

**Szegedi Tudományegyetem
Informatikai Biztonsági Szabályzata**

2009.

Tartalomjegyzék

1. Bevezetés

1.1. A szabályzat célja, hatálya, alapelvei

1.2. Fogalmak

1.3. Felelőségek és hatáskörök

1.4. Kapcsolódó szabályozások, szabályzatok

2. Az információbiztonsággal kapcsolatos részletes szabályok

2.1. IT Rendszerek biztonsági osztályai

2.2. Az SZTE információbiztonsági alapelvei és politikája

2.3. Az információbiztonsági politika és szabályzat közzététele

2.4. Az információbiztonsági politika és szabályzat rendszeres felülvizsgálata

2.5. Az információbiztonság szervezeti kérdései

2.6. Bizalmassági nyilatkozatok

2.7. Kapcsolattartás hatóságokkal

2.8. Kapcsolattartás különleges érdekközösségekkel

2.9. Az információbiztonság független felülvizsgálata

2.10. Külső felekkel kapcsolatos rendelkezések

2.11. Az információvagyon menedzsmentje

2.12. Emberi erőforrással kapcsolatos biztonsági kérdések

2.13. Fizikai és környezeti biztonság

2.14. Kommunikáció és üzemelés menedzsment

2.15. Hozzáférés szabályozás

2.16. Információs rendszerek beszerzése, fejlesztése és karbantartása

2.17. Információbiztonsági események menedzsmentje

2.18. Működés-folytonosság biztosítása

2.19. Megfelelőség

3. Záró rendelkezések

3.1. Fegyelmi vétségek

3.2. Hatálybalépés

3.3. A szabályzat rendszeres felülvizsgálata

3.4. Helyi rendelkezések

3.5. A szabályzat megismertetése

1. Bevezetés

A Szegedi Tudományegyetem (SZTE) Szenátusa a Szegedi Tudományegyetemen az információbiztonsággal kapcsolatos elveket, szabályokat, az elvárt és betartandó magatartásformákat és gyakorlatot az alábbiakban határozza meg:

1.1. A szabályzat célja, hatálya, alapelvei

1.1.1. A szabályzat célja, hogy a Szegedi Tudományegyetem (a továbbiakban: SZTE) 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.

1.1.2. A szabályzat hatálya kiterjed az SZTE valamennyi dolgozójára, függetlenül attól, hogy alkalmazására milyen jogviszonyban kerül sor, hallgatójára, függetlenül az oktatás formájára, az informatikai szolgáltatásokat nyújtó és igénybevevő valamennyi szervezeti egységre minden olyan esetben, amikor oktatási, kutatási, tudományos vagy az SZTE adminisztrációs és egyéb feladataihoz az SZTE számítógép-hálózatát vagy egyéb informatikai és telekommunikációs eszközeit használja.

1.1.3. Ha az SZTE harmadik félnek is lehetőséget biztosít infrastruktúrájának használatára, akkor harmadik félre nézve is kötelező a szabályzatban foglaltakat betartani.

1.1.4 A szabályzat 2. fő fejezete követi az ISO 27001:2005 információbiztonsági szabvány struktúráját és elveit, annak „A” melléklete felépítése szerint.

1.1.5 Jelen dokumentumban a szolgáltatásokon a továbbiakban az IT és telekommunikációs szolgáltatások egyaránt értendők.

1.2. Fogalmak

1.2.1. Az **SZTENET** az **SZTE számítógépes hálózata**. Részét képezik a következő típusú eszközök: passzív adatátviteli vonalak (típusuk szerint Ethernet, Token Ring, FDDI, ATM szegmensek, optikai és hagyományos összeköttetések, amelyek részben egyetemi tulajdonúak, részben béreltek) és csatlakozók, aktív hálózati elemek (repeaterek, bridge-ek, switchek, routerek, transceiverek, modemek, terminálszerverek), továbbá minden hálózatra kötött számítógépes munkahely (PC, workstation, terminál, hálózati nyomtató) és szerver függetlenül attól, hogy az mely egyetemi egység tulajdonában vagy használatában van. A hálózatra nem csatlakoztatott számítástechnikai berendezések nem részei az SZTENET-nek. Az SZTENET nyitott bármely olyan technikai megoldás befogadására, amely a meglévő szolgáltatásokat nem veszélyezteti, üzembiztonsága az elvárható szintet nyújtja.

1.2.2. Az eszköz (passzív és aktív hálózati elem, számítógépes munkahely, szerver) **üzemeltetője** annak az egyetemi egységnek a vezetője, amelynek a tulajdonában vagy

használatában van az eszköz, ill. megbízás vagy szerződés alapján az üzemeltetésért felelős. Egyes eszközökhöz, eszközcsoportokhoz az SZTE rektora üzemeltetőt vagy üzemeltető egységet jelölhet ki. Az üzemeltető egységek aktuális nyilvántartását az egyetemi hálózati rendszeradminisztrátor vezeti.

1.2.3. **Felhasználó** az a személy, aki az SZTENET valamely szolgáltatását igénybe veszi. Belső felhasználó az egyetemen munka-, óraadói- vagy hallgatói jogviszonyban álló személy (a továbbiakban felhasználó). Külső felhasználó az egyetemen ilyen jogviszonyban nem álló személy. Külső felhasználók az SZTENET publikus szolgáltatásait vehetik igénybe, egyéb szolgáltatások igénybevételére csak az üzemeltető határozott időre szóló engedélyével jogosultak. Ez utóbbi esetben rájuk is a belső felhasználókra vonatkozó szabályok érvényesek.

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

1.2.5. **IT szolgáltatás:** bármilyen, az Egyetemen használt vagy bevezetni szándékozott IT rendszerrel összefüggő, azzal kapcsolatos szolgáltatás.

1.2.6. **Adatvédelem:** Az 1992. évi LXIII. tv. a személyi adatok védelméről és a közérdekű adatok nyilvánosságáról szóló törvény hatálya alá eső adatkör védelme.

1.2.7. **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.

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

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

- **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 fenyegetés figyelembe lett véve a védelmi intézkedések megtervezésénél és megvalósításánál.
- **Folyamatos** a védelem, ha az időben változó körülmények és viszonyok ellenére is megszakítás nélkül valósul meg.
- **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.

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

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

1.2.12. **Információvédelem:** az informatikai rendszerek által kezelt adatok által hordozott információk védelme a bizalmasság, a hitelesség és a sértetlenség sérülése, elvesztése ellen. Az információvédelem az informatikai biztonság egyik alapterülete.

1.2.13. **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.

1.2.14. **Informatikai biztonságpolitika:** A Szegedi Tudományegyetem átfogó informatikai biztonságpolitikája minden munkatárs és választott tisztségviselő számára egységes értelmezésben azt határozza meg, hogy az informatikai rendszerek által kezelt adatok bizalmasságának, hitelességének, sértetlenségének, rendelkezésre állásának és funkcionalitásának megőrzésével kapcsolatosan milyen biztonsági struktúrát és elveket kell követni, illetve milyen követelményeket szükséges teljesíteni.

1.2.15. **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

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

1.2.17. **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.

1.2.18. **Szolgáltatásért felelős szervezeti egység:** az IT és telekommunikációs szolgáltatás nyújtására alkalmas infrastruktúrával rendelkező önálló szervezeti egység, mely az adott szolgáltatás nyújtásának feltételeit a felhasználók számára nyilvánosságra hozza.

1.2.19. **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.

1.2.20. **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.

1.2.21. **SLA:** Service Level Agreement – Szolgáltatási szint megállapodás egy olyan írásos megállapodás, mely két fél között jön létre: a szolgáltató (a jelen szabályzat alkalmazása során a szolgáltatásért felelős szervezeti egység) és a szolgáltatás felhasználója között. Az SLA meghatározza a két fél között nyújtandó szolgáltatás tartalmát és feltételeit.

1.2.22. **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 támogatják az informatika területén.

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

1.2.24. **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.

1.2.25 **IBSZ:** Informatikai Biztonsági Szabályzat, a jelen dokumentum rövidítése a szabályzat további fejezeteiben.

