INFORMATIKAI BIZTONSÁGI SZABÁLYZAT

(Jelen szabályzatot a Szenátus a 19/2022. (IV.27.) sz. határozatával fogadta el)

2022

Kiadás	Készítette	Ellenőrizte	Jóváhagyta
	Koczka Ferenc adatvédelmi tisztviselő, dr. Dargai-Huszti Ivett jogtanácsos	Rákosiné dr. Jakab Éva kabinetvezető	EKKE Szenátus 19/2022. (IV.27.) sz. határozatával valamint az Egri Főegyházmegye
Módosítás	Fejezet száma	Változás tárgya	Kiadás dátuma

Tartalom

1. Preambulum 3
2. Az IBSZ célja 3
3. Általános rendelkezések 4
4. Az IT rendszerek és adatok biztonsági besorolása 4
5. Információbiztonsági alapelvek 6
6. Az informatikai biztonság alapterületei 6
7. Az Egyetem biztonsági politikája 6
8. Az üzemeltető hatásköre 7
9. A felhasználók felelőssége 8
10. Az Informatikai Osztály feladatai és felelőssége 9
11. Az IBSZ-ben foglaltak megszegésének szankciói 9
12. Környezeti és fizikai biztonság 10
13. Fejlesztési és támogatási feladatok 11
14. Üzemeltetés menedzsment 12
15. Emberi erőforrások 15
16. Hozzáférés és jogosultságok szabályozása 16
17. Megfelelőség 17
18. Új információs rendszerek elfogadási eljárása 17
19. Működés folytonosságának biztosítása 18
20. Információbiztonsági események menedzsmentje 18
21. Az egyetemen kívülre történő adatátadás 18
22. Az IBSZ felülvizsgálata 18

1. Preambulum

1) Az informatikai rendszerek üzemeltetése során számos kockázati tényezővel és veszélyhelyzettel kell számolni, előtérbe helyezve azt a tényt, hogy ezeket a veszélyforrásokat teljes mértékben nem lehet megszüntetni. A kockázatok csökkentésére az Eszterházy Károly Katolikus Egyetem (a továbbiakban Egyetem) információs vagyonát kezelő felhasználóinak és a rendszer üzemeltetőinek egyaránt törekednie kell, a cél ezeknek az elfogadható mértékre történő leszorítása. A cél elérése érdekében az Egyetem a kockázati elemeket folyamatosan vizsgálja, és az adott helyzetnek megfelelően kezeli.
2) A szabályozás egyaránt lefedi az információk helytelen kezeléséből származó kár megelőzésére tett lépéseket, az informatikai események és incidensek kezelését, valamint egy incidens bekövetkezése esetén a kár minimalizálását, illetve mentesítését.
3) Az informatikai incidensek elkerülésének érdekében a cél a veszélyhelyzet elkerülése és annak kivédése, amit adminisztratív és technikai eszközök segítségével kívánunk elérni. A cél elérését informatikai védelmi eszközökkel, azok működési felügyeletével, és észlelő kontrollokkal biztosítjuk azért, hogy a káros hatást megelőzzük vagy minimalizáljuk. Az adminisztratív eszközök (szabályzások) leírják az adott helyzet esetén szükséges cselekvések sorozatát is.
4) Az informatikai rendszerek védelmére az arányosság elvének betartása mellett a legnagyobb mértékű technikai védelmet biztosítjuk. A humán oldalról érkező incidensek minimalizálására szabályzási és képzési lépéseket teszünk.

2. Az IBSZ célja

A jelen Informatikai Biztonsági Szabályzat (a továbbiakban IBSZ) célja, hogy az Egyetem működtetett informatikai rendszerekre vonatkozó biztonsági intézkedéseket szabályozza, meghatározza a számítástechnikai eszközök beszerzésének és használatának, az üzemeltetés, a fejlesztés és alkalmazás, valamint az adatkezelés folyamatának biztonsági szabályait, definiálja az informatikai szerepköröket, és előírja az egyes szereplők informatikai biztonságot érintő feladatait. Az IBSZ feladata, hogy a célok eléréséhez keretet adjon az informatikai rendszerekben és azon kívül kezelt adatok bizalmasságának, hitelességének és rendelkezésre állásának biztosítása érdekében. A szabályozás alapja az egyetem folyamatainak, adatainak és az azt kezelő rendszereknek biztonsági besorolása. Az IBSZ strukturális alapját az MSZ ISO/IEC 27001:2014-es szabvány képezi. Az IBSZ az alábbi fő feladatokat tűzi ki:

1) Az Egyetem informatikai rendszereinek biztonsági osztályba sorolása.
2) A titok- és adatvagyon védelmére vonatkozó előírások betartása.
3) A személyes adatok védelméhez fűződő jogok kellő védelme.
4) Az üzemeltetett számítástechnikai eszközök, hardverek, szoftverek, hálózatok stb. rendeltetésszerű használata és megfelelő üzemeltetése.
5) Az üzembiztonságot szolgáló műszaki fenntartási és karbantartási teendők elvégzése.
6) A számítógépes feldolgozások és az eredményadatok további hasznosítása során az illetéktelen hozzáférésből és felhasználásból eredő károk megelőzése, illetve minimális mértékűre való csökkentése.
7) Az adatállományok formai és tartalmi helyességének és épségének megőrzése.
8) Az alkalmazott szoftverek sértetlenségének, megbízható működésének biztosítása.
9) Az adatállományok biztonságos mentése.
10) A felhasznált és keletkezett írásos dokumentumok megfelelő kezelésének biztosítása.
11) Az Egyetem vezető beosztású, és az informatikai rendszerekkel összefüggő feladatokat irányító dolgozói számára meghatározza a felelősségi körükbe tartozó informatikai rendszerekkel kapcsolatos adatvagyonát, valamint az azt kezelő informatikai rendszer védelmével, biztonságával és megbízható működésével kapcsolatos feladatokat, definiálja az ehhez kapcsolódó felelősségi- és hatásköröket.
12) Az informatikai rendszerekkel kapcsolatos jogosultság és a hozzáférés rendszerének meghatározása.

13) A célok elérése érdekében az e szabályzatban foglaltaknak az egyes rendszerelemek teljes életciklusa alatt működnie kell – a megtervezéstől a működtetésükön át a felszámolásukig.

Az IBSZ-hez kapcsolódó egyéb dokumentumok:

1) Informatikai Biztonsági Politika.
2) Üzemeltetési szabályzatok.
3) Balesetvédelmi szabályzat.
4) Tűzvédelmi szabályzat.

3. Általános rendelkezések

1) Az IBSZ hatálya kiterjed az Egyetem összes dolgozójára, hallgatójára, és minden olyan személyre, aki az Egyetemmel olyan jogviszonyba kerül, mely során az egyetemi informatikai infrastruktúrát és adatvagyont, vagy annak valamilyen részét kezeli, vagy az Egyetem informatikai rendszerét használja.
2) Jelen szabályzat kiterjed minden olyan harmadik félre is, amely számára az Egyetem hozzáférést biztosít az adatvagyon részének vagy egészének kezelésére, illetve az egyetemi informatikai infrastruktúra használatára. A harmadik fél számára hozzáférés csak abban az esetben biztosítható, ha a felhasználni kívánt információs rendszer felelőse ahhoz írásban hozzájárul, az igénybe vevő a jelen szabályzatban foglaltak betartását elfogadja, illetve titoktartási nyilatkozatot tesz.

4. Az IT rendszerek és adatok biztonsági besorolása

1) Az Egyetemen működtetett rendszereket az alábbi öt biztonsági szint valamelyikébe kell besorolni. A besorolás alapja a rendszer és adatai által kiszolgált folyamatok kritikussága, az adatok értéke, a rendszer és adatainak kiesése, illetve elvesztése esetén keletkező kárérték. Ugyancsak a besorolás alapját jelenti az adatok érzékenysége, különös tekintettel a személyes és a különleges jellegükre.
2) Az 5. biztonsági osztályba sorolandó rendszerek és adatok olyan, az Egyetem feladatainak ellátása szempontjából kritikus adatok és rendszerek azok, amelyekre sérülésük vagy kiesésük esetén az alábbiak valamelyike fennáll:
    a. Igen nagy káresemény következhet be, mivel a keletkező kár nagysága elérheti az intézmény éves költségvetésének 15%-át.
    b. Emberi életek kerülhetnek veszélybe, vagy személyi sérülések nagy számban következhetnek be.
    c. Nagymennyiségű személyes vagy különleges adat kerülhet nyilvánosságra.
    d. A nemzeti adatvagyon körébe tartozó adatvagyon megsérülhet vagy illetéktelen kezekbe kerülhet.
    e. Az ország vagy a társadalom működőképességének fenntartását biztosító létfontosságú információs rendszer rendelkezésre állása nem biztosított.
    f. Súlyos bizalomvesztés jöhet létre az Egyetemmel szemben, vagy a felsővezetésben felelősségre vonást kell alkalmazni.
    g. Az Egyetem ügymenete szempontjából nagyértékű, nem nyilvános információ kerülhet illetéktelen felhasználásra vagy nyilvánosságra.

    Az Egyetem esetében ezek a rendszerek:
    a) Tanulmányi Rendszer.
    b) Gazdálkodási rendszer.

