

# AZ EÖTVÖS LORÁND TUDOMÁNYEGYETEM

INFORMÁCIÓBIZTONSÁGI SZABÁLYZATA

2007.<sup>1</sup>

---

<sup>1</sup> Egységes szerkezetben a módosításáról szóló XXXI/2012. (II. 13.) Szen. sz. határozattal.

## Tartalom

1	Az IBSZ kiadásának célja, hatálya, szerkezete .....	4
2	A kiadás dátuma, érvényessége.....	4
3	A kötelező felülvizsgálat (revízió) időpontja és az IBSZ változásmenedzsmentje .....	4
4	Kapcsolódó szabályozások (hivatkozások) .....	4
5	Információbiztonsági politika .....	5
5.1	IT rendszerek biztonsági osztályai, besorolás.....	5
5.1.1	Kritikus rendszerek (A).....	5
5.1.2	Kiemelt rendszerek (B) .....	5
5.1.3	Normál rendszerek (C).....	5
5.1.4	Egyéb rendszerek (D).....	5
5.2	Az információbiztonsági politika elfogadása és közzététele.....	7
5.3	Az információbiztonsági politika rendszeres felülvizsgálata.....	7
6	Az információbiztonság szervezeti kérdései .....	7
6.1	Az információbiztonság belső szervezete.....	7
6.1.1	Vezetői elkötelezettség.....	7
6.1.2	Információbiztonsági koordináció (érintett felekkel egyeztetés).....	7
6.1.3	Az információbiztonsági felelősségek allokációja .....	8
6.1.4	Új információ-feldolgozó rendszerek elfogadási eljárása .....	8
6.1.5	Bizalmassági nyilatkozatok .....	8
6.1.6	Kapcsolattartás hatóságokkal .....	8
6.1.7	Kapcsolattartás különleges érdekközösségekkel .....	8
6.1.8	Az információbiztonság független felülvizsgálata .....	9
6.2	Külső felek.....	9
6.2.1	A külső felekhez, partnerekhez kapcsolódó kockázatok azonosítása .....	9
6.2.2	Ügyfelekkel kapcsolatos információbiztonsági feladatok (jogosultság kiadás felhasználóknak).....	9
6.2.3	Harmadik féllel kötött megállapodások biztonsági kérdései .....	9
7	Az információvagyon menedzsmentje .....	9
7.1	Felelősség az információvagyonért.....	9
7.1.1	Információs vagyon leltár.....	9
7.1.2	Az információs vagyon tulajdonjoga.....	9
7.1.3	Az információs vagyon használatának szabályai .....	10
7.2	Az információvagyon osztályozása .....	10
7.2.1	Az osztályozás elvei, vezérfonala.....	10
7.2.2	Az osztályba sorolt információs vagyonelemek jelölése és kezelése .....	10
8	Emberi erőforrással kapcsolatos biztonsági kérdések .....	11
8.1	Alkalmazás előtti tennivalók (szerepek és felelősségek, „átvilágítás”, alkalmazási feltételek).....	11
8.2	Az alkalmazás alatti tennivalók (felelősségek menedzsmentje, információbiztonsági képzések és tréningek, fegyelmi ügyek) .....	11
8.3	Elbocsátás vagy munkakör-változás (elbocsátási felelősségek, dolgozónak kiadott eszközök visszavétele, hozzáférési jogok megvonása).....	11
9	Fizikai és környezeti biztonság .....	11
9.1	Biztonsági zónák, területek.....	11
9.1.1	Fizikai biztonsági határvédelem.....	11
9.1.2	Fizikai belépési szabályozás.....	12
9.1.3	Irodák, szobák és egyéb létesítmények fizikai biztonsága .....	12
9.1.4	Külső és környezeti károk elleni védelem.....	12
9.1.5	Munkavégzés biztonsági zónákban .....	12
9.1.6	Nyilvános hozzáférés, szállítási és töltési területek.....	13
9.2	Eszköz biztonság .....	13
9.2.1	Eszközök elhelyezése, védelme .....	13
9.2.2	Támogató közművek (szolgáltatások) .....	13
9.2.3	Kábelbiztonság.....	13
9.2.4	Eszközkarbantartás.....	13
9.2.5	Telephelyen kívül használt eszközök biztonsági szabályai .....	13
9.2.6	Eszközök biztonságos megsemmisítése vagy újrahasznosítása.....	13
9.2.7	Eszközök (HW, SW) kivitele telephelyről .....	14
10	Kommunikáció és üzemelés menedzsment.....	14

10.1	Működési folyamatok és felelőségek.....	- 14 -
10.2	Harmadik fél által nyújtott szolgáltatások menedzsmentje .....	- 14 -
10.3	Rendszertervezés és elfogadás .....	- 14 -
10.4	Védekezés vírusok és egyéb kártékony kódok ellen .....	- 15 -
10.5	Biztonsági mentések .....	- 15 -
10.6	Hálózatbiztonság menedzsmentje .....	- 15 -
10.7	Média kezelés.....	- 16 -
10.8	Információcsere.....	- 16 -
10.9	Elektronikus kereskedelem .....	- 16 -
10.10	Monitorozás .....	- 16 -
11	Hozzáférés szabályozás .....	- 16 -
11.1	Működési követelmények a hozzáférés szabályozása érdekében (hozzáférési politika).....	- 16 -
11.2	Felhasználói hozzáférés menedzsmentje.....	- 17 -
11.3	Felhasználói felelőségek.....	- 17 -
11.4	Hálózati hozzáférés .....	- 17 -
11.5	Operációs rendszer hozzáférés.....	- 18 -
11.6	Alkalmazásokhoz és információkhoz való hozzáférés szabályozása .....	- 18 -
11.7	Mobil számítógép használat és telefonos munkavégzés .....	- 18 -
12	Információs rendszerek beszerzése, fejlesztése és karbantartása.....	- 18 -
12.1	Információs rendszerek biztonsági követelményei .....	- 18 -
12.2	Alkalmazások helyes használata .....	- 18 -
12.3	Kriptográfiai szabályozások.....	- 19 -
12.4	Rendszer fájlok biztonsága .....	- 19 -
12.5	Fejlesztési és támogatási folyamatok biztonsága .....	- 19 -
12.6	Műszaki sérülékenység menedzsment .....	- 19 -
13	Információbiztonsági események menedzsmentje.....	- 20 -
13.1	Biztonsági események és gyengeségek jelentése .....	- 20 -
13.2	Információbiztonsági események és fejlesztések menedzsmentje .....	- 20 -
14	Működés-folytonosság biztosítása .....	- 20 -
14.1	A működés folytonosság információbiztonsági vetülete.....	- 20 -
15	Megfelelőség.....	- 20 -
15.1	Jogszabályi megfelelés.....	- 20 -
15.2	Megfelelés biztonsági politikának, szabványoknak és műszaki előírásoknak .....	- 21 -
15.3	Információs rendszerek felülvizsgálatával kapcsolatos megfontolások .....	- 21 -
16	Fogalmak, rövidítések.....	- 22 -
17	Mellékletek .....	- 25 -
1.	IBSZ változáskezelési lap.....	- 25 -
2.	Felhasználói nyilatkozat .....	- 27 -
3.	A legfontosabb információbiztonsággal kapcsolatos törvények, jogszabályok, szabványok .....	- 28 -

## **1 Az IBSZ kiadásának célja, hatálya, szerkezete**

Az információbiztonsági szabályzat célja, mindazon intézkedések és betartandó szabályok összefoglalása, melyek által az ELTE információbiztonsága (rendszerek adatok és információk rendelkezésre állása, sértetlensége és bizalmassága) fenntartható legyen.

Az IBSZ-ben foglaltak a szolgáltatók és a szolgáltatást igénybevevők számára egyaránt kötelező érvényűek.

Jelen szabályzat mindenkire nézve kötelező, aki használja az ELTE számítógép-hálózatát, annak berendezéseit (későbbiekben felhasználók). Az előbbieknél megfelelően a szabályzat személyi hatálya kiterjed az ELTE összes hallgatójára és dolgozójára, aki oktatási, kutatási, tudományos vagy az intézmény adminisztrációs feladataihoz az ELTE számítógép-hálózatát és eszközeit használja. Ha az intézmény harmadik félnek is lehetőséget biztosít hálózatának használatára, akkor harmadik félre nézve is kötelező a szabályzatban foglaltakat betartani.

A szabályzat alapszerkezete követi az ISO 27001:2005 szabvány „A” mellékletének („Szabályozási célok és kontrollok”) szerkezetét. Ennek célja, hogy az ELTE hatékony és nemzetközi szabványon alapuló információbiztonsági irányítási rendszert alapozzon meg.