1.2.26 **ITSZ:** Informatikai Szabályzat egy olyan átfogó informatikai tárgyú szabályozás, melynek megfelelője jelenleg az SZTE szabályozási rendszerében az ún. Számítógépes Infrastruktúra Szabályzat (2000)

1.3. Felelőségek és hatáskörök

1.3.1. Minden, az SZTE-en üzemeltetett IT Rendszer esetében a jelen Szabályzatnak való megfelelés az adott rendszer üzemeltetőjének felelőssége.

1.3.2. SZTE-en kívüli, harmadik személyek által szerződés útján üzemeltetett IT Rendszerek esetében a hatályos jogszabályoknak, szabályzatoknak – különösen a jelen Szabályzatnak - és a vonatkozó szerződésnek való megfelelés kikötése és szükség szerinti ellenőrzése, illetve az ezektől való eltérés észlelése esetén a szükséges intézkedések megtétele a szolgáltatásért felelős szervezeti egység feladata és kötelessége.

1.3.3. Az adott szolgáltatással kapcsolatos információbiztonsági feladatok ellátásáért (illetve az 1.3.2. bekezdésben rögzített feladatok ellátásáért) felelős személyt, illetve a szervezeti egység vezetőjét dokumentáltan nevesíteni kell.

1.3.4. Az egyes szolgáltatások üzemeltetői teljes felelősséggel tartoznak minden olyan beavatkozásért, melyek esetében nem tartották be a rendszer üzemeltetésére vonatkozó biztonsági előírásokat.

1.3.5. A nyilvános, minden, az egyetemmel alkalmazotti vagy hallgatói jogviszonyban álló személy által igénybe vehető szolgáltatások információbiztonsági megfelelőségének ellenőrzése a Belső Ellenőrzési Osztály jogköre.

1.3.6. Az ESZK munkatársai segítséget nyújtanak a szolgáltató és a szolgáltatás igénybevevője között a szolgáltatás információbiztonsági paramétereinek, jellemzőinek egyeztetésében, a megállapodás információbiztonsági aspektusú ellenőrzési feltételeinek kialakításában.

1.3.7. Az informatikai szolgáltatások igénybevétele során elkövetett bűncselekményekért, illetve egyéb jogsértésekért (betörésből fakadó károkozás, stb.) a szolgáltatást igénybevevő a jogszabályok szerinti (pl. büntetőjogi) felelősséggel, valamint fegyelmi és kártérítési felelősséggel is tartozik.

1.3.8. Törvényes megkeresés alapján, a vonatkozó jogszabályi kereteknek megfelelően az ESZK igazgatója minden, a bűncselekmény elkövetésének gyanúja alá eső felhasználó adatait, valamint a rendelkezésre álló naplózott adatokat az eljáró hatóságnak bírói végzés vagy hatósági megkeresés alapján kiszolgáltatja az egyetemi főtitkár engedélyével.

1.3.9. A felhasználókat a szabályzatban leírtak megsértése esetén az alábbi szankciók sújthatják:

- szolgáltatás megtagadás (kizárás a szolgáltatásból), melyről az ESZK igazgatója dönt,
- fegyelmi határozat (az SZTE Szervezeti és Működési Szabályzata alapján)
- az okozott anyagi kár megtérítése, (a vonatkozó - hallgatói, közalkalmazotti – az SZMSZ és Hallgatói Fegyelmi és Kártérítési Szabályzat szerint, az egyetemmel polgári jogi jogviszonyban állók esetén a polgári törvénykönyv szerint).

1.3.10. Az információbiztonsági incidenst az ESZK bejelenti a közalkalmazottat foglalkoztató gazdálkodó szervezeti egység vezetőjének, hallgatók esetében az illetékes dékánának, aki intézkedik a szükséges eljárások lefolytatásáról, a megfelelő fegyelmi és kártérítési szabályzatokban foglaltak szerint.

1.3.11. A szolgáltatásokat igénybe vevők bármilyen szankcionálása csak akkor történhet meg, ha az üzemeltető dokumentálta a szankció elrendelését kiváltó eseményt, incidenst, vagy ilyet az ESZK közvetlenül észlelt.

1.4. Kapcsolódó szabályozások, szabályzatok

1.4.1. A Szegedi Tudományegyetem Szervezeti és Működési Szabályzata - 2007

1.4.2. A Szegedi Tudományegyetem Számítógépes Infrastruktúra Szabályzata - 2000

1.4.3. A Szegedi Tudományegyetem Adatvédelmi Szabályzata - 2000

1.4.4. A Szegedi Tudományegyetem Informatikai stratégiája – 2008. június

1.4.5. A Szegedi Tudományegyetem Hallgatói fegyelmi és kártérítési szabályzat – 2006

2. Az információbiztonsággal kapcsolatos részletes szabályok

2.1. IT Rendszerek biztonsági osztályai

Az SZTE-en üzemeltetett IT rendszereket az alábbi négy kategória valamelyikébe kell besorolni. A besorolás fő szempontjai: tartalmazznak-e érzékeny vagy személyes adatokat, illetve mennyire kritikus a működésük az SZTE egészét tekintve.

- Kritikus rendszerek: („A” osztály) Az SZTE alaptevékenységeinek ellátása szempontjából kritikus rendszerek, amelyek érzékeny, illetve személyes adatokat tartalmazznak. Adatvédelmi szempontból kiemelt védelmet igényelnek, és az SZTE működése szempontjából kiemelt fontosságú rendszerek
 - Bérügyviteli rendszer: BERENC - NEXONBÉR (üzemeltető: GMF Informatikai Osztály és ESZK)
 - Teljes körű Ügyviteli és Szolgáltató Rendszer: TÜSZ (üzemeltető: GMF és ESZK)
 - Hallgatói adminisztrációs és tanulmányi rendszer, továbbá az ehhez kapcsolódó hallgatói szolgáltató rendszerek: ETR (üzemeltető: ESZK)
 - Központi névtár (üzemeltető: ESZK)
 - Központi levelező kiszolgálók (üzemeltető: ESZK és Karok)
 - Központi tárhely-kiszolgálók (üzemeltető: ESZK)
 - Autentikációs rendszerek (üzemeltető: ESZK)
 - Eduroam (üzemeltető: EK, ESZK, és Informatikai Tanszékcsoport)
 - Integrált könyvtári rendszer: Corvina (üzemeltető: EK)
 - Kiemelt felhasználók (lásd 1. számú függelék) asztali számítógépei
 - SZTE Vezetői Információs Rendszer: VIR (üzemeltető: GMF)
- Kiemelt rendszerek: („B” osztály) Az SZTE egyes fontos tevékenységének ellátása szempontjából kiemelt fontosságú rendszerek, amelyek elsősorban technikai jellegűek, a rajtuk tárolt adatok nem elsősorban személyes jellegűek.
 - Számítógép hálózat
 - Technológiai (environment, middleware) rendszerek
 - Elektronikus Pályázat Nyilvántartó Rendszer (EPER)
 - SZTE web szerver-szolgáltatás (SZTE portál)
 - Kari web-szolgáltatás
 - Telefonközpontok (IP és hagyományos) és a hozzájuk tartozó kábelhálózat
 - Ingatlan nyilvántartó és energia program (GMF)
- Normál rendszerek: („C” osztály) Az SZTE egészének napi működése szempontjából nem kiemelt fontosságú rendszerek, ill. a nyújtott szolgáltatások felhasználói köre az SZTE egyes intézményeire, csoportjaira korlátozódik. Védendő, akár személyes adatokat is tartalmazhatnak.
 - Kari, tanszékcsoporti, intézeti, tanszéki, kiszolgálók (pl.. web, levelezés, fájl szerverek)
 - Kutatói, csoportmunka rendszerek
 - Szuper-számítástechnika
 - Hallgatói számítógépes laborok
 - Kollégiumi rendszerek

- Egyéb rendszerek: („D” osztály) Működésük az SZTE egészére nincs kihatással. Szűkebb csoportok vagy személyek oktatási, tanulmányi vagy kutatási munkáját segítik. Ide tartozik minden más, fenti kategóriákba be nem sorolt rendszer. Érzékeny, incidensektől védendő adatokat tartalmazhatnak. Mennyiségüket tekintve kiemelendők.
 - SZTENET-re kapcsolódó oktatói, kutatói számítógépes munkahelyek
 - Hallgatói szabad felhasználású számítógépes munkahelyek
 - Felhasználói tulajdonú, az SZTENET-re (vezetékes vagy vezeték nélküli technológiával) kapcsolható eszközök

