltetőt terhelik.

b) Súlyos SLA sértés gyanúja esetén az ISZK igazgatója külön rendkívüli biztonsági ellenőrzést és felülvizsgálatot rendelhet el.

c) A felülvizsgálatok eredményei alapján az ISZK 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 pótolja) 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. Az ISZK igazgatója felelős az információbiztonsági események, incidensek tanulságai és a pozitív példák megjelenítéséért az ISZK szokásos információs csatornáin.

Az információvagyon menedzsmentje

19.§

(1) Az információs vagyon az üzemeltetési dokumentációkban leírtak alapján meghatározott. Az „5.”, „4.” és „3.” biztonsági osztályú 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 „5.”, „4.” és „3.” biztonsági osztályú 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.

a) Információvédelmi alapbiztonsági osztály: Személyes adatok, üzleti titkok, pénzügyi adatok, illetve az Egyetem belső szabályozásában hozzáférés-korlátozás alá eső (pl. egyes feladatok végrehajtása érdekében bizalmas) adatfeldolgozásra, tárolásra alkalmas rendszer biztonsági osztálya.

b) 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.

c) 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.

Informatikai rendszerek beszerzése, fejlesztése és karbantartás

20.§

(1) **Alkalmazások helyes használata:**

a) Az „5.” biztonsági 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:**

a) Az”5.” és „4.” biztonsági osztályú rendszerekbe történő, módosítási jogosultságot is lehetővé tevő bejelentkezés csak titkosított kommunikációval (p. SSH, SSL, IPsec) engedélyezett, kivéve azon bejelentkezési területeket, ahol a felhasználó munkahelye és a szolgáltató rendszer közötti csatorna fél általi lehallgatása technikailag nem lehetséges (pl. fizikai védelem miatt).

b) A hozzáférési jogosultságok elbírálását végző komponensek bármely rendszer a esetében felhasználói jelszavakat csak titkosítva tárolhatják.

(3) **Rendszer fájlok biztonsága**:

a) 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.

b) 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:**

a) Minden „5." és „4." biztonsági 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 „5." és „4." biztonsági osztályú rendszernek minősül és a hozzáférési jogosultságok ennek megfelelően adhatók ki.

b) 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.

c) Minden, a szolgáltatási felületen vagy a funkciókészletben különbséget tartalmazó alkalmazás verzió esetén a tesztelési eljárást újra 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.

d) „5." biztonsági 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.

Új információ-feldolgozó rendszerek elfogadási eljárása

21.§

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

Működés-folytonosság biztosítása

22.§

(1) A Működés-folytonosság információbiztonsági vetülete: Az Egyetem működése szempontjából kritikus „5.” és „4.” biztonsági osztályú rendszerek működés-folytonosságának biztosítása az üzemeltető feladata. Ez kiterjed a felelős incidenskezelésre, a szükséges funkcionális és biztonsági javítások telepítésére és az IBSZ betartására, valamint a rendszer fejlesztési terveinek erőforrás-kalkuláción alapuló körültekintő elkészítésére.

Információbiztonsági események menedzsmentje

23.§

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

a) „5.”, „4.” és „3.” biztonsági osztályú szolgáltató rendszer esetében a szolgáltatás üzemeltetője köteles incidens bejelentési lehetőséget biztosítani a felhasználónak, és a bejelentés módjáról 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 beállításának módosítása) megtenni. Az üzemeltető köteles a bejelentőt tájékoztatni a biztonsági esemény következményeiről és a megtett intézkedésekről. Tömeges érintettség esetén lehetőség van az ISZK központi tájékoztató csatornáinak használatára is.

b) 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.).

c) 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**:

a) 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.

b) 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.

Az információbiztonság független felülvizsgálata

24.§

(1) Az ISZK igazgatója kéri fel, vagy jelöli ki a felülvizsgálatot végző szervezetet vagy személyt. A független audit szükségességére és módjára esetileg az ISZK igazgatója tesz javaslatot az adott IT szolgáltatásért felelős szervezeti egység vezetőjének. Az „5.” biztonsági osztályú

rendszerek esetén a felülvizsgálat 3 évente javasolt. Az információbiztonsági vizsgálat eredményeit meg kell küldeni a belső ellenőrzési csoportnak.

Egyetemen kívülre irányuló adatszolgáltatás, adatátadás

25.§

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

a) Személyes vagy egyetemi adatok kiadása csak a hatályos jogszabályoknak és az egyetemi belső szabályozásokban foglalt felhatalmazásoknak megfelelően történhet, és kizárólag az arra jogosult által.

b) Az átadott adatoknak a hatályos jogszabályok által előírt védelméért az adatot megkapó tartozik felelősséggel.

c) Az adatszolgáltató, adatátadó az adatátadást megelőzően véleményt, tájékoztatást kérhet az ISZK igazgatójától adatvédelmi és információbiztonsági kérdésekben

(2) Adatok kiadása az „5.” és „4.” biztonsági biztonsági osztályba sorolt rendszerekből a Rektor, illetve a Kancellár engedélyezésével lehetséges, kivétel ez alól az olyan eset képe, amikor az adatcserét, adatátadást – jogszabály felhatalmazása alapján – jogszabály vagy szerződés rögzíti. Utóbbi esetben a szerződésnek tartalmaznia kell az adatkezelésre vonatkozó szabályokat.