A mindenkori szabályzat felhasználók számára készült kivonata az Informatikai Házirend.

## **2 A kiadás dátuma, érvényessége**

Jelen szabályzat az Egyetemi Szenátus által történő jóváhagyás pillanatában lép hatályba. A szabályzat jelen változata mindaddig érvényesnek tekintendő, amíg annak egy új változatát az Egyetemi Szenátus jóvá nem hagyja.

## **3 A kötelező felülvizsgálat (revízió) időpontja és az IBSZ változásmenedzsmentje**

A szabályzat felülvizsgálatára az alábbiak szerint kerül sor:

- évente egy alkalommal (az esedékes következő felülvizsgálati időpontot a dokumentum lezárásakor kell kijelölni.)
- minden olyan esetben, amikor a szabályzatban leírtakban jelentős változás(ok) történnek.

Jelen szabályzat hivatkozott mellékletei IIG Igazgatói utasítás alapján módosíthatóak.

Az IBSZ-szel kapcsolatos észrevételeket, változtatási javaslatokat az IIG igazgatójának címzett, az 1. mellékletben található változáskezelési lapon lehet benyújtani.

A változtatási javaslatot az ELTE Informatikai Bizottságának véleményezése alapján a Szenátus hagyja jóvá. Az IIG igazgatója a szenátusi határozatot követő 8 napon belül írásban köteles tájékoztatni az indítványozót a javaslat vagy beadvány sorsáról.

A szabályzat mellékleteinek módosítását az IIG igazgatója saját hatáskörben végzi konzultálva az érintett szervezeti egységek vezetőivel, illetve az egyes szolgáltatásokért felelős IIG vezetővel. A mellékletek IIG Igazgatói utasítások formájában készülnek és módosulnak.

## **4 Kapcsolódó szabályozások (hivatkozások)**

- ELTE Szervezeti és Működési Szabályzata (továbbiakban ELTE SZMSZ)
- ELTE Informatikai Szabályzat
- Munkaköri leírások
- Hallgatók jogállását leíró dokumentumok

## **5 Információbiztonsági politika**

Az információbiztonsági politika célja, hogy az ELTE szervezeti egységei részére 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.

### **5.1 IT rendszerek biztonsági osztályai, besorolás**

#### **5.1.1 Kritikus rendszerek (A)**

Az intézmény működése szempontjából kritikus, az intézmény egészére kiterjedő rendszerek, amelyek szenzitív, illetve személyes adatokat tartalmaznak. Adatvédelmi szempontból kiemelt védelmet igényelnek.

- Bér- és Munkaügyi rendszer
- Gazdasági, ügyviteli rendszer
- Dokumentumkezelési rendszer
- Tanulmányi rendszer
- Központi levelező kiszolgálók
- Központi tárhely-kiszolgálók
- Intézményi autentikációs rendszerek

#### **5.1.2 Kiemelt rendszerek (B)**

Az intézmény működése szempontjából kritikus rendszerek, amelyek elsősorban technikai jellegűek, a rajtuk tárolt adatok nem személyes jellegűek.

- Telekommunikációs hálózat
- Technológiai (environment, middleware) rendszerek
- Kommunikációs rendszerek

#### **5.1.3 Normál rendszerek (C)**

A vagy B kategóriába nem sorolt, a teljes intézmény napi működése szempontjából nem kritikus, illetőleg az intézménynek csak egyes részeire kiterjedő olyan rendszerek, amelyek indítása/üzemeltetése során központi felülvizsgálat történik, illetőleg teljes körű dokumentáció készül.

- Interaktív kiszolgáló szerverek
- Kutatói rendszerek
- HPC

#### **5.1.4 Egyéb rendszerek (D)**

Az előző három kategóriába nem sorolt rendszerek.

Információbiztonsági alapelvek:

Az ELTE szervezeti egységei által kezelt adatok védelmét bizalmasság, hitelesség, sértetlenség, rendelkezésre állás és funkcionalitás szempontjából úgy kell megvalósítani, hogy az informatikai rendszernek és környezetének védelme folytonos, teljes körű, zárt és a kockázatokkal arányos legyen, valamint a megvalósuljon a zárt szabályozási ciklus, a következők szerint:

1. A teljes körűsége vonatkozó alapelveket 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 személyzetre és a külső partnerekre,
  - az MSZ OSI 7498-1. szabványban meghatározott nyílt rendszerek architektúrája minden rétegére, azaz mind a számítástechnikai infrastruktúra, mind az informatikai alkalmazások szintjén,
  - mind a központi, mind a végponti informatikai eszközökre és környezetükre.
2. A védelem zártsága akkor biztosított, ha az összes valószínűsíthető fenyegetés elleni védelmi intézkedések megvalósulnak.
3. A védelem akkor kockázatarányos, ha az informatikai rendszerek által kezelt adatok védelmének erőssége és költségei a felmért kockázatokkal arányban állnak. Célkitűzés a minimális védelmi költséggel elért maximális védelmi képesség.
4. A védelem folytonossága úgy biztosítható, hogy az informatikai rendszerek fejlesztése és megvalósítása során kialakított védelmi képességeket a rendszerből történő kivonásig folytonosan biztosítani kell a rendszeres ellenőrzéssel és az ezt követő védelmi intézkedésekkel.
5. A zárt szabályozási ciklus úgy érvényesíthető, hogy az adminisztratív védelemmel biztosítani kell a szabályozás, érvényesítés, ellenőrzés és a védelmi intézkedések/szankcionálás zárt folyamatát.

További céljaink és elveink:

Igyekszünk a kockázatainkat minimalizálni, de minden vezetőben és munkatársban tudatosítjuk, hogy teljes körű védelem és biztonság nincsen, és ezzel összefüggésben a maradvány kockázatokat tudatosan vállaljuk.

A felelőségeket az információbiztonság területén hangsúlyozottan elhatároljuk és az egyes szervezeti szerepkörökhöz kötjük.

Hangsúlyozottan törekszünk a törvényi és jogszabályi megfelelésre különös tekintettel a személyes adatok kiemelt védelmére. Az Adatvédelmi Biztos ez irányú állásfoglalásait figyelembe vesszük.

Megpróbáljuk kiegyensúlyozottan kezelni a mobilitás lehetősége és a biztonság közötti ellentmondást.

Elsődleges célunk a működőképesség fenntartása, ezért az olyan felhasználókat, akik magatartásukkal más felhasználók tömegeinek munkáját veszélyezteti, haladéktalanul kizárunk a szolgáltatásból mindaddig, amíg a veszélyt okozó tevékenységét nem szünteti meg. A védelem mellett biztosítjuk az oktatási és kutatási tevékenységhez szükséges szabad információáramlást.

A felhasználói jogosultságok természetes személyhez kötöttek és nem átruházhatóak. Az információbiztonsági incidensek esetében a felelőség a jogosultsággal bíró személyhez

kötődik. Rosszhiszemű felhasználásnak tekintjük, ha a felhasználó jogosultságát meghaladó műveleteket szándékosan kezdeményez, illetve jogosultságát megkísérli módosítani. Elérendő cél, hogy a szolgáltató rendszerek üzemzavarait ne a felhasználók, hanem automatikus szolgáltatásmonitorozó komponensek jelezzék.

## **5.2 Az információbiztonsági politika elfogadása és közzététele**

Az információbiztonsági politikát az IBSZ részeként kezeljük, ezért elfogadása és közzététele az IBSZ-szel megegyező módon történik, azaz az Információbiztonsági politikát az IBSZ részeként az IIG igazgatójának előterjesztése alapján az Egyetemi Szenátus fogadja el. Az Információbiztonsági Politika az IBSZ aktuális verziójának részeként az IIG web portálján megtekinthető.

## **5.3 Az információbiztonsági politika rendszeres felülvizsgálata**

Az információbiztonsági politika az IBSZ szerves része, és az IT-SZ-szel egy időben és azonos módon történik a felülvizsgálata:

- évente egy alkalommal (az esedékes következő felülvizsgálati időpontot a dokumentum lezárásakor kell kijelölni.)
- minden olyan esetben, amikor a politikában leírtakban jelentős változás(ok) történnek.

## **6 Az információbiztonság szervezeti kérdései**

### **6.1 Az információbiztonság belső szervezete**

Az információbiztonsággal kapcsolatos felelősség megoszlik az IIG, az egyes szervezetek és a felhasználók között. A felelősség-megosztás elveit az alábbiakban tárgyaljuk.

#### **6.1.1 Vezetői elkötelezettség**

Minden szervezeti egység vezetője személyesen felel az információbiztonság kultúrájának kialakításáért és fenntartásáért.