2.2. Az SZTE információbiztonsági alapelvei és politikája

2.2.1. Információbiztonsági alapelvek:

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

1. A teljeskörűsége vonatkozó alapelvet a fizikai, a logikai és az adminisztratív védelem területén kell érvényesíteni, úgymint:
 - a) az összes információbiztonsági rendszer elem csoportra,
 - b) az informatikai rendszer infrastrukturális környezetére,
 - c) a hardver rendszerre,
 - d) az alap- és felhasználói szoftver rendszerre,
 - e) a kommunikációs és hálózati rendszerre,
 - f) az adathordozókra,
 - g) a dokumentumokra és feljegyzésekre,
 - h) a belső személyzetre és a külső partnerekre,
 - i) az MSZ OSI 7498-1. szabványban meghatározott nyílt rendszerek architektúrája minden rétegére, azaz mind a számítástechnikai infrastruktúra, mind az informatikai alkalmazások szintjén,
 - j) mind a központi, mind a végponti informatikai eszközökre és környezetükre.
2. A védelem zártsága akkor biztosított, ha az összes valószínűsíthető fenyegetés elleni védelmi intézkedés megvalósul.
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 szükséges maximális védelmi képesség.
4. A védelem folytonossága úgy biztosítható, hogy az informatikai rendszerek fejlesztése és megvalósítása során kialakított védelmi képességeket az

üzemből történő kivonásig folytonosan biztosítani kell az előírások betartását 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.

2.2.2. További céljaink és elveink:

1. Igyekszünk a kockázatainkat minimalizálni, de minden vezetőben és munkatársban tudatosítjuk, hogy tökéletes védelem és biztonság nincsen, és ezzel összefüggésben a maradvány kockázatokat tudatosan vállaljuk.
2. A felelőségeket az információbiztonság területén hangsúlyozottan elhatároljuk és az egyes szolgáltatásokban érdekelt személyekhez kötjük.
3. Hangsúlyozottan törekszünk a törvényi és jogszabályi megfelelésre különös tekintettel a személyes adatok kiemelt védelmére. Az Adatvédelmi Biztos ez irányú állásfoglalásait figyelembe vesszük.
4. Megpróbáljuk kiegyensúlyozottan kezelni a mobilitás lehetősége és a biztonság közötti ellentétet.
5. Elsődleges célunk a működőképesség fenntartása, ezért az olyan felhasználót, aki magatartásával más felhasználók munkáját veszélyezteti, a szolgáltatás üzemeltetéséért felelős szervezeti egység munkatársai a szolgáltatásból haladéktalanul kizárják mindaddig, amíg a veszélyt okozó tevékenységét nem szünteti meg.
6. A védelem mellett biztosítjuk az oktatási és kutatási tevékenységhez szükséges szabad információáramlást.
7. A felhasználói jogosultságok természetes személyhez kötöttek és nem ruházhatóak át. Az információbiztonsági incidensek esetében a felelősség a jogosultsággal bíró személyhez kötődik. Rosszhiszemű felhasználásnak tekintjük, ha a felhasználó a jogosultságát meghaladó műveleteket szándékosan kezdeményez, illetve jogosultságát megkísérli módosítani.
8. Elérendő cél, hogy a szolgáltató rendszerek üzemzavarait ne a felhasználók, hanem automatikus szolgáltatásmonitorozó komponensek jelezzék.

2.3. Az információbiztonsági politika és szabályzat közzététele

Az információbiztonsági politika és szabályzat az SZTE honlapján is hozzáférhető.

2.4. Az információbiztonsági politika és szabályzat rendszeres felülvizsgálata

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

1. A „Záró rendelkezésekben” meghatározott gyakorisággal, illetve
2. minden olyan esetben, amikor a politikában leírtakban jelentős változás(ok) történnek.

2.5. Az információbiztonság szervezeti kérdései

2.5.1. Az információbiztonság belső szervezete: Az információbiztonsággal kapcsolatos felelősség megoszlik az információbiztonsági felelős, az ESZK igazgatója, az egyes szervezetek vezetői és a felhasználók között. A felelősségmegosztás elveit az alábbiakban tárgyaljuk.

2.5.2. A Rector nevezi ki az SZTE információbiztonsági felelősét, aki a feladat ellátásához szükséges szakképzettséggel és hatáskörrel rendelkezik. Az információbiztonsági felelős nincs függelmi kapcsolatban az informatikai szolgáltatásokat nyújtó szervezeti egységek vezetőivel. A Szenátus döntését igénylő kérdések előkészítésének fóruma az egyes információbiztonsági védelmi intézkedésekkel kapcsolatban az Egyetemi Informatikai Bizottság.

2.5.3. 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.

2.5.4. 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.

2.5.5. Az intézmény informatikai rendszerei IBSZ-nek való megfelelése az adott rendszer működtetéséért felelős szervezeti egység vezetőjének a hatáskörébe tartozik.

2.5.6. Információbiztonsági koordináció (érintett felekkel egyeztetés): Az informatikai rendszerek IBSZ megfeleléségi vizsgálatát, illetőleg az ezzel kapcsolatos tanácsadást az ESZK igazgatója, illetve az általa kijelölt személyek végzik. Az IBSZ-nek való megfeleléségi vizsgálatát az információbiztonsági felelős, az ESZK igazgatója vagy a rendszert üzemeltető szervezeti egység vezetője (üzemeltető szervezet vezetője) kezdeményezheti.

2.5.7. Az információbiztonsági felelőségek allokációja: Azon informatikai rendszerek esetében, amelyeknek nem volt sikeres IBSZ megfeleléségi vizsgálata, minden incidens felelőssége 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 dokumentáltan pótolta) az incidensek felelőseit és okait egyedi vizsgálat alapján kell megállapítani és értékelni. Az IBSZ (és a rendszerre vonatkozó mellékleteinek) betartása esetén az üzemeltető jóhiszeműnek minősül. Az ESZK igazgatója felelős az információbiztonsági események, incidensek tanulságai és a pozitív példák megjelenítéséért.

2.5.8. Új információ-feldolgozó rendszerek elfogadási eljárása: Új informatikai szolgáltatás indítási kérelméhez csatolni kell a rendszer vázlatos leírását és a tervezett SLA-t. Ezen anyagok alapján az ESZK igazgatója a szolgáltatás engedélyezése előtt javaslatot kérhet az IBSZ mellékletek aktualizálására, az új szolgáltatás IBSZ paramétereinek megállapítására. A szolgáltatás indítási kérelem automatikusan az ITSZ és az IBSZ elfogadási szándéknyilatkozatának tekintendő.

2.6. Bizalmassági nyilatkozatok

2.6.1. Az információbiztonsági szabályok betartásával és betartatásával kapcsolatban a 1. számú mellékletben részletezett bizalmassági nyilatkozatot írják 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 a fentiekben érintett egyetemi külső (üzleti, tudományos, non-profit stb.) partnerek is a 2. számú mellékletben részletezett titoktartási nyilatkozat kitöltésével és aláírásával.

2.6.2. A rendszer üzemeltetői a rendszer üzemeltetése során különféle személyes, illetőleg bizalmas adatokhoz férnek hozzá, ezért az ilyen rendszerek üzemeltetőivel titoktartási nyilatkozatot köt az egyetemnek a szolgáltatásért felelős szervezeti egységének vezetője.

2.6.3. A munkavégzés során a munkavégzők részére átadott, illetve tudomásukra jutott adatvédelmi szempontból érzékeny információkat védeni kell, ezért ők is titoktartási nyilatkozatra kötelezettek.

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

2.7. Kapcsolattartás hatóságokkal

A különböző törvényekben és rendeletekben előírt adatszolgáltatási kötelezettség teljesítése az adott szolgáltatást üzemeltető szervezeti egység vezetőjének felelőssége. Az SZTE jogi képviseletet nem lát el az egyének jogvitáiban a hatóságokkal.