    A gazdálkodási rendszer üzemeltetése azonban külső szolgáltatás keretében történik, így az arra vonatkozó követelmények csak részben teljesíthetők a helyi informatikai környezetben.

3) A 4-es biztonsági osztályba sorolandó rendszerek és adatok olyan, az Egyetem feladatainak ellátása szempontjából kritikus adatok és rendszerek, amelyek sérülése vagy kiesése esetén az alábbiak valamelyike fennáll:
    a. Nagymennyiségű személyes vagy különleges adat sérülhet vagy kerülhet nyilvánosságra.
    b. Különlegesen érzékeny folyamatokat kezelő információs rendszer vagy különlegesen érzékeny folyamathoz kapcsolódó adat jelentős mértékben sérülhet.
    c. Megnőhet a személyi sérülések veszélye.
    d. Az Egyetem ügymenete szempontjából nagyértékű, nem nyilvános információ kerülhet illetéktelen felhasználásra vagy nyilvánosságra.
    e. Bizalomvesztés következik be, vagy az adott szolgáltatási terület vezetésében személyi felelősségre vonást kell alkalmazni.
    f. A közvetlen és a közvetett kár eléri az Egyetem költségvetésének 10%-át.

    Az Egyetem esetében ezek az alábbi rendszerek:
    a. Iktatási rendszer.
    b. Modulo.
    c. Informatikai hálózat.
    d. Telefonközpont és kapcsolódó hálózat.
    e. Központi levelező kiszolgálók.
    f. Központi tárhely kiszolgálók.
    g. Központi címtár.

4) A 3-as biztonsági osztályba sorolandó rendszerek és adatok olyan, az Egyetem feladatainak ellátása szempontjából kritikus adatok és rendszerek azok, amelyekre sérülésük vagy kiesésük esetén az alábbiak valamelyike fennáll:
    a. Személyes vagy különleges adat sérülhet vagy kerülhet nyilvánosságra.
    b. Az Egyetem ügymenete szempontjából érzékeny folyamat alapjául szolgáló rendszer vagy adat sérülhet.
    c. Bizalomvesztés állhat elő az adott rendszerrel, ennek következtében az azt működtető szervezeti egységgel szemben.
    d. A szervezeti szabályokban foglalt kötelezettségek ellátása veszélybe kerülhet.
    e. A közvetlen és a közvetett kár eléri az Egyetem költségvetésének 5%-át.

    Az Egyetem esetében ezek az alábbi rendszerek:
    a. Szerver számítógépek.
    b. Kutatói rendszerek.
    c. Technológiai (middleware) rendszerek.
    d. EKERNEL keretrendszer
    e. Katolikus tananyagok Portálja.
    f. Pegazus.

5) A 2-es biztonsági osztályba sorolandó rendszerek és adatok olyan, az Egyetem feladatainak ellátása szempontjából kritikus adatok és rendszerek azok, amelyekre sérülésük vagy kiesésük esetén az alábbiak valamelyike fennáll:
    a. Csak csekély mennyiségű személyes adat sérülése következhet be.
    b. Csak csekély értékű adat, vagy kis fontosságú információs rendszer sérülhet meg vagy eshet ki.
    c. A keletkezett anyagi kár legfeljebb az éves költségvetés 1%-át érheti el.

    Az Egyetem esetében ezek az alábbi rendszerek:
    a. Hallgatói laborok, géptermek.

6) 1-es biztonsági osztályba kell sorolni azokat az informatikai rendszereket, amelyek sérülésekor csak jelentéktelen káresemény következik be. Az 1-es biztonsági osztályba sorolt rendszerek nem

kezelhetnek számottevő mennyiségű személyes adatot. A rendszer sérülésekor nem következhet be bizalomvesztés, a probléma az Egyetemen belül marad és saját hatáskörben meg is oldható. Az esetleg bekövetkező anyagi kár jelentéktelen.

5. Információbiztonsági alapelvek

1) Az IBSZ szempontjából biztonságos állapot az, amikor az intézményi adatvagyon, az azt tároló, és a folyamatokat kiszolgáló rendszerek bizalmassága, sértetlensége és rendelkezésre állása zárt, teljes körű és a biztonsági besorolásuknak megfelelő szinttel arányos és folyamatos.
2) A 3-as, 4-es és 5-ös biztonsági osztályba sorolt rendszerek által kezelt adatok és az arra alapuló rendszerek védelmét a bizalmasság, sértetlenség és a rendelkezésre állás szempontjából úgy kell megvalósítani, hogy az informatikai rendszer és környezetének védelme folyamatos, teljes körű, zárt és kockázatokkal arányos legyen, és megvalósuljon a zárt szabályozási ciklus az alábbiak szerint:
    a. A védelem *folyamatos*, ha a változó környezeti feltételek mellett is megszakítás nélkül látja el a funkcióit. A folyamatos védelem megvalósítását az informatikai rendszer teljes életciklusa alatt, a beszerzéstől az üzemelésből történő kivonásig biztosítani kell.
    b. A védelem *teljes körű* abban az esetben, ha a védelmi intézkedések az informatikai rendszer összes elemére kiterjednek, beleértve az alkalmazott hálózati modellt, és bármely két végpont között működő eszközt. A védelmet a fizikai, logikai és adminisztratív területek mindegyikén érvényesíteni kell az alábbiak szerint:
        i. Minden információbiztonsági rendszerelemre vagy csoportra, ideértve a központi, köztes és végponti berendezéseket.
        ii. Az informatikai rendszer infrastrukturális környezetére.
        iii. A rendszer működésében résztvevő hardver elemekre.
        iv. Az operációs rendszerekre és a folyamatokat kiszolgáló rendszerekre.
        v. A kommunikációs rendszerre, kiemelten a számítógépes hálózati kapcsolatokra.
        vi. A rendszert és adatait tároló adathordozókra.
        vii. A rendszerhez kapcsolódó dokumentumokra.
        viii. A rendszer üzemeltetőire.
        ix. A rendszer adataihoz hozzáféréssel rendelkező adatfeldolgozókra.
        x. A rendszer működtetésében résztvevő külső partnerekre.
    c. A védelem *zárt*, ha tervezése során minden szóba jöhető fenyegetést figyelembe vettek, és a védelem ezek mindegyikével szemben megvalósul.
    d. A védelem *kockázatarányos* abban az esetben, ha hosszú időtartamra vetítve a védelem költségei arányosak a potenciális kárértékkel úgy, hogy a védelemi intézkedések eredményeként a kockázatok elviselhető mértékűre csökkennek. A cél az elviselhető kockázatvállalás mellett a minimális költségráfordítás.

6. Az informatikai biztonság alapterületei

1) Az információvédelem, amely az Egyetem adatvagyonának védelmét jelenti a *bizalmasság*, és a *sértetlenség* területén függetlenül attól, hogy az adatvagyon elemeit elektronikus, vagy más formában tárolják.
2) A megbízható működés, amely az Egyetem információs rendszereinek rendelkezésre állását és az elvárt funkcionalitás képességének fennállását jelenti.

7. Az Egyetem biztonsági politikája

1) Az Egyetem biztonsági politikája minden üzemeltető és felhasználó számára meghatározza azokat az elveket és szabályokat, amelyek az intézményi adatvagyon, valamint az azt kezelő rendszerek bizalmasságának, sértetlenségének és rendelkezésre állásának kialakítása és fenntartása érdekében szükségesek.

2) Az Egyetem biztonsági politikájának elsődleges célja az adatvagyon és az információs rendszer elemeinek védelmén keresztül az Egyetem működési folyamatainak fenntartása. Az Egyetem ennek szellemében minden, az adatvagyon kezelésében részt vevő munkatársától elvárja, hogy annak szakszerű kezelését a tőle elvárható mértékben valósítsa meg. Az adatvagyon bármely elemének veszélyeztetése az azt kezelő kizárását eredményezheti az adott szakrendszerből vagy annak mértékétől függően a teljes informatikai rendszerből.
3) Minden területen törekedni kell az arányossági elv betartása mellett a kockázatok minimalizálására.
4) Az adatvagyon minden területére meg kell határozni a felelősségi köröket.
5) Az információbiztonsággal kapcsolatos felelősségi köröket úgy kell meghatározni, hogy azok az egyes üzemeltetői és adatkezelői feladatok ellátásához legyenek kötve.
6) Törekedni kell a jogszabályi kötelezettségek betartására, különös tekintettel a GDPR-ra, a 2012 évi C. törvény 43. fejezetére és az 2011 évi CXII. törvényre.
7) Az információbiztonsági ismeretek átadása valamint, az ahhoz szükséges erőforrások rendelkezésre állásának biztosítása az Informatikai Osztály (a továbbiakban IO) vezetőjének feladata. Az adott szervezeti egység információbiztonsági kultúrájának az IBSZ-ben foglaltak szerinti betartása, valamint annak fenntartása az adott szervezeti egység vezetőjének feladata. A vezetők az elkötelezettségüket személyes példájukkal és felelősségvállalásukkal demonstrálják.
8) Az információbiztonsággal kapcsolatos felelősségi kör a fentiek alapján megoszlik az IO, az egyes szervezeti egységek vezetői és a felhasználók között az alábbi általános elvek szerint.