A vezetők elkötelezettségüket személyes példamutatással (szabályozások betartása) és személyes felelősségvállalással demonstrálják.

A belső és külső szolgáltatói megállapodások (SLA-k) figyelése, figyelembe vétele és a bennük megfogalmazott paraméterek mérése a vezetői elkötelezettség kinyilvánítása. Az információbiztonsági intézkedések megvalósításához szükséges erőforrások biztosítása szintén a vezetői elkötelezettséggel összhangban zajlik.

Az intézmény informatikai rendszereinek IBSZ-nek való megfelelése az IIG igazgatójának hatásköre.

#### **6.1.2 Információbiztonsági koordináció (érintett felekkel egyeztetés)**

Az informatikai rendszerek IBSZ megfelelési vizsgálatát, illetőleg az ezzel kapcsolatos tanácsadást az IIG szolgáltatásmenedzsere végzi (a külső audit igények kivételével). Az IBSZ megfelelési vizsgálatot az IIG igazgatója vagy a rendszert üzemeltető szervezeti egység vezetője (üzemeltető osztály vezetője) kezdeményezheti.

Az ELTE információbiztonsági vezetője az IIG igazgatója, és ebben a minőségében az osztályértekezletek a döntések fórumai az egyes információbiztonsági védelmi intézkedésekkel kapcsolatban.

### **6.1.3 Az információbiztonsági felelőségek allokációja**

Azon informatikai rendszerek esetében, amiknek nem volt sikeres IBSZ megfelelési vizsgálata, minden negatív biztonsági esemény felelősége az üzemeltető szervezeti egység vezetőjét terheli.

Azon rendszerek esetében, ahol az IBSZ vizsgálat sikeres volt (illetőleg a vizsgálat során készült és elfogadott hiánylistát az üzemeltető pótolta) a negatív biztonsági események felelősége egyedi vizsgálat alapján állapítható meg. Az IBSZ (és annak a rendszerre vonatkozó mellékleteinek) betartása esetén az üzemeltető jóhiszeműnek minősül.

Az IIG szolgáltatásmenedzserének felelősége az információbiztonsági események, incidensek tanulságait és a pozitív példák megjelenítése az IIG szokásos információ csatornáin.

### **6.1.4 Új információ-feldolgozó rendszerek elfogadási eljárása**

Új informatikai szolgáltatás indítási kérelméhez az IT-SZ szerint csatolni kell a rendszer vázlatos leírását és a tervezett SLA-t. Ezen anyagok alapján az IIG igazgatója a szolgáltatás engedélyezése előtt javaslatot kérhet a szolgáltatásmanagertől az IBSZ mellékletek aktualizálására, az új szolgáltatás IBSZ paramétereinek megállapítására. A szolgáltatás indítási kérelem automatikusan az IT-SZ és az IBSZ elfogadási szándéknyilatkozatának tekintendő.

### **6.1.5 Bizalmassági nyilatkozatok**

Az információbiztonsági szabályok betartásával és betartatásával kapcsolatban a 3. számú mellékletben részletezett bizalmassági nyilatkozatot írnak alá az A és B osztályú rendszerek üzemeltetői, illetve abban az esetben a felhasználók is, amennyiben erről az adott rendszer SLA-ja erről külön rendelkezik. Ugyanezt teszik az ELTE üzleti partnerei is a 4. számú mellékletben részletezett titoktartási nyilatkozat kitöltésével és aláírásával.

A rendszer üzemeltetői a rendszer üzemeltetése során különféle személyes, illetőleg bizalmas adatokhoz férnek hozzá. Ezen adatok védelméről gondoskodni kell.

A munkavégzés során a munkavégzők részére átadott, illetve tudomásukra jutott információkat védeni kell.

Minden bizalmassági kérdésben érintett szereplővel bizalmassági nyilatkozatot kell kitölteni, melynek aláírásával felvállalja, hogy a birtokában levő információval nem él vissza.

### **6.1.6 Kapcsolattartás hatóságokkal**

A különböző törvényekben és rendeletekben előírt információbiztonsági adatszolgáltatási kötelezettség teljesítése az IIG igazgatójának felelősége. Az ELTE illetve az IIG jogi képviselőt nem lát el az egyének jogvitáiban a hatóságokkal.

### **6.1.7 Kapcsolattartás különleges érdekközösségekkel**

Az ELTE IIG igazgatója felelős a kapcsolattartásért a különleges érdekközösségekkel, mint például a Magyar non-profit internet használók közössége (Hungarnet). Minden hivatalos tagsági és kapcsolattartási kérdésben az ELTE érdekeinek figyelembe vételével az IIG igazgatója dönt.

A felhasználók egyéni tagságai (pl. ISACA, IVSZ stb.) az adott személy felelősége. Egyéni tagként is köteles a kapcsolattartás során az IBSZ vonatkozatható előírásait betartani.



### **6.1.8 Az információbiztonság független felülvizsgálata**

Mivel az ELTE Belső Ellenőrzési Osztálya információbiztonsági vizsgálatot nem végez, ezt az funkciót az IIG szolgáltatásmanageré látja el. A független audit szükségességéről és módjáról esetileg az IIG igazgatója dönt, az A osztályú rendszerek esetén 3 évente javasolt.

## **6.2 Külső felek**

### **6.2.1 A külső felekhez, partnerekhez kapcsolódó kockázatok azonosítása**

A külső felekkel, partnerekkel való kapcsolattartás szabályai:

- Személyes vagy intézményi adatok kiadása, csak a hatályos jogszabályoknak megfelelően történhet.
- Az átadott adatok védelméért a szerződő fél tartozik felelősséggel.
- A kapcsolattartó tanácsot kérhet a szolgáltatás menedzsertől adatvédelmi és információbiztonsági kérdésekben.

### **6.2.2 Ügyfelekkel kapcsolatos információbiztonsági feladatok (jogosultság kiadás felhasználóknak)**

Az IT-SZ szerinti A,B és C osztályú rendszerek esetében az installálási időszakon kívüli partner hozzáférést az üzemeltetők eseti kérelme alapján az IIG igazgatója vagy az általa megbízott felelős engedélyezheti. A kérelemnek tartalmaznia kell az ügyfél adatait, a hozzáférés indokát, módját, paramétereit és tervezett időtartamát. Engedély nélküli hozzáférés biztosítása esetén az adott informatikai rendszer nem minősül IBSZ megfelelőnek.

### **6.2.3 Harmadik féllel kötött megállapodások biztonsági kérdései**

Minden harmadik féllel kötött megállapodás esetében a megállapodásban rögzítendőek az adatvédelmi és az információbiztonsági kérdések.

## **7 Az információvagyon menedzsmentje**

### **7.1 Felelősség az információvagyonért**

#### **7.1.1 Információs vagyon leltár**

Az információs vagyon az IT-SZ alapján készített üzemeltetési dokumentációkban leírtak alapján meghatározott.

Az intézmény IT-SZ szerinti A, B és C kategóriájú rendszereinek nyilvántartását és az általuk biztosított szolgáltatások paramétereinek nyilvántartását az IIG szolgáltatásmenedzsere végzi. Az ehhez szükséges adatszolgáltatás a rendszerek üzemeltetőinek IT-SZ-ből fakadó kötelezettsége.

#### **7.1.2 Az információs vagyon tulajdonjoga**

Az intézmény IT-SZ szerinti A, B és C kategóriájú rendszereinek intézmény-specifikus konfigurációs adatai és beállításai (minden olyan konfigurációs komponens, ami a vásárolt rendszerben található állapottól eltér) az intézmény tulajdonát képezi. Ugyanezen rendszerekben tárolt minden intézményi adat (és annak minden felhasználási joga) az intézmény tulajdonát képezi.

### **7.1.3 Az információs vagyon használatának szabályai**

Minden alkalmazott és üzleti partner a számára meghatározott jogosultsággal léphet be a különböző rendszerekbe. A jogosultság változását az alkalmazottak esetében a felettesnél, üzleti partner esetében a megbízó szervezeti egység vezetőjénél kell kezdeményezni.

Az SLA-k rögzítik az egyes szolgáltatásokkal kapcsolatos információvagyon és jogosultságkezelési és használati szabályokat. Minden fajta változtatás az SLA-k változtatási rendjének megfelelően végezhető. (Lásd IT-SZ).

Adatok kiadása a különböző biztonsági osztályba sorolt rendszerekből csak az adott szervezeti egység vezetőjének engedélyével lehetséges, kivételt ez alól az az eset képez, amikor az adatcserét, adatátadást vállalkozói szerződés rögzíti. Ebben az esetben a szerződésnek tartalmaznia kell az adatkezelésre vonatkozó szabályokat.