2.8. Kapcsolattartás különleges érdekközösségekkel

2.8.1. Az ESZK igazgatója felelős a kapcsolattartásért a különleges érdekközösségekkel, mint például a magyar non-profit Internet használók közössége (Hungarnet) vagy a magyar felsőoktatási informatikai egyesület (Huninet). Az előzőekben megfogalmazott hivatalos tagsági és kapcsolattartási kérdésben - az SZTE rektorának útmutatásai alapján - az ESZK igazgatója dönt az SZTE érdekeinek figyelembe vételével.

2.8.2. A felhasználók egyéni tagsága (pl. ISACA, IVSZ, Hétpecsét Információbiztonsági Egyesület stb.) az adott személy felelőssége, aki egyéni tagként is köteles a kapcsolattartás során az IBSZ vonatkozatható előírásait betartani.

2.9. Az információbiztonság független felülvizsgálata

Az SZTE Belső Ellenőrzési Osztálya információbiztonsági vizsgálatot közvetlenül nem végez, ezt a funkciót az információbiztonsági felelős látja el olyan módon, hogy ő kéri fel, vagy jelöli ki a felülvizsgálatot végző szervezetet vagy személyt. A független audit szükségességéről és módjáról esetleg az ESZK igazgatója vagy az információbiztonsági felelős dönt. Az ilyen vizsgálat az „A” osztályú rendszerek esetén legalább 3 évente kötelező.

2.10. Külső felekkel kapcsolatos rendelkezések

2.10.1. A külső felekkel, partnerekkel való kapcsolattartás szabályai:

- Személyes vagy intézményi adatok kiadása, csak a hatályos jogszabályoknak megfelelően történhet.
- Az átadott adatok védelméért a külső szerződő fél tartozik felelősséggel.
- Az egyetemi kapcsolattartó tanácsot kérhet adatvédelmi kérdésekben az adatvédelmi vezetőtől, információbiztonsági kérdésekben pedig az információbiztonsági felelőstől vagy az ESZK igazgatójától.

2.10.2. Ügyfelekkel kapcsolatos információbiztonsági feladatok (jogosultság kiadás felhasználóknak): Az ITSZ szerinti „A”, „B” és „C” osztályú rendszerek esetében az installálási időszakon kívül partner hozzáférést az üzemeltetők eseti kérelme alapján a rendszer üzemeltetéséért felelős szervezet vezetője 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.

2.10.3. Harmadik féllel kötött megállapodások biztonsági kérdései: Minden harmadik féllel kötött IT tartalmú megállapodás esetében a megállapodásban rögzítendőek az adatvédelmi és az információbiztonsági feltételek és előírások.

2.11. Az információvagyon menedzsmentje

2.11.1. Információs vagyonleltár: Az információs vagyon az üzemeltetési dokumentációkban leírtak alapján meghatározott. Az intézmény IBSZ szerinti „A”, „B” és „C” kategóriájú rendszereinek nyilvántartását és az általuk biztosított szolgáltatások paramétereinek nyilvántartását az adott szolgáltatást nyújtó szervezeti egység vezetője által kijelölt személy végzi. Az ehhez szükséges adatszolgáltatás a rendszereket üzemeltető szervezeti egységek vezetőinek kötelezettsége.

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

2.11.3. Az információs vagyon használatának szabályai:

1. Minden alkalmazott és külső partner a számára meghatározott jogosultsággal léphet be a különböző rendszerekbe. A jogosultság változását az alkalmazottak esetében a felettesnél, külső partner esetében a megbízó szervezeti egység vezetőjénél kell kezdeményezni.
2. Az SLA-k rögzítik az egyes szolgáltatásokkal kapcsolatos információvagyon, jogosultságkezelési és használati szabályokat. Minden fajta változtatás az SLA-k változtatási rendjének megfelelően végezhető.

3. Adatok kiadása az „A” és „B” biztonsági osztályba sorolt rendszerekből csak az adott szervezeti egység vezetőjének engedélyével lehetséges, kivételt ez alól az olyan eset képez, amikor az adatcserét, adatátadást szerződés rögzíti. Ebben az esetben a szerződésnek tartalmaznia kell az adatkezelésre vonatkozó szabályokat.

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

1. Információvédelmi alapbiztonsági osztály: Személyes adatok, üzleti titkok, pénzügyi adatok, illetve az intézmény belső szabályozásában hozzáférés-korlátozás alá eső (pl. egyes feladatok végrehajtása érdekében bizalmas) adat feldolgozására, tárolására alkalmas rendszer biztonsági osztálya.
2. 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.
3. 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.

2.11.5. Az osztályba sorolt információs vagyonelemek jelölése és kezelése: Az információs vagyonelemek besorolása, jelölése az IBSZ szerint történik és a végrehajtásáért a szolgáltatás üzemeltetője a felelős.

2.12. Emberi erőforrással kapcsolatos biztonsági kérdések

2.12.1. Alkalmazás előtti tennivalók: Az SZTE-en a felvételt a Rektori Hivatal Humánpolitikai Osztálya végzi. Erkölcsi bizonyítvány szükséges az „A”, „B” és „C” rendszerek üzemeltetői és fejlesztői esetében.

2.12.2. Az alkalmazás alatti tennivalók:

1. 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.)
2. Az „A” és „B” osztályú rendszerek bizonyos szolgáltatásainak igénybeviteléhez (pl. gazdasági rendszer) a szolgáltatásért felelős szervezeti egység vezetője tanfolyam és/vagy vizsga teljesítését írhatja elő. A kritériumok teljesítésének költsége az intézményt terheli.
3. Az IBSZ előírásainak szándékos és tudatos megsértése esetén az alkalmazott az SZTE vonatkozó előírásainak megfelelően szankcionálható.

2.12.3. Elbocsátás vagy munkakör-változás:

1. A dolgozó munkaviszonyának megszűnése esetén minden „A”, „B” és „C” kategóriájú rendszer esetében az üzemeltetői és fejlesztői jogosultságot, ilyen tevékenységet lehetővé tevő belépési kódokat azonnal vissza kell vonni, amit az adott szolgáltatás vezetőjének kell kezdeményeznie. Amennyiben a volt dolgozó a fenti tevékenységeket külső partnerként végzi a továbbiakban, akkor a szerződés megkötése után új, partneri hozzáférés biztosítható számára az ott részletezett szabályok alapján.
2. Az elbocsátott dolgozó vagy hallgató a „C” és „D” kategóriájú rendszerekben a (kizárólag) személyes adatainak elérésére szolgáló belépési kódjait az üzemeltető eseti engedélye alapján megtarthatja.
3. Az alumni rendszerben a végzett hallgató megtarthatja a korábbi hálózati azonosítóját, és a hozzáférést az SZTE biztosítja.

2.13. Fizikai és környezeti biztonság

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

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

2.13.3. Irodák, szobák és egyéb létesítmények fizikai biztonsága:

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

2.13.4. Külső és környezeti károk elleni védelem:

1. Az „A” kategóriájú szolgáltató rendszer kritikus fizikai komponensei csak a hatályos szabályozásnak megfelelő tűz- és villámvédelmi rendszerrel felszerelt helyiségekben üzemeltethetők. Talajszinten vagy az alatt elhelyezkedő helyiségek esetében az ár- és belvízvédelmi szabályozásnak is meg kell felelni.
2. Egyedi esetben az üzemeltetésért felelős szervezeti egység vezetője egyéb előírásokat is megfogalmazhat.
3. A tűzvédelmi rendelkezéseknek megfelelően az erősáramú ellátó rendszernek tartalmaznia kell olyan központi áramtalanítókapcsolót, ami tűzjelzés esetén a biztonságos oltás feltételeit megteremti. A megfelelésről a GMF vezetője köteles gondoskodni.
4. Minden fenti helyiség esetén biztosítani kell azt a hűtési kapacitást, ami a teljes termelt hőmennyiség biztonságos elvezetését automatikusan meg tudja oldani.
5. Minden fenti helyiség esetén biztosítani kell azt az erősáramú ellátó kapacitást, ami a berendezések megtáplálását túlterhelésmentesen el tudja végezni. Az erősáramú ellátó rendszernek áramkör-szelektív megszakítóval kell rendelkeznie.

