Szegedi Tudományegyetem

Informatikai Biztonsági Szabályzat

Hatályba lépés napja: 2021. május 31.

Utoljára módosítva: 2021.május 31.

Jóváhagyta: Szegedi Tudományegyetem Szenátusa
2021. május 31-i ülésén a SZ-205-XIII/2020/2021. (V.31.) számú határozatával

Tartalomjegyzék

1. Bevezetés 6
   1.1. A szabályzat célja, hatálya, alapelvei 6
   1.2. A szabályzat rendszeres felülvizsgálata 6
   1.3. A szabályzat közzététele 7
   1.4. A szabályzat megismertetése 7
   1.5. Üzemeltetői szintű, helyi eljárásrendek, rendelkezések 7
   1.6. Felelősségek és hatáskörök 7
   1.7. Kapcsolódó szabályozások, szabályzatok 8
   1.8. Fogalmak 9
2. Az információbiztonsággal kapcsolatos részletes szabályok 12
   2.1. IT rendszerek biztonsági osztályai 12
   2.2. Az SZTE információbiztonsági politikája 13
   2.3. Az információbiztonság szervezeti kérdései 15
   2.4. Titoktartási nyilatkozatok 16
   2.5. Kapcsolattartás hatóságokkal 17
   2.6. Az információbiztonság független felülvizsgálata 17
   2.7. Külső felekkel kapcsolatos rendelkezések 17
   2.8. Az információvagyon menedzsmentje 18
   2.9. Emberi erőforrással kapcsolatos biztonsági kérdések 19
   2.10. Fizikai és környezeti biztonság 20
   2.11. Kommunikáció és üzemelés menedzsment 22
   2.12. Hozzáférés szabályozás 26
   2.13. Információs rendszerek beszerzése, fejlesztése és karbantartása 28
   2.14. Információbiztonsági események menedzsmentje 30
   2.15. Működés-folytonosság biztosítása 31
   2.16. Megfelelőség 32
   2.17. Záró rendelkezések 33
1. melléklet: Titoktartási nyilatkozat üzleti partnerek részére 34
1. függelék Informatikai Felhasználói Szabályzat 35
1. Bevezetés 36
   1.1. A szabályzat célja, hatálya, alapelvei 36
   1.2. A szabályzat közzététele 36
   1.3. A szabályzat megismertetése 36
   1.4. Fogalmak 36

2. Felhasználókra vonatkozó szabályzatok, eljárásrendek 38
2.1. Központi szintű szabályzatok 38
2.2. Üzemeltetői szintű, helyi eljárásrendek, rendelkezések 38
3. Felhasználói szabályok 38
3.1. Felhasználói nyilatkozat 38
3.2. Rendeltetésszerű használat 39
3.3. Tilalmak 39
3.4. Felhasználói magatartás 39
3.5. A felhasználó jogai 40
4. Felhasználói szabályok megsértése 41
4.1. Felhasználók szankcionálása 41
4.2. Anyagi felelősség 41
4.3. Jogosultságok megszerzésére irányuló kísérlet 41
4.4. Biztonsági rendszer feltörése 41
4.5. A jogosultságok átadása 41
4.6. Személyes jövedelemszerzés 42
4.7. Meg nem engedett egyéb tevékenység 42
2. függelék Informatikai Üzemeltetési Szabályzat 43
1. Bevezetés 44
1.1. A szabályzat célja, hatálya, alapelvei 44
1.2. A szabályzat rendszeres felülvizsgálata 44
1.3. A szabályzat közzététele 44
1.4. A szabályzat megismertetése 45
1.5. Üzemeltetői szintű, helyi eljárásrendek, rendelkezések 45
2. Üzemeltetési szabályok 45
2.1. Az üzemeltetés szervezeti felépítése, alapfeladatok 45
2.2. Az SZTENET üzemeltetése: 46
3. Üzemeltetői szabályok 47
3.1. Az üzemeltető személyzet 47
3.2. Üzemeltetői jogosultságok 49
3.3. Az eszközök felhasználási módja 50
4. Üzemeltetési szabályok megsértése, eljárásrendek 51
4.1. Üzemeltető személyek 51
4.2. Felhasználók 51
4.3. Anyagi felelősség 52
4.4. Jogosultságok megszerzésére irányuló kísérlet 52
4.5. Biztonsági rendszer feltörése 52

4.6. A jogosultságok átadása 52
4.7. Személyes jövedelemszerzés 52
4.8. Meg nem engedett egyéb tevékenység 52

1. Bevezetés

A Szegedi Tudományegyetem Szenátusa a Szegedi Tudományegyetemen (a továbbiakban: SZTE) az információbiztonsággal kapcsolatos elveket, szabályokat, az elvárt és betartandó magatartásformákat és gyakorlatot jelen Informatikai Biztonsági Szabályzatban (továbbiakban „IBSZ" vagy „a szabályzat") határozza meg.