## **7.2 Az információvagyon osztályozása**

### **7.2.1 Az osztályozás elvei, vezérfonala**

Az információvédelem területén történő osztályozás az adatok minősítési szintjével növekvő mértékű, a bizalmasság, hitelesség és a sértetlenség sérüléséből vagy elvesztéséből származó kárszinteken alapul.

- **Információvédelmi alapbiztonsági osztály:**  
Személyes adatok, üzleti titkok, pénzügyi adatok, illetve az intézmény belső szabályozásában hozzáférés-korlátozás alá eső (pl. egyes feladatok végrehajtása érdekében bizalmas) és a nyílt adatok feldolgozására, tárolására alkalmas rendszer biztonsági osztálya.
- **Információvédelmi fokozott biztonsági osztály:**  
A szolgálati titok, valamint a nem minősített adatok közül a különleges személyes adatok, nagy tömegű személyes adatok, közepes értékű üzleti titkok feldolgozására, tárolására is alkalmas rendszer biztonsági osztálya.
- **Információvédelmi kiemelt biztonsági osztály:**  
Az államtitok, a katonai szolgálati titok, valamint a nem minősített adatok közül a nagy tömegű különleges személyes adatok és nagy értékű üzleti titkok feldolgozására, tárolására alkalmas rendszer biztonsági osztálya.

### **7.2.2 Az osztályba sorolt információs vagyonelemek jelölése és kezelése**

Az információs vagyonelemek besorolása, jelölése az IT-SZ szerint (lásd IT-SZ 5.4 fejezet) történik és a végrehajtásáért a szolgáltatás menedzser a felelős.

## **8 Emberi erőforrással kapcsolatos biztonsági kérdések**

### **8.1 *Alkalmazás előtti tennivalók (szerepek és felelőségek, „átvilágítás”, alkalmazási feltételek)***

Az ELTE-n a felvételt központilag a személyügyi előadó végzi. Erkölcsi bizonyítvány szükséges az A, B és C rendszerek üzemeltetői és fejlesztői esetében.

### **8.2 *Az alkalmazás alatti tennivalók (felelőségek menedzsmentje, információbiztonsági képzések és tréningek, fegyelmi ügyek)***

Az A, B és C kategóriájú rendszerek esetében minden üzemeltető, fejlesztő vagy felhasználó csak a munkakörének ellátásához szükséges jogosultságokat birtokolhatja. (Azon fejlesztői rendszerek, amik személyes vagy intézményi adatokat nem tartalmaznak, nem minősülnek kategorizált rendszernek.)

Az A és B osztályú rendszerek bizonyos szolgáltatásainak igénybevételéhez (pl. gazdasági rendszer) az IIG igazgatója tanfolyam és/vagy vizsga teljesítését írhatja elő. A kritériumok teljesítésének költsége az intézményt terheli.

Az IBSZ előírásainak szándékos és tudatos megsértése esetén az alkalmazott az ELTE vonatkozó előírásainak megfelelően szankcionálható.

### **8.3 *Elbocsátás vagy munkakör-változás (elbocsátási felelőségek, dolgozónak kiadott eszközök visszavétele, hozzáférési jogok megvonása)***

A dolgozó elbocsátása esetén minden A, B és C kategóriájú rendszer esetében az üzemeltetői és fejlesztői jogosultságokat, ilyen tevékenységet lehetővé tevő belépési kódokat azonnal vissza kell vonni, amit az adott szolgáltatás vezetőjének kell kezdeményeznie. Amennyiben a volt dolgozó a fenti tevékenységeket céges partnerként végzi a továbbiakban, akkor a szerződés megkötése után új, partneri hozzáférés biztosítható számára az ott részletezett szabályok alapján.

Az elbocsátott dolgozó a C és D kategóriájú rendszerekben a (kizárólag) személyes adatainak elérésére szolgáló belépési kódjait az üzemeltető eseti engedélye alapján megtarthatja.

## **9 Fizikai és környezeti biztonság**

### **9.1 *Biztonsági zónák, területek***

#### **9.1.1 *Fizikai biztonsági határvédelem***

A, B kategóriájú szolgáltató rendszer kritikus fizikai komponensei (szerver, tároló alrendszer, router, stb.) csak külön erre a célra kialakított, megfelelő biztonsági paraméterekkel rendelkező helyiségekben működtethetők. A helyiségeknek mechanikai nyitórendszerrel (biztonsági zár vagy beléptető kártyával működtethető mágneses zár) és beléptető rendszerrel kell rendelkezniük. A beléptető rendszer szükséges alapfunkciói: belépő személy azonosítása kód vagy kártya alapján, belépési jogosultság megállapítása, belépési időpont regisztrálása, jogosulatlan belépés jelzése a biztonsági személyzet felé. A C kategóriájú rendszerek esetében minimálisan biztonsági zárral ellátott helyiséget kell biztosítani, a kulcsokról és a belépésről írásos helyiségnaplót kell vezetni.

### **9.1.2 Fizikai belépési szabályozás**

Az A, és B kategóriájú rendszerek komponenseit tartalmazó szolgáltató helyiségekbe (gépterem, kábelrendezők) való belépési jogosultságot az IIG igazgatója, C kategóriájú rendszer esetében az üzemeltető szervezeti egység vezetője engedélyezi a dolgozónak vagy a partnernek a helyiségek és a végezhető tevékenységek felsorolásával. A belépési lehetőséggel rendelkezők ezen jogosultságukat nem ruházhatják át másik dolgozóra vagy partnerre. Jogosulatlan személy beengedéséből fakadó eseményekért a felelősség a beengedő személyt terheli. Az illegálisan szerzett belépési lehetőség használata betörésnek minősül és jogi következményeket von maga után.

### **9.1.3 Irodák, szobák és egyéb létesítmények fizikai biztonsága**

Az informatikai rendszerek működtetéséhez szükséges egyéb munkaterületek használatának módja megegyezik az általános egyetemi területek használati módjával. Kitüntetett hozzáférést vagy védett adatokat tartalmazó kiegészítő rendszerkomponensek (mentési berendezés, fejlesztői rendszer, felügyelő terminál, stb.) csak beléptető rendszerrel védett munkaszobában és irodában helyezhető el.

Az informatikai célú helyiségekkel kapcsolatos kérdésekben a gépterem vezető technikus a felelős a ki- és az átalakítás és koordinációjáért, a szakmai a biztonsági szempontok betartásáért.

### **9.1.4 Külső és környezeti károk elleni védelem**

A, B és C kategóriájú szolgáltató rendszer kritikus fizikai komponensei csak a hatályos szabályozásnak megfelelő tűz- és villámvédelmi rendszerrel felszerelt helyiségekben üzemeltethetők. Talajszinten vagy az alatt elhelyezkedő helyiségek esetében az ár- és belvízvédelmi szabályozásnak is meg kell felelni.

Egyedi esetben az IIG igazgatója egyéb előírásokat is megfogalmazhat.

A tűzvédelmi rendelkezéseknek megfelelően az erősáramú ellátó rendszernek tartalmaznia kell olyan központi áramtalanítókapcsolót, ami tűzjelzés esetén a biztonságos oltás feltételeit megteremti. A megfelelőségről a gépterem vezető technikus köteles gondoskodni.

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

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

### **9.1.5 Munkavégzés biztonsági zónákban**

A minősített rendszereket tartalmazó helyiségekben minden olyan munkavégzés, ami az informatikai rendszereket vagy azok működését veszélyeztetheti, csak előzetes egyeztetés alapján, felügyelet mellett végezhető. Az egyeztetést a munkavégző cég és az üzemeltető szervezeti egység vezetője végzi, az IIG gépteremvezető technikusának szervezésében és lebonyolításával. A helyiség gépészeti berendezését veszélyeztető munkák csak a gépteremvezető technikus előzetes engedélyével folytathatók.

### **9.1.6 Nyilvános hozzáférés, szállítási és töltési területek**

A minősített rendszereket tartalmazó helyiségekben minden szállítási tevékenység csak belépésre jogosult munkatárs felügyelete mellett végezhető.

## **9.2 Eszköz biztonság**

### **9.2.1 Eszközök elhelyezése, védelme**

Minden minősített rendszerkomponens fizikai elhelyezésénél törekedni kell a gépterem / kábelrendező felépítési elveinek betartására (pl. rackben történő elhelyezésre, megfelelő ventilációs irányra, stb.) Ezen irányelveket új komponens beszerzése esetén az IIG előírhatja.