8. Az üzemeltető hatásköre

1) Minden, az Egyetemen működtetett informatikai rendszer esetében az IBSZ szerinti működtetés felelőssége az alábbiak valamelyike:
    a. A rendszer informatikai kiszolgáló elemeinek, ideértve a szerverek, munkaállomások, operációs rendszerek, kliens szoftverek működtetését, az elektronikus rendszerekben tárolt adatvagyon technikai értelemben vett védelmét, és az azt kiszolgáló rendszerek üzemeltetését az IO munkatársai látják el.
    b. Indokolt esetben, pl. kutatási feladatokat támogató szerver, hálózati eszköz vagy weblap üzemeltetésekor a fenti feladatot az Egyetem más munkatársa is elvégezheti, amennyiben rendelkezik az adott rendszer működtetéséhez szükséges üzemeltetési, biztonsági, és adatbiztonsági ismeretekkel, valamint az IO vezetője írásban engedélyezte azt. Az üzemeltetőre ugyanazok a szabályok vonatkoznak, mint az IO munkatársaira, de az adatvédelmi incidensek felelőssége az IO-től az adott szervezeti egység vezetőjéhez kerül. Az IO az adott rendszert érintő hálózati védelmét továbbra is az IBSZ-ben foglaltak szerint látja el. Publikus szolgáltatást ilyen informatikai rendszer csak kifejezetten indokolt esetben, az informatikai védelem magas szintű megvalósítása mellett nyújthat. Amennyiben az üzemeltetést végző infrastruktúrán adatvédelmi incidens történik, az IO vezetője kezdeményezi az üzemeltetési engedély visszavonását.
    c. A rendszer működtetését az Egyetemmel vállalkozási vagy megbízási szerződésben álló, az adott rendszer működtetésével megbízott személy vagy szervezet is végezheti. Ebben az esetben az IBSZ hatálya rájuk, és alvállalkozóikra is kiterjed.
2) Minden, az Egyetemen működtetett informatikai rendszer esetében *az abban tárolt adatok kezelésének felelőse az adott egység vezetője*. Az ő feladata az adatok hozzáférési körének, valamint a rendszer által megvalósított folyamatok személyi körének meghatározása, annak rendszeres áttekintése, és a változások átvezetése az adott rendszerben. A feladatot a vezető a szervezeti egység általa kijelölt munkatársa számára delegálhatja. Az 5-ös, 4-es és 3-as biztonsági osztályba sorolt rendszerek esetében a hozzáférések beállítását a megfelelő informatikai ismeretekkel rendelkező vezető a jogkörök birtokában a vezető személyesen, vagy az Informatikai Osztály erre kijelölt munkatársa számára adott írásos vagy e-mailben történő utasítás alapján végzi. A megbízásnak tartalmaznia kell a hozzáférésre jogosított munkatárs nevét, a hozzáférési jogokat vagy szerepköröket, a hozzáférés időtartamát és a jogosultságok kezelésével kapcsolatos elvek leírását. Az Egyetemmel jogviszonyban nem álló személy esetében hozzáférés csak a kancellár engedélyével lehetséges abban az esetben, ha annak megadása elkerülhetetlen.
3) A hozzáférési kör szabályozása az egységvezető feladata abban az esetben is, ha az adatokat nem elektronikus információs rendszerben tárolják.

4) Abban az esetben, ha az adott informatikai rendszer üzemeltetését külső személy vagy szervezet végzi, a szervezeti egység vezetője felelős azért, hogy vele szemben érvényesítse az IBSZ követelményeit. Ennek érdekében a szolgáltatási szerződésekben szerepeltetni kell a következőket:
    a. A külső személy vagy szervezet felelősségvállalását az szerződés tárgyát képező informatikai rendszereire vonatkozóan, ideértve a mindenkor hatályos törvényi szabályzások, és az Egyetem belső szabályzásainak betartását.
    b. A szolgáltató által vállalt szolgáltatási szint megállapodást (SLA). Ebben ki kell térni a pontos vállalási körre, annak minőségi kritériumaira és azok mérésére és esetleges szankcióira. A szolgáltatói szerződéseknek minden esetben ki kell térnie az információbiztonsági, titoktartási és adatbiztonsági kérdésekre is.

   A szolgáltatási szerződésben foglaltak betartásának ellenőrzése, valamint a szükséges intézkedések foganatosítása az adott szakrendszer vezetőjének feladata és felelőssége.

9. A felhasználók felelőssége

1) Az Egyetem informatikai rendszerének minden felhasználója köteles az IBSZ-ben foglaltak szerint használni az informatikai rendszert.
2) Minden személy és program csak a számára meghatározott jogosultságokkal léphet be az informatikai szolgáltatásokba, és ezen jogok mentén használhatja a rendszert. A jogosultság változását az adott szakrendszer vezetőjénél kell kezdeményezni, aki jelen IBSZ-ben szabályozott módon gondoskodik a hozzáférési engedélyek beállításáról.
3) Tilos a személyre szóló jogosultsági hozzáférések átadása más személy részére, és tilos egy személyes hozzáférést több személyhez hozzárendelni.
4) Amennyiben egy szolgáltatás kezelője, illetve felhasználója megállapítja, hogy valamely informatikai rendszerben a számára szükségesnél magasabb jogosultsági szint érhető el számára, ennek tényét jeleznie kell a szervezeti egységének vezetője felé, az IO üzemeltetési körébe tartozó rendszer esetén az IO vezetője felé. A magasabb jogkör meglétének okát ki kell vizsgálni.
5) A szolgáltatás kezelője, illetve felhasználója teljes felelősséggel tartozik az adott szolgáltatás igénybevételekor vállalt kötelezettségei betartásáért.
6) Az Egyetem adatvagyona, függetlenül attól, hogy azt információs rendszerben vagy más módon tárolja, az Egyetem tulajdona. Az információs rendszereket minden munkatárs köteles csak a munkakörének megfelelően, az adott rendszer kezelési utasításainak és a kapcsolódó utasításoknak megfelelően eljárni.
7) Az 5-ös, 4-es és 3-as biztonsági osztályba sorolt adatok, illetve az ebbe az osztályba sorolt rendszerekből származó adatok eltérő jogszabály hiányában kizárólag az Egyetemi infrastruktúrán tárolhatók. Ezek az adatok hordozható számítógépeken, adathordozókon történő rögzítésükkor csak titkosítva tárolhatók azért, hogy esetleges elvesztésük esetén az adatokhoz való hozzáférés elkerülhető legyen.
8) Külső adattárolási szolgáltatások (Google Drive, Dropbox és alternatíváik) csak különösen indokolt esetben, és csak publikus adatok tárolására vehetők igénybe, helyettük az Egyetem saját felhőszolgáltatását kell használni. Nem vehetők igénybe olyan külső adattárolási szolgáltatók, amelyek a náluk elhelyezett adatokat saját céljukra felhasználhatják, ennek ellenőrzése a tárolást végző személy feladata. Egy külső adattárolási szolgáltatónál elhelyezett, az Egyetem tulajdonát képező adatot érintő incidens megvalósulása esetén a felelősség a kihelyezést elrendelő vezetőt, illetve az azt elvégző munkatársat terheli.
9) Az információs rendszerek kezelői csak munkaköri feladatuk ellátásához, csak annak szükséges mértékéig, és a titoktartási kötelezettségük betartásával kezelhetnek adatokat.
10) Az informatikai rendszer erőforrásaival minden felhasználónak takarékoskodnia kell, különösen ideértve az e-mailek tárolására szolgáló tárhelyet.
11) Az IBSZ előírásait abban az esetben is be kell tartani, amikor a felhasználók az Egyetemet valamely szakmai szervezetben képviselik.
12) Az Egyetem bármely informatikai rendszerének felhasználója, vagy az adatvagyon valamely részének kezelője számára 2022. szeptember 1-jétől kötelező információbiztonsági ismeretekkel rendelkeznie, a kurzus tananyagának biztosítása az IO feladata. Az újonnan belépő munkatársak számára a

munkafolyamat megkezdése előtt, de legkésőbb az első munkahéten, az egyéb kötelező oktatásokkal (tűzvédelmi, balesetvédelmi stb.) egyidőben meg kell történnie.

13) Amennyiben a felhasználó a magatartásával veszélyezteti az informatikai adatvagyont, az informatikai infrastruktúrát és az ezeken alapuló működési folyamatokat, az üzemeltető intézkedhet a szolgáltatásból történő kizárásról és jogainak visszavonásáról.
14) Az IBSZ előírásainak szándékos megsértése esetén a vonatkozó jogszabályoknak és az Egyetem előírásainak megfelelően szankcionálható.