1.1. A szabályzat célja, hatálya, alapelvei

1.1.1. A szabályzat célja, hogy a Szegedi Tudományegyetem szervezeti egységei részére egységes és általános értelmezést adjon az informatikai rendszerekben kezelt adatok bizalmassága, hitelessége, sértetlensége, rendelkezésre állása érdekében követendő irányelvekre. Az irányelvek figyelembe vételével kialakítható a zárt, teljeskörű, folytonos és kockázatokkal arányos védelem. Többek között kidolgozhatók a konkrét, rendszer szintű informatikai biztonsági kontrollok, 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 személyi 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. A szabályzat tárgyi hatálya kiterjed a teljes SZTENET-re. Az SZTENET az egyetem számítógépes hálózata, melynek részét képezik aktív és passzív hálózati eszközök, továbbá minden a hálózatra kötött számítástechnikai berendezés függetlenül attól, hogy az mely egyetemi egység tulajdonában vagy használatában van. A hálózatra nem csatlakoztatott számítástechnikai berendezések nem részei az SZTENET-nek.

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

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

1.1.6. Az SZTENET-ben lehetőség van bármely olyan technikai megoldás befogadására, amely a meglévő szolgáltatásokat nem veszélyezteti, üzembiztonsága az elvárható szintet nyújtja és jelen IBSZ követelményeinek megfelel, azonban ennek validálásához minden új technológiai megoldás esetén gondoskodni kell a megfelelő szakértők bevonásáról, és a véleményük kikéréséről (lásd kifejtve későbbi fejezetekben).

1.1.7. A szabályzat figyelembe veszi az MSZ ISO/IEC 27001:2014 információbiztonsági szabvány struktúráját és elveit.

1.2. A szabályzat rendszeres felülvizsgálata

A szabályzatot az Informatikai és Szolgáltatási Igazgatóság (a továbbiakban ISZI) minden jelentősebb változáskor, de legalább évente felülvizsgálja az Elektronikus Információs

Rendszerek Biztonságáért Felelős személy bevonásával (IBF), és amennyiben módosítást igényel, az Informatikai Menedzsment Fórummal (IMF) frissíti jelen Szabályzatot. A módosított szabályzat csak az integrált irányításért felelős szervezet jóváhagyásával helyezhető hatályba.

1.3. A szabályzat közzététele

A Szabályzat az SZTE honlapján mindenki által hozzáférhető.

1.4. A szabályzat megismertetése

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

1.5. Üzemeltetői szintű, helyi eljárásrendek, rendelkezések

1.5.1. Az üzemeltető szervezeti egységek kötelesek kidolgozni és kihirdetni mindazon helyi eljárásrendeket, amelyek alapján az általuk üzemeltetett „A", „B" és „C" osztályú rendszerek használhatóak. Ezek minimum a következők:

- Eszközök adminisztrációjának eljárásrendje (bevételezés, leltárba vétel, személyhez rendelés, igénylés, jóváhagyás, kiadás, visszavétel, selejtezés, leltározás)
- Felhasználók és jogosultságok adminisztrációjának eljárásrendje (igénylésre jogosultak köre, igénylés módja, igénylés elbírálása, beállítás, zárolás, visszavonás, ellenőrzés)
- Incidensek, problémák (rendszerhibák) adminisztrációjának eljárásrendje (bejelentés, eszkalálás, megoldás, lezárás, monitorozás)
- Változáskezelés adminisztrációjának eljárásrendje (fejlesztési igények, jóváhagyások, hibajavítások, konfigurációs beállítások, paraméterezés, patch-elés, tesztelés, élesbe állítás)

1.5.2. Amennyiben a szervezeti egységek sajátosságai indokolják, az IBSZ-t ki lehet egészíteni helyi rendelkezésekkel is. Az adott egység e szabályzat alapján elkészítheti a specialitásokat meghatározó helyi rendelkezéseket, melyeket köteles a Szenátus elé terjeszteni, és amelyek elfogadásuk után jelen szabályzat mellékletét képezik.

1.6. Felelősségek és hatáskörök

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

1.6.2. 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 az ISZI és az IBF előzetes írásos tájékoztatása mellett.

1.6.3. Az adott szolgáltatással kapcsolatos információbiztonsági feladatok ellátásáért (illetve az 1.2.2. bekezdésben rögzített feladatok ellátásáért) felelős személyt, illetve a szervezeti egység vezetőjét dokumentáltan nevesíteni kell az ISZI előzetes bevonásával.