### **9.2.2 Támogató közművek (szolgáltatások)**

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

### **9.2.3 Kábelbiztonság**

A kiemelt rendszerek védett helyiségen kívül húzódó, összekötő komponenseit (telefon és gerinchálózati kábeleket) tartalmazó ELTE tulajdonú alépítmények, kábelaknák és védőcsövek IIG által felügyelt területnek minősülnek. Azokban munkát végezni, vagy a megközelíthetőségüket korlátozni csak a rendszerkomponens üzemeltetőjének előzetes engedélyével lehet.

### **9.2.4 Eszközkarbantartás**

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

A Gépészet külön karbantartási tervvel rendelkezik.

A karbantartás során a felmerült biztonsági sérülékenységeket megfelelően kell kezelni, illetve úgy kell a karbantartásokat elvégezni, hogy újabb biztonsági kockázatok ne merüljenek fel. Ennek felelőse a karbantartást végrehajtó személy vagy szervezet.

### **9.2.5 Telephelyen kívül használt eszközök biztonsági szabályai**

A telephelyekről kivitt eszközök használata során bekövetkező károkért (adatvesztés, adatszivárgás) az a személy viseli a felelősséget aki az eszközt kivitte. A telephelyen kívüli használat során mindazon elvek és gyakorlat követendő, amelyeket az IBSZ egyes fejezetei leírnak.

### **9.2.6 Eszközök biztonságos megsemmisítése vagy újrahasznosítása**

A használt eszközök selejtezése a ELTE hatályos szabályainak figyelembevételével történik. Speciális eszközök selejtezése esetén az üzemeltető gondoskodik a szakszerű elhelyezésről, illetve átadás-átvételi jegyzőkönyv alapján ezt a tárolási/elszállítási feladatot átadhatja az

ELTE selejtezési csoportjának. „A”, „B” és „C” kategóriás eszközök selejtezésénél gondoskodni kell az azon tárolt adatok selejtezés előtti fizikai megsemmisítéséről.

### **9.2.7 Eszközök (HW, SW) kivitele telephelyről**

Az eszközök ki/be szállítását szállítólevéllel kell kísélni, amin az eszköz(ök) egyedi azonosítóját (ha értelmezhető) fel kell tüntetni.

## **10 Kommunikáció és üzemelés menedzsment**

### **10.1 Működési folyamatok és felelőségek**

Amennyiben egy szervezeti egység szolgáltatás-indítási kérelemmel fordul az IIG igazgatójához, ezzel elismeri megfelelési szándékát az ELTE IT-SZ és IBSZ kritériumainak. A szolgáltatás-indítási kérelem csak adathiány és IT-SZ vagy IBSZ sértés esetén utasítható el. Az elutasítást részletesen indokolnia kell az IIG igazgatójának, nem kizárva az esetleges módosított újbóli kérelem beadását.

Minősített (IT-SZ A, B ill. C osztályú rendszerek) esetében az IT-SZ és IBSZ megfelelést az IIG esetileg vizsgálhatja és az esetleges hiánypótlásra az üzemeltetőt felszólíthatja. Amennyiben a vizsgált informatikai rendszer maga is más informatikai szolgáltatásokat használ, úgy a használt szolgáltatás SLA-ja is vonatkozik rá.

Minden informatikai rendszer esetében a használatra vonatkozó igény bejelentése (hozzáférés vagy felhasználói azonosító igénylése) a szolgáltatási SLA elfogadásának szándéknyilatkozatát is jelenti. A hozzáférés megadásával az SLA a szolgáltató és az igénybevevő között életbe lép.

Az IT-SZ szerinti A és B osztályú rendszerek esetében az SLA-ban vállalt szolgáltatási és rendelkezésre állási paraméterek alulteljesítése miatt az intézményt anyagi és egyéb kár érheti. Ilyen esetekben a felelősség megállapítására és a szükséges lépések megtételére (rendszer-módosítás, szabályzat-módosítás) az IIG igazgatója eseti bizottságot nevezhet ki. Ezen bizottságnak mindig tagja az IIG szolgáltatásmanager.

### **10.2 Harmadik fél által nyújtott szolgáltatások menedzsmentje**

A harmadik fél által nyújtott informatikai szolgáltatások is SLA kötelezettek, a kritikus paramétereket a partnerrel kötött szolgáltatási szerződésben is rögzíteni kell. A szerződésnek ki kell terjednie az információbiztonsági és adatbiztonsági kérdésekre is.

Az SZMSZ-ben meghatározott IIG kompetenciák (IT szolgáltatások) esetében az ELTE egykapus ügyintézés és érdekképviselőt alkalmaz. Ezen szolgáltatók esetében az ügyfélkapcsolatra és szerződéskötésre jogosult ELTE szervezeti egység az IIG.

### **10.3 Rendszertervezés és elfogadás**

Az informatikai szolgáltató rendszerek esetében az IT-SZ és IBSZ megfelelést már a tervezési szempontok között szerepeltetni kell. Az IIG által üzemeltetni tervezett A, B és C osztályú rendszerek esetében az IT-SZ és IBSZ megfelelés a szolgáltatás indításának szükséges feltétele. Az ELTE informatikai rendszerei esetében a szolgáltatás megindítását az IIG igazgatója engedélyezi a szolgáltatásmenedzser javaslata alapján.

#### **10.4 Védekezés vírusok és egyéb kártékony kódok ellen**

Azon rendszerek esetében, ahol a kártékony és mobil kódok előfordulhatnak, a detektálásukat és elhárításukat végző komponensek installálása a szolgáltatási engedély kiadásának feltétele. Minden olyan rendszer esetében, ahol vírusfenyegetés fennáll és lehetséges installálni vírusvédelmi rendszert, valamint a kémprogram jelző komponenst, akkor ott az a szolgáltatás üzembe helyezésének és üzemeltetésének feltétele.

Publikus levelező rendszerek esetében az intézményen kívüli kapcsolat létesítésének feltétele a levelek informatikailag veszélyes tartalmának vizsgálati képessége illetőleg az „open relay” lehetőség kiküszöbölése.

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

#### **10.5 Biztonsági mentések**

Minden A, B és C osztályú szolgáltató rendszer üzemeltetési leírásának tartalmaznia kell az alkalmazások és adatok mentési rendjét (a mentendő adatok körét, a mentés módját és gyakoriságát, és a mentésért felelős személyt, a mentés tárolási rendjét, mentés külső tárolásának rendje).

A és B osztályú rendszerek esetén külső tárolású (offsite) mentésekkel is kell rendelkezni, C és D osztályú rendszerek esetén onsite mentések is elfogadhatóak.

A mentési rendnek az alkalmazásra vonatkozó részét úgy kell megállapítani, hogy a rendszer működőképessége tetszőleges komponens meghibásodása vagy adatvesztése esetén helyreállítható legyen (új hardware biztosítása esetén). Ennek érdekében az alkalmazás futó kódját legalább minden release váltás előtt és után menteni kell, a mentést minimum 3 release-re vagy egy évre visszamenőleg meg kell őrizni.

Az alkalmazások és rendszerek konfigurációs beállításait minden változás esetén, de leggyakrabban naponta kell menteni. A mentési eljárásnak lehetővé kell tennie egy adott konfigurációs állapot célirányos betöltését. A konfigurációs mentéseknek 10 előző állapotra ill. minimum az előző 30 szolgáltatási napra ki kell terjedniük.

Az A osztályú rendszerek esetében az alkalmazásokban tárolt intézményi adatokat minden munkanap végén teljes egészében menteni kell. A mentési módnak lehetővé kell tennie ezen adatok tesztrendszerbe történő betöltését. A C osztályú rendszerek esetében a személyi adatok inkrementális mentése is megengedett eljárás. A teljes adatpark mentése 30 naponta javasolt. Az alkalmazás üzemeltető rendszergazdája belátása szerint bármikor jogosult eseti mentés indítására.

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

#### **10.6 Hálózatbiztonság menedzsmentje**

Az intézmény teljes területére kiterjedő alpinfrastruktúra (számítógépes és telefonhálózat) védelme egységes koncepció és megvalósítás mellett történik. Az irányelvek és módszerek meghatározását és a szükséges operatív beavatkozásokat a telekommunikációs hálózat üzemeltetésével megbízott IIG szervezeti egység végzi. A kommunikációs hálózathoz való

csatlakozás feltétele a (csatlakozás módjától és a csatlakoztatott rendszertől függő) biztonsági előírások maradéktalan betartása. Ezen előírások a csatlakozásnak, mint szolgáltatásnak az igénybevételi feltételei között tekinthetők meg (lásd a vonatkozó SLA-kat).

### **10.7 Média kezelés**

Az A és C osztályú rendszerek adatterületeinek mentései jogvédelem alá első intézményi és személyes adatokat tartalmazhatnak. Ezen adathordozókat olyan körültekintéssel kell tárolni és kezelni, mint magát az adatot tároló rendszert.