10. Az Informatikai Osztály feladatai és felelőssége

1) Az Egyetem információbiztonsági vezetője az Informatikai Osztály vezetője.
2) Az Egyetem információbiztonsági szabályzását, az Információbiztonsági Szabályzatának készítését, felülvizsgálatát és aktualizálását az IO vezetője végzi.
3) Az IO ellátja az IBSZ-ben foglaltak betartásának ellenőrzését és incidens esetén lépéseket tesz annak kivizsgálására, az azt kiváltó okok megszüntetésére, a további incidensek bekövetkezésének megakadályozására, és a normál működés helyreállítására.
4) Az IO fogja össze, koordinálja és üzemelteti minden, az Egyetem és szervezetei tulajdonában levő informatikai eszközt és szolgáltatást.
5) Az IO a szolgáltatás ellátásához ticketing rendszert használ, a bejelentéseket ebben végződteti, és a feladatok elvégzését ebben tartja nyilván. A ticketing rendszert a belső feladatok ellátása során is alkalmazza.
6) Az IO koordinálja az Egyetem szoftver beszerzéseit és végzi azok nyilvántartását. A vagyongazdálkodási csoporttal együttműködve az IO feladata a szoftvervagyon nyilvántartása és az azzal kapcsolatos optimális működtetési környezet kialakítása. A szoftvergazdálkodás kiemelkedő szempontja a költségtakarékos működtetés és a legnagyobb hatásfokkal történő kihasználtság elérése.
7) Az IO engedélyezi az új informatikai elemek üzembe állítását. Ennek megadása során az IO megvizsgálja az adott elem összeegyeztethetőségét a meglevő informatikai rendszerekkel, különös tekintettel az információbiztonsági megfelelőségre. Amennyiben az adott rendszerben ilyen irányú hiányosságot tár fel, az üzembe helyezést az IO vezetője elutasítja, ebben az esetben az eszközt tilos üzembe helyezni.
8) Az IO kérésre szakmai segítséget nyújt az adott szolgáltatásért felelős szervezeti egység kijelölt munkatársa számára a szervezeti egység által megkötni kívánt szerződések informatikai tartalmának és paramétereinek kialakításában.
9) Az informatikai rendszerek IBSZ szerinti megfelelőségének vizsgálatát, az ezekkel kapcsolatos tanácsadást az IO vezetője, illetve az általa kijelölt munkatársak végzik.
10) Az IO vezetője felelős a kapcsolattartásért az IBSZ-hez kötődő szervezetekkel (pl. KIFÜ, HUNGARNET Egyesület). A tagsági és a kapcsolattartási kérdésekben az Egyetem rektora és kancellárja dönt az IO vezetőjének javaslata alapján az Egyetem érdekeinek figyelembe vételével.

11. Az IBSZ-ben foglaltak megszegésének szankciói

1) Amennyiben az IBSZ az adott folyamat felelőseként az adott szervezeti egységet határozza meg, az IBSZ-ben foglaltak betartásáért az adott szervezeti egység vezetője a felelős, és a keletkezett kárért elsősorban a szolgáltatást végző egység vezetője köteles helytállni.
2) A felhasználókat a szabályzatban foglaltak alapján az alábbi szankciók sújthatják:
    a. A jogszegés azonnali megakadályozásának módjáról az IO vezetője dönt. A további eljárás, melynek eredménye a szolgáltatás részleges felfüggesztése vagy az abból történő kizárás, az IO vezetőjének javaslata alapján a rektor dönt.
    b. A felelősség megállapítása és az okozott kár megtérítése.
3) A szolgáltatásokat igénybe vevők szankcionálása csak abban az esetben történhet meg, ha az adott rendszer üzemeltetője dokumentálja a szankció elrendelését szükségessé tevő eseményt vagy incidenst, vagy az IO észlelete azt.
4) Az Egyetemmel polgári jogi jogviszonyban állók esetén a felelősségi és a kártérítési kérdésekben a polgári jog szabályai alapján kell eljárni.

12. Környezeti és fizikai biztonság

1) Fizikai biztonsági határvédelem. Az 5-ös biztonsági osztályba sorolt rendszerek kritikus komponensei, különösen a szerverek, tároló alrendszerek, routerek és kábelrendezők csak az erre a célra külön kialakított, megfelelő biztonsági paraméterekkel rendelkező helyiségekben működtethetők. A helyiségeket magas biztonságú zárral vagy elektronikus beléptető rendszerrel, tűzvédelemmel kell védeni. Beléptető rendszer alkalmazása esetén a belépések naplózására képes rendszert kell kialakítani.
2) Az 5-ös biztonsági osztályba tartozó rendszerek komponenseit tartalmazó helyiségekbe belépési jogosultságot az IO vezetője adhat saját dolgozók vagy szerződéses partnerek számára. A belépési jogosultság nem ruházható át más személyre. Jogosulatlan személy belépéséért a felelősség a hozzáférést átadó személyt terheli.
3) Az intézmény informatikai rendszerelemeiről csak az IO hozzájárulásával adható ki információ. Különösen tiltott az informatikai rendszerről bármilyen információ közzététele nyilvános, illetve közösségi oldalalakon.
4) Az irodák, szobák és egyéb létesítmények fizikai biztonsága.
    a. Az Egyetem minden területén elvárt a „tiszta asztal, tiszta tábla, tiszta képernyő” elvének betartása. Ennek értelmében minden számítógép esetében gondoskodni kell a számítógép zárolásáról abban az esetben, ha a kezelője nem tudja a gépet a felügyelete alatt tartani. A használt operációs rendszerekben lehetőség szerint be kell kapcsolni az automatikus zárolási funkciót. Jelszóvédelem nélkül csak a nyilvános elérésű számítógépeket szabad működtetni. Iratokat csak a szükséges ideig szabad látható helyen hagyni. A nyomtató- másoló berendezésekben nem szabad iratokat hagyni. A munka végeztével, amennyiben a számítógépen egyéb munkához kötődő tevékenység nem folyik, ki kell kapcsolni, és minden iratot zárható irodabútorokban kell tárolni.
    b. Az informatikai rendszerek működtetéséhez szükséges egyéb munkaterületek használatának módja megegyezik az általános védelmi területek használati módjával. Különleges vagy védett adatot tartalmazó informatikai eszközöket, adathordozókat csak az IO munkaszobáiban, illetve beléptető rendszerrel védett helyiségekben helyezhetők el.
    c. Az informatikai célú helyiségek kialakításáról és átalakításáról az informatikai vezető dönt.

5) Külső környezeti károk elleni védelem.
    a. Az 5. biztonsági osztályú informatikai rendszerelemek kritikus fizikai komponensei csak a hatályos jogszabályozásnak megfelelő tűz- és villámvédelmi rendszerrel ellátott helyiségekben üzemeltethetők. Talajszinten, vagy az alatt működő informatikai helyiségek, irattárak esetében az ár- és belvízvédelmi szempontoknak is meg kell felelni.
    b. Egyedi esetekben a szolgáltatásért felelős szervezet vezetője egyéb előírásokat is tehet.
    c. A tűzvédelmi rendelkezéseknek megfelelően az erősáramú ellátó rendszereknek tartalmazniuk kell olyan kapcsolót, amely tűz esetén lehetővé teszi a biztonságos oltás végzését.
    d. Minden helyiség esetében biztosítani kell azt a hűtési kapacitást, amellyel az ott termelt felesleges hőmennyiség elvezetése megoldható. Az 5-ös biztonsági osztályba sorolt rendszerek komponenseit tartalmazó helyiségekben redundáns működésű hűtőberendezéseket kell alkalmazni.
    e. Minden helyiség esetén biztosítani kell azt az erősáramú ellátó kapacitást, amellyel az ott működő informatikai eszközök elektromos betáplálása túlterhelésmentesen elvégezhető. Az 5-ös biztonsági osztályú rendszerek komponenseit lehetőség szerint kettős betáplálással kell ellátni. Az erősáramú tápellátási rendszernek biztosítania kell az egyes részrendszerek áramellátásának szeparatív kapcsolhatóságát.
6) Munkavégzés. Az 5-ös biztonsági osztályú rendszerek komponenseit tartalmazó helyiségekben minden, nem az IO kijelölt munkatársai által folytatott munkavégzés, ami az informatikai rendszereket, vagy azok működését veszélyezteti, csak előzetes egyeztetés után szabad elkezdeni. Az egyeztetést a munkát ellátó harmadik fél, és az IO vezetője, vagy megbízottja végzi. A helyiség gépészeti elemeit veszélyeztető munkálatok csak az azt üzemeltető féllel történő előzetes egyeztetés és jóváhagyás után végezhetők. A szolgáltatás kiesésével járó tervezett munkavégzésekről az Egyetem minden érintett munkatársát legalább 2 nappal korábban értesíteni kell.