2.13.5. Munkavégzés biztonsági zónákban: Az „A” kategóriájú rendszereket tartalmazó helyiségekben az üzemeltetésen kívüli minden olyan munkavégzés, ami az informatikai rendszereket vagy azok működését veszélyeztetheti, csak előzetes egyeztetés alapján, felügyelet mellett végezhető. Az egyeztetést a munkát végző (egyén vagy szervezet) és az üzemeltető szervezeti egység vezetője végzi, az üzemeltetők szervezésében és lebonyolításával. A helyiség gépészeti berendezéseit veszélyeztető munkák csak az üzemeltető előzetes engedélyével folytathatók.

2.13.6. Nyilvános hozzáférés, szállítási és töltési területek: Az „A” kategóriájú rendszereket tartalmazó helyiségekben minden szállítási tevékenység csak belépésre jogosult munkatárs felügyelete mellett végezhető.

2.13.7. Eszközök elhelyezése, védelme: Minden „A” kategóriájú 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 ESZK előírhatja.

2.13.8. Támogató közművek (szolgáltatások): A gépterem / kábelrendező helyiségekben üzembe állítandó új rendszerek (vagy nagyobb rendszerkonfiguráció módosítás) esetében az installálást végző szakembereknek előzetesen konzultálniuk kell az erősáramú és hűtési igény biztosításáról az érintett szervezeti egység üzemeltetőjével. A szükséges gépészeti módosításokat az új rendszer üzembe állítása előtt el kell végezni.

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

2.13.10. Eszközkarbantartás:

- Minden szolgáltató rendszer üzemeltetője köteles a hardver komponensek karbantartási igényét felmérni és ezeket úgy ütemezni, hogy a rendszer tervezett élettartama ne rövidüljön karbantartási hiányosságok miatt.
- Az épület-gépészetének külön gépészeti karbantartási tervvel kell rendelkeznie.
- A karbantartás során a felmerült biztonsági sérülékenységeket megfelelően kell kezelni, illetve úgy kell a karbantartásokat elvégezni, hogy újabb biztonsági kockázatok ne merüljenek fel. Ennek felelőse az üzemeltetésért felelős szervezeti egység vezetője által kijelölt személy.

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

2.13.12. Eszközök biztonságos megsemmisítése vagy újrahasznosítása: A használt eszközök selejtezése az SZTE hatályos szabályainak figyelembevételével történik. Speciális eszközök selejtezése esetén az üzemeltető gondoskodik a szakszerű elhelyezésről / elszállításról a GMF bevonásával. Az „A”, „B” és „C” kategóriás eszközök selejtezésénél gondoskodni kell az azon tárolt adatok selejtezés előtti fizikai megsemmisítéséről.

2.13.13. Eszközök (hardver, szoftver) kivitele telephelyről: Az eszközök szállítását szállítólevéllel kell kísélni, amin az eszköz(ök) egyedi azonosítóját (ha értelmezhető) fel kell tüntetni.

2.14. Kommunikáció és üzemelés menedzsment

2.14.1. Működési folyamatok és felelősségek:

- Amennyiben egy szervezeti egység informatikai szolgáltatás bevezetését tervezi, akkor szolgáltatás-indítási kérelemmel fordul az ESZK igazgatójához, és ezzel elismeri megfelelési szándékát az egyetemi IBSZ kritériumainak. A szolgáltatás-indítási kérelem csak adathiány vagy az IBSZ sértés esetén utasítható el. Az elutasítást részletesen indokolnia kell az ESZK igazgatójának, nem kizárva az esetleges módosított újbóli kérelem beadását. Vitás kérdésekben az információbiztonsági felelősével szakmai konzultáció kezdeményezhető.
- Minősített („A”, „B” ill. „C” osztályú rendszerek) esetében az IBSZ megfelelést az ESZK vagy az információbiztonsági felelős esetleg vizsgálhatja és az esetleges hiánypótlásra az üzemeltető szervezet vezetőjét felszólíthatja, aki vagy saját hatáskörben intézkedik, vagy az SZTE illetékes fórumához (Rektor vagy Szenátus) fordul. Amennyiben a vizsgált informatikai rendszer maga is más informatikai szolgáltatásokat használ, úgy a használt szolgáltatás SLA-ja is vonatkozik rá.
- Minden informatikai rendszer esetében a használatra vonatkozó igény bejelentése (hozzáférés vagy felhasználói azonosító igénylése) egyúttal az

IBSZ elfogadásának szándéknyilatkozatát is jelenti. A hozzáférés megadásával a hivatkozott szabályzat a szolgáltatás nyújtója és igénybevevője között érvénybe lép.

- Az IBSZ szerinti „A” és „B” osztályú rendszerek esetében az elvárt 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 üzemeltetésért felelős szervezeti egység vezetője eseti bizottságot nevezhet ki. Ezen bizottságnak mindig tagja az ESZK igazgatója és az információbiztonsági felelős is.

2.14.2. 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 „A” és a „B” kategóriájú IT szolgáltatások esetében az SZTE szolgáltatásonként egykapus ügyintézés és érdekképviselést alkalmaz. Az ilyen szolgáltatók esetében (felhatalmazás alapján) az ügyfélkapcsolatra és szerződéskötésre jogosult az üzemeltetésért felelős szervezeti egység vezetője.

2.14.3. Rendszertervezés és elfogadás: Az informatikai szolgáltató rendszerek esetében az IBSZ megfelelést már a tervezési szempontok között szerepeltetni kell. Az üzemeltetni tervezett „A”, „B” és „C” osztályú rendszerek esetében az IBSZ megfelelés a szolgáltatás indításának szükséges feltétele.

2.14.4. Védekezés vírusok és egyéb kártékony kódok ellen:

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

2.14.5. Biztonsági mentések:

- Minden „A”, „B” és „C” osztályú szolgáltató rendszer üzemeltetési leírásának tartalmaznia kell az alkalmazások és adatok mentési rendjét (a mentendő adatok körét, a mentés módját és gyakoriságát, a mentéséért felelős személyt, a mentés tárolási rendjét).
- „A” és „B” osztályú rendszerek esetén külső tárolású (off-site) mentésekkel is kell rendelkezni, „C” és „D” osztályú rendszerek esetén on-site mentések is elfogadhatóak.
- A mentési rendnek az alkalmazásra vonatkozó részét úgy kell megállapítani, hogy a rendszer működőképessége tetszőleges komponens meghibásodása vagy adatvesztése esetén helyreállítható legyen (új hardver biztosítása esetén). Ennek érdekében az alkalmazás futó kódját legalább minden verzióváltás előtt és után menteni kell, a mentést minimum 3 verzióra vagy egy évre visszamenőleg meg kell őrizni.
- Az alkalmazások és rendszerek konfigurációs beállításait minden változás esetén, de legfeljebb naponta kell menteni. A mentési eljárásnak lehetővé kell tennie egy adott konfigurációs állapot célirányos visszaállítását. A konfigurációs mentéseknek 10 előző állapotra ill. minimum az előző 30 szolgáltatói 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 adatállomány 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 ESZK igazgatója ellenőrizheti.

2.14.6. 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 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).

2.14.7. Média-kezelés:

- Az „A” és „C” osztályú rendszerek adatterületeinek mentései jogvédelem alá eső intézményi és személyes adatokat tartalmazhatnak. Ezen

adathordozókat olyan körültekintéssel kell tárolni és kezelni, mint magát az adatot tároló rendszert.

- A mentések tárolása: Az „A” és „B” osztályú rendszerek mentéseinek tárolása az ESZK 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.

2.14.8. Információcsere:

- Az intézmény „A”, „B” és „C” osztályú rendszerei esetében az automatikus adatcserét lehetővé tevő kapcsolatok létesítéséhez adatvédelmi felelősi 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.

2.14.9. Elektronikus kereskedelem:

- Az elektronikus kereskedelmet lehetővé tevő alkalmazások esetében a biztonsági feltételek megteremtése érdekében az ESZK igazgatójának engedélyre van szüksége a rendszer működtetéséhez.
- Az alkalmazás tervezésébe és megvalósításába be kell vonni az ESZK igazgatóját vagy annak kijelölt képviselőjét.