A mentések tárolása: Az A és B osztályú rendszerek mentéseinek tárolása az IIG által kijelölt és jóváhagyott védett helyiségben történik. A médiáról nyilvántartást kell vezetni.

Mentések adathordozóinak használatból való kivonása és megsemmisítése (pl. demagnetizálás) a szolgáltatást üzemeltető feladata. A média megsemmisítésről jegyzőkönyvet kell felvenni.

### **10.8 Információcsere**

Az intézmény A, B és C osztályú rendszerei esetében az automatikus adatcserét lehetővé tevő kapcsolatok létesítéséhez IIG igazgatói engedély és az érintett adatgazdák hozzájárulása szükséges. A kérelemben az alkalmazások üzemeltetőinek részletezniük kell az elérendő adatkezelési célt és az alkalmazott informatikai megoldást, különös tekintettel a jogosulatlan adatcserét kizáró biztonsági megoldásokra.

Az adatcsere környezetét, technológiai megvalósítását dokumentálnia kell az adatcserét kezdeményező alkalmazásüzemeltetőnek.

### **10.9 Elektronikus kereskedelem**

Az elektronikus kereskedelmet lehetővé tevő alkalmazások esetében a biztonsági feltételek megteremtése érdekében az IIG igazgatójának engedélye szükséges a rendszer működtetéséhez.

Az alkalmazás tervezésébe és megvalósításába be kell vonni az IIG igazgatóját vagy annak kijelölt képviselőjét.

### **10.10 Monitorozás**

Az A és B osztályú rendszerek esetében az üzemeltetők felelőssége az automatikus szolgáltatás monitorozó komponensek bevezetési lehetőségének vizsgálata és a monitorozás megvalósítása.

## **11 Hozzáférés szabályozás**

### **11.1 Működési követelmények a hozzáférés szabályozása érdekében (hozzáférési politika)**

Minden olyan informatikai rendszer esetében, ami az intézmény működéséhez szükséges, illetőleg bármilyen védett (intézményi, magán, kutatási, jogvédett, stb. információt tartalmaz, meg kell határozni a hozzáférésre jogosultak körét és hozzáférési kísérlet esetén a jogosultságot ellenőrizni kell. Informatikai rendszerhez való, módosítást és védett adatok lekérdezését lehetővé tevő hozzáférésre kizárólag másik rendszer és természetes személy lehet jogosult. Természetes személyek egy csoportja (szervezeti egység dolgozói, cégek, stb. közös használatú hozzáférési lehetőséget kizárólag publikus adatok lekérdezésére birtokolhatnak.



A jogosultság kezelést napra készen kell tartani és dokumentálni.

### ***11.2 Felhasználói hozzáférés menedzsmentje***

Az adott informatikai rendszerhez történő hozzáférés módját (igénybe vételre jogosultak köre, igénylés módja, igénylés elbírálása) a rendszeren működő szolgáltatások SLA-i tartalmazzák. Az igénylés során a természetes személynek azonosítania kell magát egyedi adatával vagy adat-párjával. (pl. ELTE id, ETR id). Lehetőség szerint az informatikai rendszerek felhasználóinak azonosítása és jogosultság-elbírálása központilag, erre a célra szolgáló rendszerekkel történjen (pl. LDAP, Kerberos) és a felhasználói adatbázis kezelése egységesen és konzisztensen valósuljon meg. Kivételt azon már meglévő és működő rendszerek képezik, melyek nem képesek központi jogosultságkezelést megvalósítani.

A szolgáltatási SLA megszegése esetén a felhasználó az adott szolgáltatásból kizárható. Kizárás esetén a felhasználót ennek tényéről, a kizárás időtartamáról, a problémát okozó tevékenységről és a követendő magatartásról tájékoztatni kell. Ha a felhasználó tevékenysége által okozott kár csekély, akkor törekedni kell az előzetes figyelmeztetésre vagy a letiltás előtti tájékoztatásra.

Az A és B osztályú rendszerek esetében az üzemeltető a hozzáférésre jogosultak esetében is előírhat engedélyezési eljárást (pl. a kérelmező munkáltatója által) a hozzáférés megadásához. Az engedélyt írásban, a kért jogosultságokat feltüntetve kell az üzemeltetőknek eljuttatni. Minden A, B és C osztályú rendszer esetében az üzemeltető feladata, hogy a kiadott hozzáférések adatait (név, alkalmazás, jogosultsági szint, kiadás dátuma, indoka) naprakészen nyilvántartsa.

A hozzáférés indokának megszűnése esetén az üzemeltetőnek a hozzáférést haladéktalanul vissza kell vonnia az SLA-ban dokumentált módon.

### ***11.3 Felhasználói felelősségek***

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

Az A osztályú rendszerek felhasználója munkaköri felelősség keretében kezelheti az intézményi adatokat, azok bizalmas kezelése munkaköri kötelessége. Az intézményi rendszert köteles csak a munkakörének megfelelően, erőforrás-kímélő módon, a kezelési utasításoknak megfelelően használni.

### ***11.4 Hálózati hozzáférés***

A számítógépes hálózatra történő fizikai csatlakozás csak az üzemeltető által elfogadott igénylés után, az abban megadott paraméterekkel lehetséges. A jogosulatlan csatlakozást az üzemeltető a rendszer integritásának védelmében azonnal megszüntetheti. A csatlakozási lehetőségeket és az igénylés módját a hálózati szolgáltatások SLA-i tartalmazzák.

A hálózati szolgáltatások SLA-iban szereplő feltételrendszer az üzembiztonság, nyomon követhetőség és központi kezelhetőség szempontjai szerint van kialakítva, ezért az SLA be nem tartása a rendszer egészét, a többi felhasználó szolgáltatási környezetét veszélyezteti. Emiatt az SLA-t megszegő felhasználó a hálózati szolgáltatásokból utólagos figyelmeztetés mellett is kizárható.

Az Internet bármely komponenséhez történő hozzáférés esetén a felhasználó köteles az egyetem Internet-szolgáltatójának szabályzatát is betartani, valamint az Internet közösség etikai irányelveit, mások vallási, politikai és erkölcsi nézeteit tiszteletben tartani.

### **11.5 Operációs rendszer hozzáférés**

Az SLA köteles operációs rendszerekben a felhasználók kizárólag egyértelmű azonosítás után végezhetnek munkát. A hozzáférés tényét, időtartamát és forrását a rendszernek visszakereshető módon naplózni kell az SLA-ban meghatározottak szerint, illetve minimum 1 hónapig.

### **11.6 Alkalmazásokhoz és információkhoz való hozzáférés szabályozása**

Az intézményi adatokhoz való hozzáférést lehetővé tevő alkalmazások jogosultsági köreit olyan módon kell kialakítani, hogy az alkalmazottak csak a munkakörükkel kapcsolatos adatokat láthassák, illetve kezelhessék. Az intézményi adatokhoz történő hozzáférést, ezen adatok módosítását alkalmazás szinten is – visszakereshető módon - naplózni kell minimum 1 hónapra visszamenőleg.

Minden A és C osztályú rendszer esetén a személyes adatokat kizárólag az adatot birtokló természetes személy, mint felhasználó láthatja. Ez alól csak a rendszer üzemeltetését ellátó és a mentéseket készítő üzemeltetői azonosítók jelentenek kivételt. A felhasználónak ezen adatok publikálásához tevőlegesen meg kell változtatnia a publikálandó adatok jogosultságát.

### **11.7 Mobil számítógép használat és telefonos munkavégzés**

Az A osztályú rendszerekhez történő tetszőleges, illetőleg a B osztályú rendszerekhez történő menedzsment hozzáférés kizárólag az intézményi belső hálózathoz (intranet) lehetséges. A C osztályú rendszerek menedzsment hozzáférése megfelelő titkosítással bíró adatkapcsolattal külső hálózathoz is megengedett. Minden egyéb hozzáférési kísérlet incidensnek minősül és informatikai megoldásokkal is akadályozható az üzemeltetők részéről.

Speciális hálózati szolgáltatásokkal (pl. VPN) az intranet az intézmény fizikai hálózatán kívülre is meghosszabbítható, ezáltal a munkahelyen kívüli munkavégzés lehetséges. Ezen megoldások (a hálózati SLA megsértésével járó) önerős megvalósítása nem megengedett, kizárólag az IIG 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.

## **12 Információs rendszerek beszerzése, fejlesztése és karbantartása**

### **12.1 Információs rendszerek biztonsági követelményei**

Új rendszerek megvalósítása során a biztonsági követelményeket előzetesen meg kell határozni, és a szolgáltatás indítási kérelemhez mellékelni kell.