7) Az 5-ös biztonsági osztályú rendszerek komponenseit tartalmazó helyiségekben mindenfajta szállítási tevékenység csak egy belépésre jogosult egyetemi munkatárs felügyelete mellett alkalmazható.
8) Minden, a géptermekbe, illetve kábelrendezőkbe kerülő új rendszerelem elhelyezését előzetesen az informatikai vezetőnek jóvá kell hagynia. A jóváhagyás elutasítható abban az esetben ha a helyiség nem rendelkezik a szükséges szabad hellyel, tápellátási vagy hűtési kapacitással.
9) Harmadik fél informatikai berendezéseinek elhelyezése esetén az Egyetem annak tulajdonosára hárithatja annak elektromos fogyasztásának, hűtésének és tárolásának költségeit.
10) Az Egyetem épületeiben és azon kívül elhelyezett informatikai kábelezési területeket, ideértve a kábelcsatornákat, alagutakat az IO munkatársai a Műszaki Osztállyal együttműködésben felügyelik. Ezért azokban munkát végezni, a megközelítésüket korlátozni csak az IO és a Műszaki Osztály vezetőjének jóváhagyásával lehet.
11) Informatikai eszközök karbantartása.
    a. Minden informatikai komponens üzemeltetője köteles felmérni annak karbantartási igényét, meghatározni annak karbantartási ciklusát és az előírt időben betartani azt.
    b. A karbantartások során a felmerült sérülékenységeket ki kell küszöbölni, a karbantartásokat úgy kell elvégezni, hogy annak során ne merüljenek fel újabb sérülékenységek. A karbantartások lebonyolításáért az adott eszköz üzemeltetője a felelős.
12) Az Egyetem telephelyein kívül használt eszközökkel kapcsolatos szabályok.
    a. Az Egyetem telephelyeiről informatikai eszközt kivinni csak az adott szervezeti egység vezetőjének írásos engedélyével lehet. Az eszközök mozgatását átadás-átvételi dokumentummal, vagy szállítólevéllel kell kísérni. E szabály alól kivételt képeznek az IO munkaköri feladataikat ellátó munkatársai.
    b. A kivitel során vagy annak következményeként bekövetkező károkért, különös tekintettel az adatvagyonban, adatbiztonságban keletkezettekre, a kivitelt végző személy a felelős, amennyiben a kár számára felróható okból keletkezett. Az 5-ös, 4-es és 3-as biztonsági osztályú intézményi adatokat amennyiben az elkerülhető, nem szabad lemásolni, hanem az adott szakrendszert kell használni. Amennyiben az adatok másolása elkerülhetetlen, azokat kizárólag titkosított formában szabad az intézményből kivinni. Az adatok kivitelét az adott szakrendszer üzemeltetőjének engedélyeznie kell.
13) A már nem használt vagy meghibásodott adathordozók adattartalmát oly módon kell megsemmisíteni, hogy a tartalom ne legyen helyreállítható. Amennyiben az eszköz meghibásodott, az adathordozót az IO munkatársai részére kell átadni, hogy a szakszerű megsemmisítését elvégezhessék.
14) A papír alapú információk kifürkészésének elkerülésére a szükségtelenné vált iratok megsemmisítését úgy kell elvégezni, hogy azok tartalma illetéktelenek számára ne legyen megismerhető, lehetőség szerint iratmegsemmisítő gépet kell használni. Különösen tilos ezeket megsemmisítés nélkül hulladéktárolókba helyezni.
15) Az informatikai eszközöket az IO munkatársai közreműködésével kell selejtezni. Az eljárás során megállapítást nyer a selejtezés indokoltsága, és szükséges esetben az adattartalom szakszerű eltávolítása. Az 5-ös, 4-es és 3-as biztonsági osztályú rendszerek adathordozóit a selejtezés után fizikailag meg kell semmisíteni. A folyamat felelőse az adott szervezeti egység vezetője, és az IO vezetője.

13. Fejlesztési és támogatási feladatok

1) A 4-es és az 5-ös biztonsági szintű fejlesztési feladatokat csak az eredeti rendszertől elkülönülten szabad végezni.
2) Amennyiben a fejlesztési feladatok ellátásához elengedhetetlen a védett adatokhoz történő hozzáférés, a fejlesztési rendszert az eredetivel megegyező biztonsági szintűnek kell minősíteni, és a hozzáférési jogosultságok nem haladhatják meg az eredeti rendszerben életben levőket.
3) Egyetemi fejlesztésű, vagy ajándékba kapott szoftver csak funkcionális teszt után állítható üzembe. A tesznek minden, az SLA-ban meghatározott paraméterre és funkcióra ki kell terjednie.
4) Minden, a szolgáltatási felületen vagy funkciókészletében megváltozott szoftver esetében a tesztelési eljárást újra el kell végezni. A tesztelési kötelezettség nem csak az alkalmazások, hanem az azt futtató környezetek (webszerverek, adatbáziskezelők stb.) esetében is fennáll, de csak a használt funkciókra kell kiterjednie. A tesztek eredményét jegyzőkönyvben kell rögzíteni.

14. Üzemeltetés menedzsment

1) Új informatikai rendszer üzembe helyezése.
    a. Egy szervezeti egység szolgáltatási igényének az IO csak abban az esetben tesz eleget, amennyiben az abban foglaltak megfelelnek az IBSZ-nek. Az IO munkatársa a szolgáltatási igényt vagy saját szolgáltatásaival, vagy az igénylő szervezeti egység vezetőjével történt egyeztetés után az igénylő által kívánt szoftverrel oldja meg.
    b. Amennyiben egy szervezeti egység új szoftver üzembe helyezését tervezi, annak biztonsági besorolását már a tervezési fázisban el kell végezni, és az üzemeltetés szabályait ennek megfelelően kell kialakítani.
    c. Amennyiben egy szervezeti egység új szoftvert kíván üzembe helyezni az Egyetem infrastruktúráján, a szoftvernek meg kell felelnie az IBSZ követelményeinek és a jogszabályi elvárásoknak, különös tekintettel a GDPR-ra. A megfelelőségről a szoftver fejlesztőjének kell nyilatkoznia, amelyet az IO munkatársa ellenőriz. Az Egyetem a megfelelőség hiányából adódó esetleges kárt a szoftver eladója felé hárítja át.
2) Kriptográfiai alapelvek
    a. Az informatikai rendszer minden pontján, ahol az a kockázattal arányosan megoldható, kriptográfiai megoldásokat kell alkalmazni.
    b. A kriptográfiai megoldások nem hagyhatók el az egyes rendszerekbe történő bejelentkezés, és az adatok forgalmazását végző csatornák esetén.
    c. Az információs rendszerek nem tartalmazhatnak kis erőforrás igényű eljárással dekódolható jelszavakat. Ilyen kódolású rendszer nem helyezhető üzembe, a meglevő rendszerek kódolási mechanizmusának cseréjét az IO magas prioritású feladatként kell, hogy kezelje.
3) Jogkövető magatartás
    a. Tilos az Egyetem tulajdonát képező bármely informatikai eszköz vagy szolgáltatás jogsértő tevékenység során történő felhasználása, ideértve a jogszerűtlen szoftver használatot, különösen az azok terjesztésében történő közreműködést.
4) Kártékony szoftverek.
    a. Azon rendszerek esetében, amelyekben kártékony kódok előfordulhatnak, a detektálásukra és elhárításukra szolgáló szoftvert kell telepíteni. A szoftver pontos típusát az Egyetem határozza meg, ettől tilos eltérni. Különösen tilos bármilyen, a védelmi szoftvert nem tartalmazó informatikai berendezést az intézményi hálózathoz kapcsolni.
    b. A felhasználó csak abban az esetben használhatja saját tulajdonú eszközét és adattároló berendezéseit az Egyetem infrastruktúráján ha arra a jelen IBSZ szabályzásait érvényesíti és a kezelésével kapcsolatos szabályzást betartja. A saját tulajdonú adathordozó egyetemi informatikai rendszerhez történő csatlakoztatása következtében keletkezett kárért a csatlakoztatást végző személy a felelős.
5) Frissítések.
    a. Az egyetem minden információs rendszerelemére telepíteni kell az operációs rendszer és az általuk működtetett szakrendszerek frissítéseit.
    b. Az 5-ös, 4-es és 3-as biztonsági osztályba sorolt információs rendszerek frissítését megelőzően tesztelni kell a rendszer frissítés utáni funkcionalitását, és csak abban az esetben szabad a frissítést telepíteni, amennyiben a tesztek sikeresen lefutottak, vagy a korábbi állapot rövid időn belül helyreállítható.
    c. A publikált sérülékenységek elleni védelem megvalósítása az adott rendszer üzemeltetését végzők feladata és felelőssége. A bizalmasságot, hitelességet vagy rendelkezésre állást közvetlenül fenyegető publikált sérülékenységekkel szembeni védekező intézkedés a publikációt követően a lehető legrövidebb időn belül hajtandó végre. Ilyen esetben a 12.6 pontban meghatározott 2 nappal korábbi értesítési kötelezettségtől el kell tekinteni.
6) Az Egyetem hordozható számítógépet biztosíthat azon munkatársai számára, akik esetében a ellátásához ez szükséges.
7) Egyetemi tulajdonú hordozható számítógépek esetén az adathordozók titkosítását kötelező bekapcsolni.
8) Az személyes használatra átadott, az Egyetem tulajdonát képező számítógép indokolt esetben, de kizárólag az átvevő által magáncélra is igénybe vehető. Magáncélú használat esetén a magánjellegű

adatokat a gépen tárolt egyéb adatoktól jól elkülönülten, egy kifejezetten erre a célra szolgáló, Személyes_adatok nevű könyvtárból kiindulva kell tartani, más helyen tilos a személyes adatok tárolása. Az informatikai munkatársak ebben a könyvtárban semmilyen karbantartási munkát nem végezhetnek, annak tartalmát nem tekinthetik meg és azt nem menthetik. A magáncélú használat és a személyes adatok tárolása nem akadályozhatja az intézményi feladat ellátását. A számítógép leadásakor a Személyes_adatok mappát a gép használójának kell törölnie.