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

2.15. Hozzáférés szabályozás

2.15.1. Hozzáférési politika:

- Minden olyan informatikai rendszer esetében, ami az intézmény működéséhez szükséges, illetőleg bármilyen védett (intézményi, magán, kutatási, jogvédett, stb. információ) 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 birtokolhat.

- A jogosultság kezelést napra készen kell tartani és dokumentálni.

2.15.2. Felhasználói hozzáférés menedzsmentje:

- Az adott informatikai rendszerhez történő hozzáférés módját (igénybe vételre jogosultak köre, igénylés módja, igénylés elbírálása) a rendszeren működő szolgáltatások dokumentációi tartalmazzák. Az igénybevétel során a természetes személynek azonosítania kell magát egyedi adatával vagy adat-párjával. (pl. tanulmányi rendszer azonosító). Amennyiben az SZTE az informatikai rendszerek felhasználóinak azonosítását központilag valósítja meg, erre a célra szolgáló rendszerekkel (pl. LDAP) és a felhasználói adatbázis kezelése egységesen és konzisztensen történik, akkor az „A”, „B” és „C” kategóriájú rendszereknek ehhez csatlakozási képességgel kell rendelkeznie. Kivételt azok a már meglévő és működő rendszerek képeznek, melyek nem képesek központi jogosultságkezelést megvalósítani.
- A szolgáltatás igénybevételi szabályainak felhasználó általi megszegése esetén a felhasználó az adott szolgáltatásból kizárható. Kizárás esetén a felhasználót ennek tényéről, a kizárás időtartamáról, a problémát okozó tevékenységről és a követendő magatartásról tájékoztatni kell. Ha a felhasználó tevékenysége által okozott kár csekély, akkor törekedni kell az előzetes figyelmeztetésre vagy a letiltás előtti tájékoztatásra.
- Az „A” és „B” osztályú rendszerek esetében az üzemeltető a hozzáférésre jogosultak esetében is előírhat engedélyezési eljárást (pl. a kérelmező munkáltatója által) a hozzáférés megadásához. Az engedélyt az üzemeltetőnek írásban, a kért jogosultságokat feltüntetve kell eljuttatnia kérelmező részére. Minden „A”, „B” és „C” osztályú rendszer esetében az üzemeltető feladata, hogy a kiadott hozzáférések adatait (név, alkalmazás, jogosultsági szint, kiadás dátuma, indoka) naprakészen nyilvántartsa.
- A hozzáférés indokának megszűnése esetén az üzemeltetőnek a hozzáférést dokumentált módon haladéktalanul vissza kell vonnia.

2.15.3. Felhasználói felelősségek:

- A szolgáltatás felhasználója teljes felelősséggel tartozik az adott szolgáltatás dokumentációjában 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, akkor azok bizalmas kezelése munkaköri kötelessége. Az intézményi rendszert köteles csak a munkakörének megfelelően, erőforrás-kímélő módon, a kezelési utasításoknak megfelelően használni.

2.15.4. 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 leírásai tartalmazzák.

- A hálózati szolgáltatások leírásaiban szereplő feltételrendszer az üzembiztonság, nyomon követhetőség és központi kezelhetőség szempontjai szerint van kialakítva, ezért azok be nem tartása a rendszer egészét, a többi felhasználó szolgáltatási környezetét veszélyezteti. Emiatt az előírásokat megszegő felhasználó a hálózati szolgáltatásokból utólagos figyelmeztetés mellett is kizárható.
- Az Internet bármely komponenséhez történő hozzáférés esetén a felhasználó köteles az SZTE Internet-szolgáltatójának szabályzatát is betartani, valamint az Internet közösség etikai irányelveit, mások vallási, politikai és erkölcsi nézeteit tiszteletben tartani.

2.15.5. Operációs rendszer hozzáférés: Az „A”, „B” és „C” osztályú szolgáltatások operációs rendszereiben adminisztrátori beavatkozást kizárólag csak az adott szolgáltatásért felelős vezető által kijelölt személy végezhet. A hozzáférés tényét, időtartamát és forrását a rendszernek visszakereshető módon naplózni kell az egyes szolgáltatások dokumentációja szerint, illetve minimum 1 hónapig.

2.15.6. Alkalmazásokhoz és információhoz való hozzáférés szabályozása:

- Az intézményi adatokhoz való hozzáférést lehetővé tevő alkalmazások jogosultsági köreit olyan módon kell kialakítani, hogy az alkalmazottak csak a munkakörük ellátásához szükséges adatokhoz férhessenek hozzá, illetve kezelhessék. A bizalmas intézményi adatokhoz történő hozzáférést, ezen adatok módosítását alkalmazás szinten is – visszakereshető módon - naplózni kell minimum 1 hónapra visszamenőleg.
- Minden „A”, „B és „C” osztályú rendszer esetén a személyes adatokat kizárólag az adatot birtokló természetes személy férhet hozzá. Ez alól csak a rendszer üzemeltetését ellátó és a mentéseket készítő azonosított személyek jelentenek kivételt. Az adatot birtokló természetes személynek ezen adatok publikálásához tevőlegesen meg kell változtatnia a publikálendő adatok hozzáférési jogosultságát.

2.15.7. Mobil számítógép használat és telefonos munkavégzés:

- Az „A” osztályú rendszerekhez történő menedzsment hozzáférés kizárólag az intézményi belső hálózatból (intranet, otthoni internet) lehetséges. Minden egyéb hozzáférési kísérlet incidensnek minősül és informatikai megoldásokkal is akadályozható az üzemeltetők részéről.
- Speciális hálózati szolgáltatásokkal (pl. otthoni internet) az intranet az intézmény fizikai hálózatán kívülre is meghosszabbítható, ezáltal a munkahelyen kívüli munkavégzés lehetséges. Az ilyen megoldások megvalósítására kizárólag az ESZK ilyen tartalmú szolgáltatásai vehetők igénybe. Az intranet védelmi szintjének megsértése a hálózati hozzáférés nem megfelelő használatával (pl. saját átjáró, külső hálózati kapcsolat, stb.) a felhasználó általi elkövetett súlyos információbiztonsági incidensnek minősül.

2.16. Információs rendszerek beszerzése, fejlesztése és karbantartása

2.16.1. 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.

2.16.2. 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:
 - a rendszer üzemeltetői (üzemeltetői jogosultsággal)
 - a rendszer felhasználói (a munkakörükhöz, szerepükhöz szükséges lekérdező és módosító jogosultságokkal)
- A rendszer fejlesztői a szolgáltató alkalmazáson nem rendelkezhetnek üzemeltetői jogosultságokkal, mivel ez az ő munkakörük ellátáshoz nem szükséges (éles üzemű szolgáltató rendszerben fejlesztés nem történhet).

2.16.3. Kriptográfiai szabályozások:

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

2.16.4. 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 fájlokat a felhasználók nem módosíthatják.
- A rendszer fájlok védelme, az üzembiztos konfiguráció megőrzése és helyreállíthatóságának biztosítása az üzemeltető rendszergazdák munkaköri kötelessége.

2.16.5. Fejlesztési és támogatási folyamatok biztonsága:

- Minden „A” és „B” osztályú alkalmazás fejlesztési tevékenységét a szolgáltató alkalmazás-példánytól és annak adatbázisától elkülönülten kell végezni. Amennyiben a fejlesztési tevékenységhez védett intézményi adatok is szükségesek, akkor a fejlesztői rendszer is „A” és „B” osztályú rendszernek minősül és a hozzáférési jogosultságok ennek megfelelően adhatók ki.