A már működő rendszerek továbbfejlesztése, módosítása során a biztonsági követelmények nem változtathatóak olyan irányba, hogy a rendszer biztonsági szintje csökkenjen.

### **12.2 Alkalmazások helyes használata**

Az A osztályú alkalmazásokhoz kizárólag azon felhasználók férhetnek hozzá, akiknek az intézményi szerepük 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).

### ***12.3 Kriptográfiai szabályozások***

Az A és B osztályú rendszerekbe történő, módosítási jogosultságot is lehetővé tevő bejelentkezés csak titkosított kommunikációval (pl. SSH, SSL, VPN) engedélyezett, kivéve azon bejelentkezési területeket, ahol a felhasználó munkahelye és a szolgáltató rendszer közötti csatorna külső fél általi lehallgatása technikailag nem lehetséges (pl. fizikai védelem miatt).

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

Egyéb kriptográfiai szabályozások az adott szolgáltatás SLA-jában találhatóak.

### ***12.4 Rendszer fájlok biztonsága***

A szolgáltató rendszerek működését biztosító rendszer fájlokhoz a felhasználók csak olyan mértékben férhetnek hozzá, amit a szolgáltatás használata megkövetel. A szolgáltatás szempontjából kritikus rendszer fájlok felhasználók általi módosítása csak az üzembiztonságot ellenőrző köztes felületen keresztül lehetséges.

A rendszer fájlok védelme, az üzembiztos konfiguráció megőrzése és helyreállíthatóságának biztosítása az üzemeltető rendszergazdák munkaköri kötelessége.

### ***12.5 Fejlesztési és támogatási folyamatok biztonsága***

Minden 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 C osztályú rendszernek minősül és a hozzáférési jogosultságok ennek megfelelően adhatók ki.

Intézményi fejlesztésű vagy vásárolt szolgáltató rendszer csak funkcionális teszt után vonható szolgáltató üzembe. A funkcionális tesztnek az SLA-ban rögzített minden paraméterre és funkcióra, valamint a tipikus felhasználási mintákra kell kiterjednie. A funkcionális tesztről írásos jegyzőkönyvnek kell készülnie, melynek az összes mért és ellenőrzött paramétert és funkciót tartalmaznia kell.

Minden, a szolgáltatási felületen vagy a funkciókészletben különbséget tartalmazó alkalmazás verzió esetén a tesztelési eljárást újra el kell végezni. A tesztelési kötelezettség az operációs rendszerek, adatbázis kezelők és egyéb támogató alkalmazások (pl. web szerver) esetén is fennáll, de csak a használt funkciókra kell kiterjednie.

Szolgáltató üzemben működő alkalmazáson csak sikeres tesztelési jegyzőkönyv birtokában és az üzemeltető rendszergazda engedélyével végezhető változtatás (külső munkavégző cég esetében is). Ezen előírás alól csak a szolgáltatás helyreállítását célzó sürgős hibajavítás jelent kivételt, ami esetében a dokumentálást utólag kell elvégezni.

### ***12.6 Műszaki sérülékenység menedzsment***

Az adott alkalmazás üzemeltetőjének felelőssége a publikált technikai sérülékenységek elleni védekezés megvalósítása. A publikált sérülékenységek elleni védekező intézkedés (pl. patch-ek és fixek letöltése) az észlelést követő első munkanapon végrehajtandó.

## **13 Információbiztonsági események menedzsmentje**

### **13.1 Biztonsági események és gyengeségek jelentése**

Minden szolgáltató rendszer esetében a szolgáltatás üzemeltetője köteles incidens bejelentési lehetőséget biztosítani a felhasználóknak, és a bejelentés módját az SLA-ban közzétenni. A bejelentett incidenseket az üzemeltetők a szolgáltató rendszer integritásának és a kezelt adatoknak a védelmében kötelesek lehetőség szerint rövid reakcióidővel elbírálni és a szükséges lépéseket (pl. hozzáférés korlátozás, biztonsági komponensek beállításainak módosítása) megtenni. Az üzemeltető köteles a bejelentőt tájékoztatni a biztonsági esemény következményeiről és a megtett intézkedésekről. Tömeges érintettség esetén lehetőség van az IIG központi tájékoztató csatornáinak használatára is.

Biztonsági esemény vagy gyengeség bejelentése esetén a bejelentő köteles csatolni mindazon adatokat, amik az esemény megítéléséhez legjobb tudása szerint szükségesek (pl. időpont, tapasztalt jelenség, log file részlet, stb.)

A szolgáltatások felhasználása közben tapasztalt biztonsági gyengeségek jelentése (a rendszer működőképességének fenntarthatósága érdekében) minden felhasználónak kötelessége. Ennek elmulasztása vagy a gyengeség kihasználása biztonsági eseménynek minősül.

### **13.2 Információbiztonsági események és fejlesztések menedzsmentje**

Az informatikai szolgáltató rendszerek esetében egyenszilárdságú biztonsági megoldásokat kell kialakítani. Rendszerenként egységes tervezés és megvalósítás alapján kell a biztonsági megoldásokat kezelni. Amennyiben egy informatikai rendszer egy másik szolgáltatását igénybe veszi, akkor a szolgáltatási SLA biztonsági követelményei az igénybevevő rendszer egészére vonatkoznak.

A megvalósítandó vagy üzemben álló szolgáltató rendszer rendszertervének az alkalmazott és 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.

## **14 Működés-folytonosság biztosítása**

### **14.1 A működés folytonosság információbiztonsági vetülete**

Az intézmény működése szempontjából kritikus, A és B osztályú rendszerek működés-folytonosságának biztosítása az üzemeltető feladata. Ez kiterjed az SLA-k feltételrendszerének körültekintő meghatározására, a felelős incidenskezelésre, a szükséges funkcionális és biztonsági javítások telepítésére és az IBSZ betartására, valamint a rendszer fejlesztési terveinek erőforrás-kalkuláción alapuló körültekintő elkészítésére.

## **15 Megfelelőség**

### **15.1 Jogszabályi megfelelés**

Az ELTE IIG igazgatójának felelőssége a mindenkori jogszabályi megfelelés biztosítása a nyújtott szolgáltatások vonatkozásában.

Az IIG igazgatója értelemszerűen nem felel a felhasználók által elkövetett jogsértésekért (pl. jogosulatlan adatkezelés, szerzői jogokkal való visszaélés stb.), és hatósági megkeresés esetén a jogszabályban előírt adatokat az adott felhasználóval kapcsolatban kiadhatja.

Az információbiztonság témakörében érvényes legfontosabb jogszabályok jegyzékét a 6. számú melléklet tartalmazza.

### ***15.2 Megfelelés biztonsági politikának, szabványoknak és műszaki előírásoknak***

Az ELTE IIG igazgatójának felelőssége a mindenkori biztonsági politikának, szabványoknak és műszaki előírásoknak való megfelelés biztosítása a nyújtott szolgáltatások vonatkozásában.

Az információbiztonság témakörében érvényes legfontosabb szabványoknak és műszaki leírásoknak a jegyzékét a 6. számú melléklet tartalmazza.

### ***15.3 Információs rendszerek felülvizsgálatával kapcsolatos megfontolások***

Az IT-SZ-szel összhangban az IIG igazgatója felelős azért, hogy az IT-rendszerek teljes körű belső biztonsági felülvizsgálata dokumentált módon (belső felülvizsgálati jelentés) legalább évente megtörténjen, és legalább háromévente sor kerüljön külső, harmadik fél általi felülvizsgálatra az „A” osztályú rendszerek esetében.

Súlyos SLA sértés esetén az IIG igazgatója külön rendkívüli biztonsági ellenőrzést és felülvizsgálatot rendelhet el.

A felülvizsgálatok eredményei alapján az IIG igazgatója rendel el javító, helyesbítő és megelőző intézkedéseket, melyeket mindig a soron következő belső vagy külső, harmadik fél általi felülvizsgálat során kell dokumentált módon visszaellenőrizni.

## 16 Fogalmak, rövidítések

**ELTE:** Eötvös Loránd Tudományegyetem

**IIG:** Gazdasági és Műszaki Főigazgatóság Informatikai Igazgatósága

<sup>2</sup>**Adatvédelem** Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény hatálya alá eső adatkör védelme. Az IBSz az adatvédelem fogalmát a továbbiakban ebben az értelemben fogja használni.

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

**Informatikai biztonsági ajánlások** Jelen szabályzatban az Informatikai Biztonságpolitika alapján az Európai Közösség ITSEC3, valamint a logikai védelem szempontjából ezzel harmonizáló Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottsága 12. számú ajánlása (továbbiakban: MeH ITB 12. ajánlás) meghatározó jellegű.