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

1.6.5. A nyilvános, minden, az egyetemmel alkalmazotti vagy hallgatói jogviszonyban álló személy által igénybe vehető szolgáltatások információbiztonsági megfelelőségének ellenőrzése az IBF jogköre (lásd 2.6. Az információbiztonság független felülvizsgálata)

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

1.6.7. 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.

1.6.8. Törvényes megkeresés alapján, a vonatkozó jogszabályi kereteknek megfelelve az ISZI 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 JIHF főigazgató engedélyével.

1.6.9. Az üzemeltető személyzetet és a felhasználókat a szabályzatban leírtak megsértése esetén az alábbi szankciók sújthatják:

- szolgáltatás megtagadás (kizárás a szolgáltatásból), melyről az üzemeltető egység vezetője dönt,
- kötelezettségszegés alapján történő fegyelmi határozat illetve munkáltatói intézkedés (vonatkozó jogszabályok és egyetemi szabályzatok alapján)
- az okozott anyagi kár megtérítése, (vonatkozó jogszabályok és egyetemi szabályzatok alapján, az egyetemmel polgári jogi jogviszonyban állók esetén a polgári törvénykönyv szerint).

1.6.10. Az információbiztonsági incidenst az ISZI bejelenti a munkavállalót foglalkoztató gazdálkodó szervezeti egység vezetőjének, hallgatók esetében az illetékes dékánnak, aki intézkedik a szükséges eljárások lefolytatásáról, a megfelelő fegyelmi és kártérítési szabályzatokban foglaltak szerint.

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

1.7. Kapcsolódó szabályozások, szabályzatok

1.7.1. A Szegedi Tudományegyetem Szervezeti és Működési Szabályzata

1.7.2. A Szegedi Tudományegyetem Adatvédelmi Szabályzata

1.7.3. A Szegedi Tudományegyetem Informatikai Stratégiája

1.7.4. A Szegedi Tudományegyetem Hallgatói Fegyelmi és Kártérítési Szabályzat

1.8. Fogalmak

1.8.1. Az **SZTENET** az SZTE számítógépes hálózata. Részét képezik a következő típusú eszközök: passzív adatátviteli vonalak (hálózati összeköttetések, amelyek részben egyetemi tulajdonúak, részben béreltek) és csatlakozók, aktív hálózati elemek (repeaterek, bridge-ek, switchek, routerek, terminál szerverek), továbbá minden hálózatra kötött számítógépes munkaállomás (PC, workstation, terminál, hálózati nyomtató, mobil eszköz) és szerver függetlenül attól, hogy az mely egyetemi egység tulajdonában vagy használatában van. A hálózatra nem csatlakoztatott számítástechnikai berendezések nem részei az SZTENET-nek.

1.8.2. Az eszköz (passzív és aktív hálózati elem, számítógépes munkaállomás, szerver) **üzemeltető**je 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 Kancellárja üzemeltetőt vagy üzemeltető egységet jelölhet ki. Az üzemeltető egységek aktuális nyilvántartását az egyetemi hálózati rendszeradminisztrátor vezeti.

1.8.3. **Felhasználó** az a személy, aki az SZTENET valamely szolgáltatását igénybe veszi. Belső felhasználó az egyetemmel munka-, óraadói- vagy hallgatói jogviszonyban álló személy (a továbbiakban felhasználó). Külső felhasználó az egyetemmel 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.

1.8.4. **Információ-technológiai (IT) rendszer** (information technology (IT) system) információs rendszer (hardver és szoftver) nemzetközi szakkifejezése

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

1.8.6. **Adatvédelem**: A 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról szóló törvény hatálya alá eső adatkörök védelme, illetve az Európai Parlament és a Tanács 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről szóló rendelet (GDPR) hatálya alá eső adatkörök védelme

1.8.7. **Biztonsági esemény**: Minden esemény, amelynek káros kihatása lehet az informatikai eszköz vagy az azon tárolt adatok bizalmasságára, sértetlenségére illetve rendelkezésre állására.

1.8.8. **Informatikai biztonsági ajánlások**: Jelen szabályzatban az Informatikai Biztonságpolitika alapján az Európai Közösség ITSEC, valamint a 2013. L. törvény és végrehajtási rendelete a 41/2015 (VII.15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről meghatározó jellegű.

1.8.9. 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, és az összes rétegére 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.

1.8.10. **Rendelkezésre állás**: annak a valószínűsége, hogy egy adott időpontban az alkalmazás a tervezéskor meghatározott funkcionalitási szintnek megfelelően a felhasználó által használható (azaz működőképes).