- Intézményi fejlesztésű vagy vásárolt illetve ajándékba kapott szolgáltató rendszer csak funkcionális teszt után vonható szolgáltató üzembe. A funkcionális tesztnek a dokumentációban rögzített minden paraméterre és funkcióra, valamint a tipikus felhasználási mintákra kell kiterjednie. A funkcionális tesztről írásos jegyzőkönyvnek kell készülnie, melynek az összes mért és ellenőrzött paramétert és funkciót tartalmaznia kell.
- Minden, a szolgáltatási felületen vagy a funkciókészletben különbséget tartalmazó alkalmazás verzió esetén a tesztelési eljárást újra el kell végezni. A tesztelési kötelezettség az operációs rendszerek, adatbázis kezelők és egyéb támogató alkalmazások (pl. web szerver) esetén is fennáll, de csak a használt funkciókra kell kiterjednie.
- „A” osztályú alkalmazások esetében csak a teszt rendszeren végzett sikeres teszt után és az üzemeltető rendszergazda engedélyével végezhető változtatás (külső munkavégző esetében is). Ezen előírás alól csak a szolgáltatás helyreállítását célzó sürgős hibajavítás jelent kivételt. Ilyen esetben a dokumentálást utólag kell elvégezni.

2.16.6. Műszaki sérülékenység menedzsment: Az adott alkalmazás üzemeltetőjének felelőssége a publikált technikai sérülékenységek elleni védekezés megvalósítása. A publikált sérülékenységek elleni védekező intézkedés (pl. kiadott hibajavítások telepítése, a sérülékenység elkerülésére irányuló konfigurációs beállítások) legkésőbb az észlelést követő első munkanapon végrehajtandó.

2.17. Információbiztonsági események menedzsmentje

2.17.1. Biztonsági események és gyengeségek jelentése:

- „A”, „B” és „C” osztályú szolgáltató rendszer esetében a szolgáltatás üzemeltetője köteles incidens bejelentési lehetőséget biztosítani a felhasználóknak, és a bejelentés módját a leírásokban közzétenni. A bejelentett incidenseket az üzemeltetők a szolgáltató rendszer integritásának és a kezelt adatok védelmében kötelesek lehetőség szerint rövid reakcióidővel elbírálni és a szükséges lépéseket (pl. hozzáférés korlátozás, biztonsági komponensek beállításainak módosítása) megtenni. Az üzemeltető köteles a bejelentőt tájékoztatni a biztonsági esemény következményeiről és a megtett intézkedésekről. Tömeges érintettség esetén lehetőség van az ESZK központi tájékoztató csatornáinak (kör e-mail, belső portál, honlap) 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, napló-bejegyzés, stb.)
- Az informatikai szolgáltatások igénybevétele közben tapasztalt biztonsági gyengeségek jelentése (a rendszer működőképességének fenntarthatósága érdekében) minden felhasználónak kötelessége. Ennek elmulasztása vagy a gyengeség kihasználása biztonsági eseménynek minősül.

2.17.8. 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 dokumentáció biztonsági követelményei az igénybevevő rendszer egészére vonatkoznak.

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

2.18. Működés-folytonosság biztosítása

A működés-folytonosság információbiztonsági vetülete: Az intézmény működése szempontjából kritikus, „A” és „B” osztályú rendszerek működés-folytonosságának biztosítása az üzemeltető feladata. Ez kiterjed az adott szolgáltatás (alkalmazás) 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.

2.19. Megfelelőség

2.19.1. Jogszabályi megfelelés:

- Az adott szolgáltatást nyújtó szervezet vezetőjének felelőssége a mindenkori jogszabályi megfelelés biztosítása a nyújtott szolgáltatások vonatkozásában.
- Az adott szolgáltatást nyújtó szervezet vezetője 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 3. számú melléklet tartalmazza.

2.19.2. Megfelelés biztonsági politikának, szabványoknak és műszaki előírásoknak:

- Az adott szolgáltatást nyújtó szervezeti egység vezetőjének 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 3. számú melléklet tartalmazza.

2.19.3. Információs rendszerek felülvizsgálatával kapcsolatos megfontolások

- Az adott szolgáltatást nyújtó szervezet vezetője felelős azért, hogy az IT-rendszerek teljes körű belső biztonsági felülvizsgálata dokumentált módon (belső felülvizsgálati jelentés) legalább háromévente megtörténjen, és legalább háromévente sor kerüljön külső, harmadik fél általi felülvizsgálatra az „A” osztályú rendszerek esetében. Ezt az információbiztonsági felelős jogosult ellenőrizni.

- Egy adott szolgáltatás papamétereinek és egyéb feltételeinek súlyos megsértése esetén az ESZK igazgatója külön rendkívüli biztonsági ellenőrzést és felülvizsgálatot rendelhet el.
- A felülvizsgálatok eredményei alapján az ESZK igazgatója rendel el javító, helyesbítő és megelőző intézkedéseket, melyeket mindig a soron következő belső vagy külső, harmadik fél általi felülvizsgálat során kell dokumentált módon ellenőrizni.

3. Záró rendelkezések

3.1. Fegyelmi vétségek

Aki a jelen szabályzatban hivatkozott jogszabályi rendelkezéseket, valamint a jelen szabályzat előírásait megszegi, fegyelmi vétséget követ el.

3.1.1. Üzemeltető személyek: A szabályzatot sértő üzemeltető személy fegyelmi büntetésben részesíthető. Amennyiben a szabálysértés más SZTE szabályok sértésével együtt valósul meg, az egyetemi szabályzatok szerint kell eljárni. Ha a szabálysértést az üzemeltető olyan súlyosnak ítéli, a vétkes fegyelmi felelősségre vonását kezdeményezheti. A szabályzatot súlyosan sértő üzemeltető személyt az üzemeltető köteles az üzemeltető személyzet tagjai köréből véglegesen kizárni. A vétkesség súlyosságát az üzemeltető határozza meg, a vétkes a felette fegyelmi jogkört gyakorló egyetemi vezetőtől kérheti a büntetés határozott időre való módosítását vagy eltörlését.

3.1.2. Felhasználók: A szabályzatot sértő felhasználót az üzemeltető határozott időre felfüggesztheti az SZTENET használatára való minden jogosultságából. Ez esetben a szabálysértés felderítése időpontjától kezdődően a vétkest ki kell zárni az adott eszköz használati jogából, az üzemeltető rendszeradminisztrátorának értesítenie kell az egyetemi hálózati rendszeradminisztrátort, aki utasít minden rendszeradminisztrátort, hogy a vétkestől vonják meg a hatáskörük alá tartozó minden eszközön a vétkes minden jogát. A vétkest az üzemeltető értesíti a felfedett szabálysértésről, aki köteles az üzemeltető egység vezetőjénél személyesen megjelenni, aki a büntetést vele ismerteti. A felfüggesztés időtartamának kezdete a vétkes megjelenésének időpontja. Hallgató esetében a felfüggesztés időtartamába a július és augusztus hónapok nem számítanak be. A vétkes a felette fegyelmi jogkört gyakorló egyetemi vezetőtől (hallgató esetében az illetékes kar dékánjától) kérheti a büntetés mérséklését vagy eltörlését.

3.2. Hatálybalépés

Jelen szabályzat rendelkezéseit az elfogadásának napjától kell alkalmazni.

3.3. A szabályzat rendszeres felülvizsgálata

A Szabályzatot az Informatikai Bizottság évente felülvizsgálja, és módosítási javaslatát a Szenátus felé megteszi.

3.4. Helyi rendelkezések

Amennyiben a szervezeti egységek sajátosságai indokolják, az adott egység a szabályzat alapján köteles 30 napon belül elfogadni és a szenátus elé terjeszteni a specialitásokat meghatározó helyi rendelkezéseket, melyek a jelen szabályzat mellékletét képezik.

3.5. A szabályzat megismertetése

Az egyes szervezeti egységek vezetői kötelesek gondoskodni arról, hogy minden informatikai szolgáltatást nyújtó és igénybe vevő szervezeti egység és alkalmazott megismerje a jelen szabályzatot és a kapcsolódó jogszabályokat.

Záradék:

Jelen szabályzatot a Szegedi Tudományegyetem Szenátusa 2009. december 21-i ülésén a 217/2009. számú határozatával elfogadta.

I. Melléklet: Bizalmassági nyilatkozat „A” és „B” osztályú rendszerek üzemeltetői részére

Az SZTE „A” és „B” biztonsági osztályú rendszereinek üzemeltetőjeként kijelentem, hogy az Egyetem Informatikai Biztonsági Szabályzatát, valamint az adott szolgáltatásra vonatkozó speciális információbiztonsági szabályozásokat megismertem, és ennek megfelelően fogom működtetni az adott szolgáltatásokat.