9) Az Egyetem tulajdonát képező számítógépen kizárólag jogtiszta szoftverek futtathatók, különösen tilos bármilyen illegális forrásból származó, vagy feltört program futtatása, illegális tartalom letöltése. A magáncélú használatból kizárt a játékprogramok futtatása.
10) Amennyiben az Egyetem egy munkatárs számára hordozható számítógépet biztosít, ezt a gépet kell használnia minden egyéb intézményi feladat ellátásához is, ideértve az óratartást és terepi munkákat is.
11) Az Egyetem tulajdonában álló eszközök biztonságáról minden munkatársnak gondoskodnia kell. Az Egyetem tulajdonában álló eszközben keletkezett hiba, vagy kár bekövetkezését a lehető legrövidebb időn belül jelezni kell a Klienstámogatási Osztály vezetője felé, vagy az IO hibabejelentő rendszerében. A hiba javítását kizárólag az Egyetemmel szerződött szerviz partner végezheti, az Egyetem tulajdonában álló eszközt annak felhasználója az IO vezetőjének engedélye nélkül nem javíttathatja.
12) Amennyiben az Egyetem tulajdonában álló informatikai eszközt ellopják, az adott szervezeti egység vezetőjének, vagy az eszköz használójának feljelentést kell tennie. A feljelentés jegyzőkönyvében foglaltak alapján az Egyetem állapítja meg a kár mértékét és a munkatárs felelősségének mértékét.
13) A munkakör ellátásához minden munkatárs számára csak egy hordozható számítógép adható ki abban az esetben is, ha több feladatkört lát el.
14) Az egyetemi e-mail címek nem használhatók magáncélú levelezésre, és magáncélú szolgáltatások igénybe vételére. Egy intézményi postafiók tartalma csak a tulajdonosának *írásos engedélyével,* kizárólag az intézmény működésének zavartalansága érdekében adható át más felhasználó részére. A postafiókok tartalmának átadása csak abban az esetben kezdeményezhető, ha más lehetőség nem áll rendelkezésre a működés folyamatosságának fenntartására.
15) A szervezeti egységek csak a szervezeti egység vezetőjének írásos indoklásával és engedélyével rendelkezhetnek olyan hordozható számítógéppel, amely nem személyi leltárba kerül.
16) Mentési eljárások.
    a. Minden 5-ös és 4-es biztonsági osztályba sorolt információs rendszer üzemeltetési leírásának tartalmaznia kell az adott rendszer és adatainak mentési eljárását, kitérve a mentési gyakoriságra, a mentés metódusára, a mentésért felelős személy meghatározására, a mentés ellenőrzésének periódusára és gyakoriságára, illetve az ellenőrzésért felelős személy meghatározására. Az Egyetem üzemeltetésében levő, 5-ös biztonsági szintre sorolt rendszerek esetében off-site mentések tárolása is kötelező, a mentések tárolási rendjének alapkövetelménye a rendszer üzemeltetésétől távoli tárolás, illetve az őrzés biztonsága. A keletkező off-site mentések meglétét és olvashatóságát havonta egyszer ellenőrizni, az ellenőrzés tényét dokumentálni kell.
    b. A 4-es és az alatti biztonsági szintű rendszerek esetében az on-site mentések is elfogadhatók, amennyiben azok fizikai elhelyezkedése az azokat működtető rendszer komponensektől különböző épületben helyezkedik el.
    c. A mentési rendet minden esetben úgy kell megtervezni és kialakítani, hogy a rendszer működőképessége bármelyik komponensének kiesése vagy adatainak elvesztése után esetén elfogadható mértékű adatvesztés mellett helyreállítható legyen. A helyreállítási tervben szerepelnie kell a teljes rendszer helyreállítási leírásának is. A mentési és helyreállítási terveket a rendszerek verzióváltásakor, de legalább évente egyszer felül kell vizsgálni, melynek felelőse az adott rendszerért felelős informatikai munkatárs.
    d. Az alkalmazások és informatikai eszközök (ideértve a switcheket, routereket is) konfigurációját annak minden módosítása után menteni kell. A konfigurációs mentéseknek legalább három korábbi állapotát meg kell őrizni.
    e. Az 5-ös biztonsági osztályú rendszerek adatait minden munkanap végén teljes egészében menteni kell. A mentési módnak biztosítania kell, hogy azok egy teszt rendszerbe visszatölthetők legyenek. A 4-es és az alatti biztonsági osztályba tartozó rendszerek adatai esetében a növekményes mentési eljárások is választhatók. Az egyes alkalmazások üzemeltetői feladatuktól függően készíthetnek eseti mentéseket is.

f. Minden 5-ös biztonsági osztályba sorolt rendszer esetén legalább évente egyszer visszaállítási tesztet kell végezni, melynek célja annak ellenőrzése, hogy a mentésekből az eredeti rendszer és adatai biztosan visszaállíthatók-e. A visszaállítási tesztet az eredetivel funkcionálisan megegyező környezetben kell elvégezni. A visszaállítási tesztet és annak eredményét írásban dokumentálni kell.
g. A munkaállomásokon lehetőség szerint minimális mennyiségű adatot szabad tárolni. Amennyiben ez elengedhetetlen, a munkaállomások adatait rendszeres időközönként menteni kell. A mentés elvégzéséhez az IO backup szerver szolgáltatást nyújt, ennek igénybevételét a felhasználónak, illetve a szervezeti egység vezetőjének kell kezdeményeznie.
a. A mentés elvégzésének felelőssége a munkaállomást használó felhasználóé, a mentés elmulasztásából adódó kár a munkaállomást használó munkatárs felelőssége. A mentést lehetővé tevő szoftver telepítését és működésének beállítását a szervezeti egység vezetőjének, vagy a munkaállomás kezelőjének kérésére az IO munkatársa végzi el.

17) Hálózatbiztonság menedzsmentje.
a. Az Egyetem teljes hálózati és telefon infrastruktúrája egységes koncepció és megvalósítási stratégia mentén kerül kiépítésre. Az irányelvek meghatározását és a kiépítést az IO munkatársai végzik, esetenként külső szolgáltató cég bevonásával.
b. Az IO egységes intézményi WiFi hálózatot üzemeltet. Különösen nagy biztonsági kockázatot jelent, ezért kifejezetten tilos WiFi végpont (router, AP) jóváhagyás nélküli üzembe állítása.
c. A kommunikációs hálózathoz csak az IO által engedélyezett és jóváhagyott eszközt szabad kapcsolni.
d. Az Egyetem területén csak az IO által engedélyezett és jóváhagyott internet-hozzáférést szabad használni. Különösen nem megengedett az intézményi informatikai hálózat bármilyen összekötése vagy megosztása bármilyen más hálózattal, ideértve a GSM szolgáltatáson alapuló mobiltelefonos kapcsolatot is.
e. Az IO engedélye és felügyelete nélkül kifejezetten tiltott bármilyen külső hálózati kapcsolat belső hálózati szolgáltatásban végződtetése, pl. VPN szerver, vagy különféle tunnelek létrehozása.
f. A nem használt hálózati végpontok hálózati kapcsolatát fel kell függeszteni.
g. Az IO üzemelteti az Egyetem tűzfal rendszerét. A tűzfal alapértelmezés szerinti biztonsági beállítása a kapcsolatok tiltása. Az egyes szolgáltatások számára szükséges kommunikációs utakat az adott rendszer működési előírásainak megfelelően szabad megnyitni. A tűzfal újabb portjainak megnyitása kizárólag a munkavégzéshez szükséges szoftverek működésének érdekében végezhető el.
h. A tűzfal beállításait rendszeresen felül kell vizsgálni, és a szükségtelenné vált kapcsolati utakat be kell zárni.

18) Média kezelés.
a. Az 5-ös, 4-es és 3-as biztonsági osztályú rendszerek adatainak mentéseit tartalmazó adathordozók jogvédelem alá eső adatokat, személyes adatokat tartalmazhatnak. Ezeknek az adathordozóknak a kezelésére ugyanazok a szabályok vonatkoznak, mint az adatokat eredetileg tároló rendszereszközökre.
b. Az 5-ös, 4-es és 3-as biztonsági osztályú rendszerek adatainak mentéseit tartalmazó adathordozók mentéseit tartalmazó adathordozók mentéseit tartalmazó adathordozókat az IO által kijelölt, elkülönített helyiségben, zárt lemez-, vagy páncélszekrényben kell tárolni. Az adathordozókról és azokhoz történő hozzáférésről a szekrényhez hozzáféréssel rendelkező személynek nyilvántartást kell vezetni.
c. Az adathordozók mentésből történő kivonása és szakszerű megsemmisítése az IO feladata.

19) Szerviz tevékenységek.
a. Minden informatikai eszköz szerviztevékenységre történő átadása előtt gondoskodni kell az adattartalom illetéktelen személy általi megismerésének megakadályozásáról.

20) Információcsere.
a. Az 5-ös, 4-es és 3-as biztonsági osztályú rendszerek adatain automatikus adatcserét megvalósító kapcsolatok és folyamatok létesítéséhez az IO vezetőjének és az adott rendszert üzemeltető szervezeti egység vezetőjének engedélye szükséges. A kapcsolat kérelmezésekor az üzemeltetőknek pontosan részletezniük kell az adatkezelés célját, az alkalmazott műszaki megoldást kiemelten az adatcsere biztonságát megvalósító műszaki megoldásokra.

   b. Az adatcsere környezetét és technológiai megoldásait az adatcserét kezdeményező alkalmazás üzemeltetőjének dokumentálnia kell.