Az IBSZ felülvizsgálata, módosítása

26.§

(1) A szabályzat felülvizsgálatára az alábbiak szerin 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) Az IBSZ kapcsolatos észrevételeket, változtatási javaslatokat az ISZK igazgatójának címzett, az 1. számú mellékletben található változáskezelési lapon lehet benyújtani.

Záró rendelkezések

27.§

(1) Ezen Szabályzatot a Szenátus 173/2016. sz. határozatával fogadta el. A hatályba lépés napja 2016. június 27. A Szabályzat hatályba lépésével egyidejűleg a 180/2007. sz. Szenátusi határozattal elfogadott Informatikai Biztonsági Szabályzat hatályon kívül helyezésre kerül.

(2) A Miskolci Egyetem Informatikai Biztonsági Szabályzatát az Egyetem központi honlapján nyilvánosságra kell hozni.

Miskolc, 2016. június 27.

Prof. Dr. Torma András
rektor
a Szenátus elnöke

MISKOLCI EGYETEM 3. Rektora

Mellékletek

1. számú melléklet

IBSZ változáskezelési lap

Benyújtó neve:

Beosztása:

Szervezeti egysége:

e-mail:

telefon:

Benyújtás száma:

Aláírás:

A változtatni kívánt IBSZ bekezdés száma, megnevezése:

A változtatási javaslat rövid indoklása:

A javasolt új szövegrész:

ISZK tölti ki:
Beérkezés időpontja:

Átvevő:

Az igény vizsgálatával kapcsolatos megjegyzések:

Az igény elbírálása: Bekerül a dokumentumba a változás

Nem kerül be a dokumentumba a változás

Indoklás:

Aláírás:

2. számú melléklet

Felhasználói nyilatkozat

Alulírott, mint Miskolci Egyetem és annak szervezeti egységei (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 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.
- 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról
- 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, tűzvédelmi 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 előírásai.
- MeH ITB 12. ajánlása: az informatikai rendszerek fizikai, logikai és adminisztratív védelmi követelményeit és 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 Sístem Evaluation Criteria (Biztonságos Számítógépes Rendszerek érékelési 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 Miskolci Egyetemmel ……..-án megkötött …….. szerződés (a továbbiakban: a szerződés) teljesítése során a Miskolci Egyetemről (a továbbiakban: ME) a szerződéssel kapcsolatosan, azzal összefüggésben a ……. tudomására jutott információkat, adatokat, így különösen a személyes adatokat, valamint az ME tulajdonát, vagyonkezelését képező, vagy a tevékenységével, gazdálkodásával, működésével, pénzügyi és jogi helyzetével kapcsolatos információkat (amelyeket a szerződéskötés, vagy annak teljesítése érdekében az ME előtte felfed, illetőleg amelynek a szerződéssel összefüggésben váltak számára ismertté vagy egyébként hozzáférhetővé)

- üzleti titokként kezeli
- azt jogosulatlan személy részére nem szolgáltatja ki, illetve nem teszi egyéb módon hozzáférhetővé,
- 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
- 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 ME előzetes, írásbeli hozzájárulásának birtokában használhatja fel a szerződés teljesítésének érdekében kívül eső céllal összefüggésben. A jelen nyilatkozatban vállalt titoktartási kötelezettség nem vonatkozik az olyan információkra

- amely köztudomású,
- amelyet nem a szerződés vagy a jelen nyilatkozat megértésével hozunk nyilvánosságra,
- amely nyilvánosságra hozatali korlátozás nélkül a ……. birtokában volt már azelőtt, hogy a ME-től megkapta volna,
- amelyet a …….. olyan harmadik Féltől kapott, aki jogszerűen szerezte meg, és jogszerűen továbbította, vagy hozta létre azt, és akit nem köt titoktartási kötelezettség,
- amelyet a …… a ME bizalmas információjának felhasználása nélkül maga hozott létre, vagy
- 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 ME érdekében, illetve ha az információ nem került egyébként is nyilvánosságra.

Tudomással bírunk arról, hogy a jelen nyilatkozatban foglaltak megértését a ME súlyos szerződésszegésként tekinti.

A ……. vállalja, hogy a jelen nyilatkozatban meghatározott bármely információs 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 ME felhívására megfelelően igazolja.

Miskolc, ……

……

cégszerű aláírás

5. számú melléklet

Értelmező rendelkezések

Adatvédelem: az informatikai 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 hatása 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 rendelkezésre bocsátott informatikai infrastruktúrát (IT Rendszert) használja.

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

GI: ME Gazdasági Igazgatóság

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 architektúrája az ISO/OSI 7498-2 szabvány vonatkozik. Magyar megfelelője: MSZ OSI 7498-1.

ISZK: Informatikai Szolgáltató Központ

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 a melyet 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 hasonló tünete 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.

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

SLA: Service Level Agreement – Szolgáltatási szint megállapodás egy olyan írásos megállapodás, amely 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 változás az SLA-k változtatási rendjének megfelelően végezhető. AZ SLA-ra vonatkozó részletes szabályokat az Egyetem Informatikai Szabályzata tartalmazza.

Üzletmenet-folytonosság és katasztrófa-elhárítás tervezés: Az informatikai rendszer és a benne kezelt adatok, valamint a környezetüket képező 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 esetén. Angol nyelvű elnevezése: Business Continuilty Planning (rövidítése: BCP) és Disaster Recovery Planning (rövidítése: DRP).