Az ITSEC az informatikai rendszerek logikai védelmével kapcsolatos funkcionális, valamint az informatikai termékek és rendszerek egységes szemléletű minősítési követelményeit írja le biztonsági osztályonként.

A MeH ITB 12. ajánlása az informatikai rendszerek fizikai, logikai és adminisztratív védelmi követelményeit és az ezek alapján foganatosítandó védelmi intézkedéseket írja le.

Fontos ajánlás az Egyesült Államok Védelmi Minisztériuma által kiadott TCSEC<sup>4</sup> ajánlás, amely az ITSEC alapját képezi.

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

- *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.
- *Zárt* a védelem, ha az összes releváns fenyegetést figyelembe lett véve a védelmi intézkedések megtervezésénél és megvalósításánál.
- *Folyamatos* a védelem, ha az időben változó körülmények és viszonyok ellenére is megszakítás nélkül megvalósul a teljes körű, zárt és kockázattal arányos védelem

---

<sup>2</sup> Megállapította az ELTE SzMSz I. kötete, az SzMR és egyes mellékletei módosításáról az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény hatálybalépésére tekintettel című XXXI/2012. (II. 13.) Szen. sz. határozat. Hatályos: 2012. II. 14. napjától.

<sup>3</sup> ITSEC = Information Technology Security Evaluation Criteria (Információtechnológia Biztonsági Értékelési Kritegiumok) az Európai Közösség ajánlása az informatikai rendszerek biztonságának funkcionális és minősítési követelményeire

<sup>4</sup> TCSEC = Trusted Computer System Evaluation Criteria (Biztonságos Számítógépes Rendszerek Értékelési Kritegiumai), az Egyesült Államok Védelmi Minisztériuma által kiadott informatikai biztonsági ajánlás

- *Kockázattal arányos* a védelem, ha kellően nagy időintervallumban a védelem költségei arányosak a potenciális kárértékek összegével és a megvalósított védelmi intézkedések következtében a kockázatok elviselhető mértékűre mérséklődtek

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

*Funkcionalitás:* az informatikai rendszer megfelelő tervezésének és üzemeltetésének köszönhetően az adat tartalmi és formai használhatóságának biztosítása a funkcionális használat követelményeinek megfelelően.

*Információvédelem:* az informatikai rendszerek által kezelt adatok által hordozott információk védelme a bizalmasság, a hitelesség és a sértetlenség sérülése, elvesztése ellen.

Az információvédelem fogalmát jelen szabályzat a továbbiakban ebben az értelemben használja.

Az információvédelem az informatikai biztonság egyik alapterülete.

*Megbízható működés:* az informatikai rendszerek által kezelt adatok által hordozott információk védelme a rendelkezésre állás, és a funkcionalitás sérülése, elvesztése ellen.

A megbízható működés az informatikai biztonság másik alapterülete.

**Informatikai biztonságpolitika** Az ELTE átfogó informatikai biztonságpolitikája minden munkatárs és tisztségviselő számára egységes értelmezésben határozza meg, hogy az informatikai rendszerek által kezelt adatok bizalmasságának, hitelességének, sértetlenségének, rendelkezésre állásának és funkcionalitásának megőrzésével kapcsolatosan a biztonsági struktúrát, az elveket és a követelményeket, amelyek meghatározzák az informatikai biztonsághoz kapcsolódó viszonyukat.

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

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

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

**DRP:** Disaster Recovery Plan – Katasztrófa utáni helyreállítási terv magába foglalja az üzletmenet (működés) szempontjából kritikus adatok, hardver, és szoftver működésének újraindítását természeti vagy ember által okozott katasztrófák esetén.

**BCP:** Business Continuity Plan – Üzletmenet (működés) folytonossági terv az üzletmenet (működés) fenntartása érdekében teendő intézkedések összessége, ha az adott üzleti folyamat vagy alkalmazás végrehajtása, működtetése valamilyen természeti vagy ember által okozott katasztrófa miatt akadályokba ütközik.

**SLA:** Service Level Agreement – Szolgáltatási szint megállapodás egy olyan írásos megállapodás, mely két fél között jön létre: a szolgáltató és a szolgáltatás igénybevevője között. Ez az alapkoncepciója az IT szolgáltatások menedzselésének. Az SLA meghatározza a két fél között nyújtandó szolgáltatás tartalmát és feltételeit-

**ITIL:** Information Technology Infrastructure Library – egy olyan nemzetközileg elfogadott keretrendszer (de facto szabvány), mely a magas szintű IT szolgáltatások nyújtását a „legjobb gyakorlatok gyűjteménye” elv mentén szabályozza. Az ITIL olyan üzleti (működési) folyamatokat ír le, melyek mind a minőségi mind a gazdaságos szolgáltatás elérését támogatja az informatika területén.

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

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

Budapest, 2007. május 7.

Dr. Hudecz Ferenc  
rektor



## 17 Mellékletek

### 1. IBSZ változáskezelési lap

.....

#### Fejléc adatok:

Benyújtó neve:

Beosztása:

Elérhetősége:

e-mail:

telefon:

Benyújtás dátuma:

Aláírás:

.....

A változtatni kívánt IBSZ bekezdés száma, megnevezése:

A változtatás rövid indoklása:

A javasolt új szövegrész:

.....

#### IIG tölti ki

Beérkezés időpontja:

Átvevő:

Az igény vizsgálatával kapcsolatos megjegyzések:

Az igény elbírálása: Bekerül a dokumentumba a változtatás

NEM kerül be a dokumentumba a változtatás

Indoklás:

Aláírás:

## *2. Felhasználói nyilatkozat*

Mint az egyetem által nyújtott szolgáltatás felhasználója kijelentem, hogy az egyetem informatikai rendszereinek Informatikai Házirendjét megismertem, és ennek megfelelően fogok eljárni, betartom a vonatkozó szabályokat.

.....

A nyilatkozatot nyomtatott betűkkel kell kitölteni!

Név:

Dátum:

Aláírás

.....

A nyilatkozatot átvettem

Név:

Aláírás

### **3. A legfontosabb információbiztonsággal kapcsolatos törvények, jogszabályok, szabványok**

Az alábbi lista értelemszerűen nem teljes, de tartalmazza a napi működéssel kapcsolatos leginkább releváns törvényeket, jogszabályokat, szabványokat és ajánlásokat:

#### *Jogszabályok*

1. <sup>5</sup>2011. évi CXII. tv. az információs önrendelkezési jogról és az információszabadságról
2. 1995. évi CXXII. tv. a polgárok személyes adatainak nyilvántartásáról szóló 1992. évi LXVI. tv. módosításáról
3. 1992. évi XXII. tv. a Munka Törvénykönyvéről
4. 1978. évi IV. tv. a Büntető Törvénykönyvről
5. 1995. évi LXV. tv. Államtitok és szolgálati titok
6. 1996. évi LVII. tv. a tisztességtelen piaci magatartás és a versenykorlátozás tilalmáról
7. 1995. évi LXVI. tv. Köziratok, köz- és magánlevéltári anyagok
8. 1999. évi LXXVI. tv. a szerzői jogról
9. 2001. évi XXXV. tv. az elektronikus aláírásról

#### *Biztonságtechnikai, tűzvédelmi szabványok, előírások:*

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

#### *Egyéb szabványok, ajánlások*

MSZ EN 60950 Adatfeldolgozó berendezések és irodagépek biztonsági előírásai.

A MeH ITB 12. ajánlása az informatikai rendszerek fizikai, logikai és adminisztratív védelmi követelményeiről és az ezek alapján fogantatosítandó védelmi intézkedésekről

ITSEC = Information Technology Security Evaluation Criteria (Információtechnológia Biztonsági Értékelési Kritériumok) az Európai Közösség ajánlása az informatikai rendszerek biztonságának funkcionális és minősítési követelményeire

<sup>1</sup> TCSEC = Trusted Computer System Evaluation Criteria (Biztonságos Számítógépes Rendszerek Értékelési Kritériumai), az Egyesült Államok Védelmi Minisztériuma által kiadott informatikai biztonsági ajánlás

MeH ITB 8. ajánlásán alapuló kockázatkezelési módszertan

TCSEC = Trusted Computer System Evaluation Criteria (Biztonságos Számítógépes Rendszerek Értékelési Kritériumai), az Egyesült Államok Védelmi Minisztériuma által kiadott informatikai biztonsági ajánlás

---

<sup>5</sup> Megállapította a XXXI/2012. (II. 13.) Szen. sz. határozat. Hatályos: 2012. II. 14. napjától.

ISO/OSI 7498-2 szabvány a nyílt rendszerek biztonsági architektúrájára vonatkozik. Magyar megfelelője: MSZ OSI 7498-1