21) Monitorozás.
   a. Az informatikai rendszer felügyeletére az IO-nek automatikus felügyeleti rendszert kell üzemeltetnie.
   b. A felügyeleti rendszer komponenseinek ki kell terjednie a szerverek, aktív hálózati elemek, menedzselhető nyomtató-másoló berendezések és minden, a rendszerbe beköthető informatikai berendezés állapotára és folyamatainak felügyeletére.
   c. A felügyeleti rendszernek a rendszer eseményeiről jelzéseket kell küldenie a kezelő személyzet számára. A jelzéseknek tartalmaznia kell az esemény idejét, súlyossági fokát és leírását. Az üzenetkezelési eljárásnak hierarchikusnak kell lennie, az egyes eseménytípusok kezelési határidejének lejárata után a felettes vezető számára kell továbbítania az esemény kezelésének feladatát.
   d. A felügyeleti rendszernek alkalmasnak kell lennie arra, hogy adatai alapján az informatikai berendezések éves rendelkezésre állásának mértéke kiszámítható legyen.
   e. A felügyleti rendszer eseményeit két évig kell megőrizni.

22) Archiválás.
   a. Az Egyetem kivezetésre került rendszereit, amennyiben azt az adott szervezeti egység vezetője elrendeli, archiválni kell. Az archivált rendszernek alkalmasnak kell lennie az abban tárolt adatok kereshetőségére, de új adatok rögzítését, a korábbiak módosítását már nem szabad lehetővé tennie.
   b. Az archív rendszerek biztonsági besorolását az azokban tárolt adatok jellege alapján a használatban levő rendszerekre vonatkozó szabályok szerint kell elvégezni.
   c. Az archív rendszerekre ugyanazok a szabályok vonatkoznak, mint a használatban levőkre, különös tekintettel a hozzáférési jogosultságok meghatározására.
   d. Az archivált rendszerekről már nem szükséges rendszeres biztonsági másolatot készíteni, de rendelkezni kell off-site mentéssel, amelyből szükség esetén az archivált rendszer helyreállítható.

15. Emberi erőforrások

1) Az Egyetem információs rendszeréhez történő hozzáférés alapja az Egyetem címtára, melyet az IO üzemeltet.
2) Új munkatárs felvétele esetén a munkatárs adatait az IO címtárába fel kell venni. Az ehhez szükséges adatokat a személyügyi osztály vezetője által megbízott munkatárs a felvételi döntés után küldi meg az IO számára.
3) A címtárban alapvetően csak az Egyetemmel határozatlan vagy határozott idejű *munka jogviszonyban* állók szerepelhetnek. Megbízásos jogviszonyú munkatársak számára csak a megbízás fennállásáig érvényes, csak az adott feladatkör ellátására alkalmas hozzáférés biztosítható. A hozzáférésnek a megbízás vagy munka jogviszony lejártakor automatikusan meg kell szűnnie.
4) Az Egyetem dolgozói számára minden információs rendszerben csak azok a jogkörök biztosíthatók, amelyek a munkakörének ellátásához szükségesek. A munkakör megváltozását a HEO, az ehhez kapcsolódó jogosultsági változásokat a munkavállaló régi és új szervezeti egységének vezetője írásban jelzi az IO munkatársa felé. Amennyiben a szervezeti egység vezetője a jogosultsági változás kérelmét elmulasztja, az ebből adódó következmények felelőssége őt terheli.
5) Egy munkatárs jogviszonyának megszűnése esetén a hozzáféréseit meg kell szüntetni. A megszüntetés az erre szolgáló leszámoló lap kitöltésével történik. Az IO munkatársa a lap elfogadásával a kilépés határnapjával megszünteti az informatikai rendszerekhez adott hozzáféréseit, átveszi a munkatárs számára átadott informatikai eszközöket. A kilépést követően a munkatárs még egy hónapig fogadhatja az intézményi e-mail címére érkező leveleit, de e-mail küldését már nem kezdeményezheti.
6) Amennyiben egy munkatársnak a kinevezéses jogviszony megszűnése után az Egyetem információs rendszeréhez további hozzáférésre van szüksége, az az igénylő szervezeti egység vezetőjének írásos kérésére meghosszabbítható. A hosszabbítás kizárólag határozott időtartamra történhet, lejárata a HEO

által igazolt szerződésben foglalt határidő. A lejárt érvényességi idejű hozzáféréseket automatikusan tiltani kell.

7) A jogviszony megszűnése után a munkatárs az Egyetem adatvagyonának semmilyen részének másolatával nem rendelkezhet. A titoktartási kötelezettség a jogviszony megszűnése után is fennáll.

16. Hozzáférés és jogosultságok szabályozása

1) Hozzáférési politika.
    a. Authentikáció. Minden, az Egyetem információs rendszerében tárolt adatot és szolgáltatást hozzáférési védelemmel kell ellátni. A hozzáféréseket személyre szólóan kell kialakítani. A hozzáféréseket csak az a személy használhatja, akinek azt kiadásra került. A hozzáférés történhet felhasználói névvel és jelszóval, vagy lehetőség esetén BALE[1] eszközzel.
    b. Authorizáció. A hozzáférésekhez az egyes alrendszerekben szerepköröket, ennek hiányában objektum szintű jogosultságokat kell meghatározni. A szerepköröket és a jogosultságokat abban a legkisebb körben kell meghatározni és beállítani, hogy a felhasználó feladatköre még elvégezhető legyen. A minimális jogkör elve az adott szervezeti egység vezetőire is érvényes, számukra sem állítható be a szerepkörükhöz nem szükséges jogkör. A rendszer üzemeltetését és a mentéseket készítő rendszer adminisztrátorok számára, amennyiben feladatuk másképp nem végezhető el, teljes hozzáférési jogosultságot kell adni.
    c. Hozzáférés nélkül az egyes rendszerekből kizárólag publikus adatok lehetnek kinyerhetők.
    d. A szerepköröket és a jogosultságokat évente egyszer felül kell vizsgálni. A felülvizsgálat eredményét a rendszert üzemeltető szervezeti egység vezetőjének kell ellenőriznie és jóváhagynia.
2) A hozzáférési jelszavakat minden rendszerben egyirányú titkosítással kell tárolni. Az Egyetem informatikai rendszerében nem működhet olyan komponens, amely jelszavakat olvasható formában, vagy elavult titkosítással kódol. Az elvárt titkosítási algoritmusnak SHA256-nak, vagy annál fejlettebbnek kell lennie.
3) Amennyiben az Egyetem adatvagyonának titkosítása során felhasznált kódolási eljárás elavulttá válik, a kódolási eljárást le kell cserélni egy megbízható változatra.
4) Az 5-ös, 4-es és 3-as biztonsági osztályú rendszerekhez szükséges jelszavakat meghatározott időszakonként cserélni kell.
5) A Egyetem rendszereit úgy kell kialakítani, hogy azok ne tegyék lehetővé egyszerű jelszavak használatát.
6) Minden rendszerben korlátozni kell a sikertelen bejelentkezési kísérletek számát. A sikertelen bejelentkezési kísérleteket naplózni kell. A belépési kísérletekről az 5-ös, 4-es és 3-as biztonsági osztályú rendszerekben a naplózáson túl lehetőség szerint az automatikus felügyeleti rendszernek jelzést kell adnia az üzemeltető személyzet számára.
7) Az 5-ös, 4-es és 3-as biztonsági osztályú rendszerekhez hozzáféréssel rendelkező munkatársak esetében a hozzáférés megadása az adott szakrendszer üzemeltetését végző szervezeti egység vezetőjének fel kell hívnia a figyelmet az IBSZ-ben foglaltak betartására.
8) Címtár.
    a. Az Egyetem annak érdekében, hogy az információs rendszerében központi nyilvántartást valósíthasson meg, központi címtárat alakít ki. A címtárban minden, az Egyetemmel munkavállalói jogviszonyban álló személynek szerepelnie kell. A címtár személyes adatokat tartalmaz, ezek köréről, felhasználási céljairól, valamint kezelésükről az Egyetem az iig.uni-eszterhazy.hu oldalon ad tájékoztatást.
    b. A többszörös adminisztráció elkerülésére lehetőség szerint minden informatikai rendszernek a címtárból kell azonosítást végeznie.
    c. A címtár adatainak aktualizálása minden felhasználó saját felelőssége. Amennyiben annak adataiban (telefonszám, e-mail cím, szobaszám, munkakör stb.) változás következik be, az aktualizálás elvégzése legrövidebb időn belül a munkavállaló kötelessége.
9) Távoli hozzáférés.
    a. Az 5-ös biztonsági osztályú rendszerekhez kizárólag az Egyetem belső hálózatából működtethetők hálózati kapcsolatok. Minden egyéb hozzáférési kísérlet informatikai

[1] Biztonságos Aláírás Létrehozó Eszköz.

incidensnek minősül, amelyet az informatikai üzemeltető személyzetnek detektálnia kell, és ki kell vizsgálnia.

b. Az egyetem internet eléréseinek kezelését az IO vezetője kezeli. Az Egyetemen tilos az IO vezetőjének engedélye nélkül további internet kapcsolatok kialakítása.
c. Az Egyetem a távmunka lehetőségének biztosítására VPN megoldáson alapuló távoli elérést biztosít a dolgozói számára. A VPN kapcsolati végpontok kiépítése és felügyelete az IO feladatköre. Szigorúan tilos az IO engedélye nélküli VPN kiszolgáló telepítése.