Az informatikai rendszer üzemeltetése során keletkező naplóállományok személyes adatokat is tartalmazhatnak.

.....

A nyilatkozatot nyomtatott betűkkel kell kitölteni!

Név:

Szervezeti egység:

Elérhetőség:

Dátum:

Aláírás

.....

A nyilatkozatot átvettem

Név:

Aláírás

II. melléklet: Bizalmassági nyilatkozat üzleti partnerek részére

Bizalmassági nyilatkozat

amely létrejött egyrészről a

Szegedi Tudományegyetem

(Székhelye: 6720 Szeged, Dugonics tér 13.)

(továbbiakban, mint egyik Fél), másrészről a

Üzleti partner

(székhelye: xxxx YYYYY, zzzzzz)

(a továbbiakban, mint másik Fél) között a mai napon az alábbi feltételek mellett:

1. A Felek megállapodnak abban, hogy jelen együttműködés során a másik Félről tudomásra jutott információkat, adatokat, így különösen a tulajdonukat képező, vagy az üzleti tevékenységükkel, gazdálkodásukkal, pénzügyi és jogi helyzetükkel kapcsolatos információkat (amelyeket a együttműködés teljesítése érdekében egymás előtt felfednek, illetőleg amelynek a együttműködéssel összefüggésben váltak számukra ismertté vagy egyébként hozzáférhetővé)
 - a. üzleti titokként kezelik,
 - b. azt jogosulatlan személy részére nem szolgáltatják ki, illetve nem teszik egyéb módon hozzáférhetővé,
 - c. azt csak az együttműködés teljesítéséhez, az ehhez szükséges mértékben használják fel, és csak a teljesítésben közvetlenül részt vevő alkalmazottaik, illetve alvállalkozóik számára teszik hozzáférhetővé, és
 - d. azzal egyéb módon nem élnek vissza.
 2. A Felek az ilyen bizalmas, üzleti titkot képező információkat kizárólag indokolt esetben és kizárólag a másik Fél előzetes, írásbeli hozzájárulásának birtokában használhatják fel az együttműködés teljesítésének érdekében kívül eső céllal összefüggésben.
 3. A jelen pontban vállalt titoktartási kötelezettség nem vonatkozik az olyan információra
 - a. amely köztudomású;
 - b. amelyet nem az együttműködés megsértésével hoztak nyilvánosságra;
 - c. amely nyilvánosságra hozatali korlátozás nélkül a másik Fél birtokában volt már azelőtt, hogy a nyilvánosságra hozó Féltől megkapta volna;
 - d. amelyet a használó Fél olyan harmadik Féltől kapott, aki jogszerűen szerezte meg, vagy hozta létre azt, és akit nem köt a nyilvánosságra hozatali tilalom;
 - e. amelyet az egyik Fél a másik Fél bizalmas információjának felhasználása nélkül maga hozott létre; vagy
 - f. amelyet az adott Félnek – jogszabályban meghatározott – kötelessége átadni az illetékes hatóság számára.
 4. A jelen pontban vállalt kötelezettségek az együttműködés megszűnését követően határozatlan ideig hatályban maradnak, kivéve, ha a kérdéses információ hozzáférhetővé tételének megakadályozása – jogszabályváltozás, vagy egyéb körülmények beálltának következtében – kétséget kizáró módon nem áll többé az érintett Fél érdekében, illetve ha az információ nem került egyébként is nyilvánosságra.
- Az **Üzleti partner** vállalja, hogy az együttműködés tartalmára vonatkozó bármely információ megszerzésével érintett munkatársaival titoktartási nyilatkozatot írat alá, mely titoktartási nyilatkozat legalább a együttműködésben meghatározott megkötéseket tartalmazza.

Szeged, 20.., xxxx, yy

.....
Szegedi Tudományegyetem

.....
Üzleti partner

III. melléklet: Az információbiztonság témakörében érvényes legfontosabb jogszabályok, szabványok és műszaki leírások jegyzéke

Az információbiztonság témaköréhez kapcsolódó legfontosabb törvények, szabványok és műszaki leírások

Az információbiztonsághoz legszorosabban kapcsolódó fontos törvények, jogszabályok Magyarországon:

- 1992. évi LXIII. tv. a személyi adatok védelméről és a közérdekű adatok nyilvánosságáról.
- 1995. évi CXXII. tv. a polgárok személyes adatainak nyilvántartásáról szóló 1992. évi LXVI. tv. módosításáról.
- 1992. évi XXII. tv. a Munka Törvénykönyvéről
- 1978. évi IV. tv. a Büntető Törvénykönyvről
- 1996. évi LVII. tv. a tisztességtelen piaci magatartás és a versenykorlátozás tilalmáról.

Biztonságtechnikai, tűzvédelemi szabványok, előírások:

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

Egyéb szabványok, ajánlások:

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

Magyar információbiztonsági szabványok

- Biztonságmenedzsment

- MSZ ISO/IEC 13335 – X Informatika. Biztonságtechnika. Az informatikai és távközlési biztonság menedzselése.
 - -1:2005 Az informatikai és távközlési biztonság menedzselésének fogalmai és modelljei
 - -TR -1:2004 – Az informatikai biztonság fogalmai és modelljei
 - -TR -2:2004 – Az informatikai biztonság menedzselése és tervezése
 - -TR -3:2004 – Az informatikai biztonság menedzselésének technikái
 - -TR -4:2004 – A biztonsági ellenintézkedések meghatározása
 - -TR -5:2004 – Ellenintézkedések külső kapcsolatok esetén

- MSZ ISO/IEC 20000 – X Az informatikaszolgáltatás irányítása.
 - -1:2007 Előírás a szolgáltatásirányításhoz
 - -2:2007 Útmutató a szolgáltatásirányításhoz

- MSZ ISO/IEC 27001:2006 Informatika. Biztonságtechnika. Az információbiztonság irányítási rendszerei. Követelmények (ISO/IEC 27001:2005)

- MSZ ISO/IEC TR 18044:2006 Informatika. Biztonságtechnika. Az információbiztonsági incidensek kezelése

- Biztonságértékelés, a biztonság szavatolása
 - MSZ ISO/IEC 15408 – X Informatika. Biztonságtechnika. Az informatikai biztonságértékelés közös szempontjai
 - -1:2002 Bevezetés és általános modell
 - -2:2003 A biztonság funkcionális követelményei
 - -3:2003 A biztonság garanciális követelményei

 - MSZ ISO/IEC 15292:2005 Informatika. Biztonságtechnika. A védelmi profil regisztrációs eljárásai

 - MSZ ISO/IEC TR 15443-X
 - :2006 Informatika. Biztonságtechnika Az informatikai biztonság szavatolási rendszere Áttekintés és keretrendszer
 - :2007 Informatika. Biztonságtechnika Az informatikai biztonság szavatolási rendszere A szavatolás módszerei

- Jogos és nem jogos hozzáférések
 - MSZ ISO/IEC 15816:2005 Informatika. Biztonságtechnika. A hozzáférés-ellenőrzés biztonsági információobjektumai

 - MSZ ISO/IEC TR 15947:2004 Informatika. Biztonságtechnika. Az informatikai behatolás érzékelésének keretszabálya

 - MSZ ISO/IEC 18028 – X Informatika. Biztonságtechnika. IT hálózatbiztonság
 - -4:2005 Biztonságos távoli hozzáférés

- Elektronikus aláírás, rejtjelezés, időbélyegzés
 - MSZ ISO/IEC 9594-8:2004 – névtár, attribútumok és nyilvános kulcs összekapcsolás
 - MSZ ISO/IEC 11770-1 (keretrendszer) 2, (szimmetrikus kulcsgondozás), 3:2005 (aszimmetrikus kulcsgondozás)
 - MSZ ISO/IEC 13888-1:2005 (általános ismertetés) 2 (letagadhatatlanság – aszimm.), 3:2001 (letagadhatatlanság – szimm.)
 - MSZ ISO/IEC 18014-1 (időbélyegzés, keret), 2 (független adatok előállítása):2004
 - MSZ ISO/IEC 18014-3 (összerendelt adatokat előáll. Mechanizmusok):2005