10) Operációs rendszer hozzáférés.
    a. Azokon a számítógépeken, melyekről 5-ös, 4-es és 3-as biztonsági osztályú rendszerekhez privilegizált felhasználóként történik hozzáférés, a felhasználók nem rendelkezhetnek teljes hozzáféréssel.
    b. A teljes jogú hozzáférést indokolt esetben az adott szervezeti egység vezetője által megbízott személy, vagy az IO munkatársa birtokolja.
11) Naplózás.
    a. Az 5-ös, 4-es és 3-as biztonsági osztályú rendszerek informatikai komponenseiben, valamint az szerver szoftverekben és alkalmazásokban keletkező naplóeseményeket rögzíteni kell.
    b. A 3-as és az alatti biztonsági osztályú rendszerekben az operációs rendszer és szerver szoftverek rendszer szintű naplóeseményeit kell rögzíteni.
    c. A naplóeseményeket egy kizárólag erre a célra szolgáló naplószerveren is tárolni kell.
    d. A naplóeseményeket egy évig kell megőrizni.
    e. A naplózáshoz TCP kapcsolatokat kell használni, a naplózás során az időpontok rögzítését ezredmásodperces pontosságúra kell állítani.
    f. A logszervereken minden olyan eseménynaplót meg kell őrizni, amely az informatikai rendszer elemeinek biztonságát érinti.
    g. A naplók képzése és tárolása alkalmas kell, hogy legyen arra, hogy azzal bizonyítani lehessen az esetleges illetéktelen hozzáféréseket és megállapíthatók legyenek a felelősségek.
    h. Az eseménynaplók tartalmát automatizált vagy manuális úton rendszeresen át kell vizsgálni.
    i. Incidens esetén a naplóeseményeket a lehető legrövidebb időn belül át kell vizsgálni és az incidens kezelésének kidolgozásában alapul kell venni.

17. Megfelelőség

1) A mindenkori jogszabályi megfelelőség biztosítása az adott szervezeti egység vezetőjének felelőssége.
2) Az adott szervezeti egység vezetője nem felel a rendszer felhasználói által elkövetett jogsértésekért, ideértve a jogosulatlan adatkezelést, szerzői jogokkal történő visszaélést.
3) Hatósági felszólításra a jogszabályban előírt adatokat az Egyetem a hatóság részére kiadja és amennyiben szükséges, az adott ügyben a hatóságokkal a jogszabályi előírás mértékékéig együttműködik.
4) Az információbiztonsági követelmények betartását és az információ biztonság tudatosság szintjének mérését az IO penetrációs tesztekkel is végezheti.
5) Azon rendszerek esetében, amelyek üzemeltetése nem felel meg az IBSZ-ben foglaltaknak, egy esetleges incidens felelőssége az adott szervezeti egység vezetőjét terheli.

18. Új információs rendszerek elfogadási eljárása

1) Új információs rendszer bevezetése előtt, már a tervezési fázisban egyeztetni kell a szolgáltatás üzemeltetőivel az alábbi szempontok alapján:
    a. Meg kell határozni a rendszer fejlesztőjét, üzemeltetőit és a rendszer életciklusát.
    b. Az üzemeltetést végzőknek jóvá kell hagyni a rendszer adatainak tárolásával és a biztonságos üzemeltetéssel kapcsolatos funkcióit és eljárásait. Amennyiben a biztonságos üzemeltetés nem valósítható meg, az üzemeltetők a rendszer működtetését megtagadhatják.
    c. Meg kell határozni és jóvá kell hagyni a rendszerekkel kapcsolatos támogatási feladatok, az azt ellátó személyek és az SLA körét a rendszer teljes életciklusára vonatkozóan.

19. Működés folytonosságának biztosítása

1) A 4-es és az 5-ös biztonsági szintű rendszerek esetében üzletfolytonossági tervet kell készíteni. A tervnek tartalmaznia kell az incidenskezelési eljárásokat, az adott rendszert használó szervezetek működési rendjét az egyes rendszerelemek, vagy a teljes rendszer kiesése esetére, a mentési tervet és az ellenőrzés leírását.
2) Az üzletfolytonossági tervben előírt előkészítő termékeket, tartalék szolgáltatásokat és erőforrásokat a normál működési időszakban kell biztosítani.
3) Az üzletfolytonossági terv vonatkozó részeit az adott szervezeti egység munkatársaival meg kell ismertetni.

20. Információbiztonsági események menedzsmentje

1) Az Egyetem információs rendszerével és az adatvagyonával kapcsolatos szokatlan, vagy a normál működéstől eltérő eseményeket be kell jelenteni a szolgáltatás üzemeltetőjének.
2) Az adott szolgáltatás üzemeltetője és az IO minden, az Egyetem kezelésében levő informatikai rendszer és adatvagyon esetében köteles kialakítani azokat a kommunikációs csatornákat, amelyeken incidens bejelentéseket fogad. Ezek az IO esetében a következők:
    a. E-mail: helpdesk@uni-eszterhazy.hu
    b. Telefon: +36 36 520400/2229-es, 2027-es, és a 2251-es mellékek.
    c. Személyesen az IO vezetőjénél, klienstámogatási, vagy hálózatüzemeltetési osztályvezetőjénél.
3) Az informatikai rendszerekkel kapcsolatos biztonsági hiba észlelése vagy megismerése esetén azt be kell jelenteni az adott rendszer üzemeltetője és az IO felé. A biztonsági hiba kihasználása a BTK-ba ütköző cselekmény, az Egyetem ilyen esetekben jogi eljárást kezdeményez minden olyan esetben, amikor a hibát észlelő személy elmulasztja annak jelzését az üzemeltetők felé, vagy a biztonsági hibát nyilvánosságra hozza.
4) Biztonsági esemény bejelentésekor a bejelentőnek minden olyan birtokában levő adatot csatolnia kell, amely az esemény kezeléséhez szükséges lehet.
5) Tömeges érintettség esetében az üzemeltetőknek a normál kommunikációs csatornákon kell tájékoztatást nyújtaniuk.
6) A 4-es és 5-ös szintű rendszerek esetében üzletfolytonossági és incidenskezelési tervet kell készíteni.
7) Az incidensek bejelentését az üzemeltetők kötelesek súlyosságuk szerint besorolni és annak megfelelően az incidenskezelési eljárást megindítani és lefolytatni.

21. Az egyetemen kívülre történő adatátadás

1) Adatok kiadása a 4-es és az 5-ös biztonsági szintbe sorolt adatvagyonból csak a rektor, illetve a kancellár engedélyével történhet, mely alól kivételt képeznek a törvényi kötelezettségek alapján történő adatszolgáltatások.
2) Személyes adatok kiadása csak az arra jogosultak által, a hatályos jogszabályoknak megfelelően, a GDPR ide vonatkozó előírásainak különös figyelembevételével, a belső egyetemi szabályozás alapján történhet.
3) Az átadott adatok védelméért a hatályos jogszabályok alapján az átvevő fél felel.
4) Az adatszolgáltató az átadást megelőzően tájékoztatást kérhet az IO vezetőjétől adatvédelmi és információbiztonsági kérdésekben.

22. Az IBSZ felülvizsgálata

1) Jelen IBSZ felülvizsgálatára háromévente kerül sor. A következő esedékes felülvizsgálat időpontját a dokumentum lezárásakor kell meghatározni. Az IBSZ felülvizsgálatát emellett el kell végezni minden olyan esetben, amikor:
    a. azt érintő jogszabályi változás lép életbe, vagy az olyan technikai, műszaki, információbiztonsági változás történik, amely az IBSZ-módosítását igényli.

b. Új munkafolyamatok, szervezeti egységek, szolgáltatások kerülnek bevezetésre vagy szűnnek meg.
c. Új, lényeges kockázati elem válik ismertté.
d. Biztonsági incidens elemzése utáni intézkedés bevezetése érdekében.

2) Az IBSZ-szel kapcsolatos véleményeket, változtatási igényeket az IO vezetőjének kell benyújtani. Az igénynek tartalmaznia kell a benyújtó adatait, a megváltoztatásra javasolt bekezdés(ek) számát, a javasolt új szövegrészt és annak indoklását.

23. Záró rendelkezések

1) Jelen szabályzatot az Egyetem Szenátusa a 19/2022. (IV.27.) sz. határozatával fogadta el és az – 2022. május hó 1. napján lép hatályba.

Eger, 2022. április 27.

_____
Dr. Pajtókné Dr. Tari Ilona s.k.
rektor

Az Egri Főegyházmegye képviseletében jóváhagyom:

Eger, 2022. május 3.

_____
Dr. Ternyák Csaba s.k.
érsek