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

1.8.12. **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.

1.8.13. **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.

1.8.14. **Informatikai Biztonsági Szabályzat (IBSZ)**: A Szegedi Tudományegyetem informatikai biztonsági szabályzata minden munkatárs és választott tisztségviselő számára egységes értelmezésben azt határozza meg, hogy az informatikai rendszerek által kezelt adatok bizalmasságának, hitelességének, sértetlenségének, és rendelkezésre állásának megőrzésével kapcsolatosan milyen elveket kell követni, illetve milyen követelményeket szükséges teljesíteni.

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

1.8.16. **BCP**: Business Continuity Plan – Üzletmenet (működés) folytonossági terv, az üzletmenet (működés) fenntartása érdekében teendő intézkedések összessége. Részletes akciótervek kidolgozását jelenti arra az esetre, ha az adott üzleti folyamat vagy alkalmazás végrehajtása, működtetése valamilyen természeti vagy ember által okozott katasztrófa miatt akadályokba ütközik (például hosszabb időre kiesik egy rendszer). Ekkor alternatív módszereket kell kidolgozni a munkavégzésre (például telefonos vagy papír alapú üzenet továbbítás email helyett).

1.8.17. **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. Részletes akciótervek kidolgozását jelenti, melyeknek célja hogy a rendszerek újra működőképesek legyenek (például hardver beszerzés, üzembe helyezés, installálás, stb.).

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

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

1.8.20. **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.

1.8.21. **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.

1.8.22. **Incidens**: Minden esemény, amelynek káros kihatása van az informatikai eszköz vagy az azon tárolt adatok bizalmasságára, sértetlenségére illetve rendelkezésre állására.

1.8.23. **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.

1.8.24. **IBSZ:** Informatikai Biztonsági Szabályzat, a jelen dokumentum rövidítése.

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: tartalmaznak-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 tartalmaznak. Adatvédelmi szempontból kiemelt védelmet igényelnek, és az SZTE működése szempontjából kiemelt fontosságú rendszerek, és melyeknek az elvárt rendelkezésre állása is általában magasabb.

    - Bérügyviteli rendszer: BERENC - NEXONBÉR (üzemeltető: ISZI)
    - Teljes körű Ügyviteli és Szolgáltató Rendszer: TÜSZ (üzemeltető: ISZI)
    - Hallgatói tanulmányi rendszer, továbbá az ehhez kapcsolódó hallgatói szolgáltató rendszerek: Neptun, ETR (üzemeltető: Oktatási Igazgatóság és ISZI)
    - Betegellátásban használt rendszerek (üzemeltető SZAKK, ISZI)
    - Központi névtár (üzemeltető: ISZI)
    - Központi levelező kiszolgálók (üzemeltető: ISZI)
    - eduID authentikációs rendszer (üzemeltető: ISZI)
    - Eduroam (üzemeltető: ISZI)
    - Integrált könyvtári rendszer: Corvina (üzemeltető: ISZI)
    - EOS rendszer (üzemeltető: ISZI)
    - MODULO Elektronikus ügyintézési rendszer (üzemeltető: ISZI)
    - Felsőoktatási COOSPACE rendszer (üzemeltető: Oktatási Igazgatóság és ISZI)
    - Adminisztrációs COOSPACE rendszer (üzemeltető: ISZI)

- 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.

- Teljes számítógépes hálózat (aktív és passzív eszközök)
- Technológiai (environment, middleware) rendszerek
- Pályázat Nyilvántartó Rendszer (Proant)
- SZTE web szerver-szolgáltatás (SZTE portál)
- Kari web-szolgáltatás
- Telefonközpontok (IP és hagyományos) és a hozzájuk tartozó kábelhálózat
- Kari, tanszékcsoporti, intézeti, tanszéki, kiszolgálók (pl. web, levelezés, fájl szerverek)

- 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.

  - Kutatói, csoportmunka rendszerek
  - 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 kiemelendőek.

  - SZTENET-re kapcsolódó oktatói, kutatói számítógépes munkaállomások
  - Hallgatói szabad felhasználású számítógépes munkaállomások
  - Felhasználói tulajdonú, az SZTENET-re (vezetékes vagy vezeték- nélküli technológiával) kapcsolható eszközök

2.2. Az SZTE információbiztonsági politikája

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

2.2.1. Információbiztonsági alapelvek:

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

1. A teljes körűségre vonatkozó alapelvet a fizikai, a logikai és az adminisztratív védelem területén kell érvényesíteni, úgymint:

a) az összes információbiztonsági rendszerelem 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) a rendszerek architektúrájának 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, vagy elfogadható kockázati szinten van.

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 rendszeres ellenőrzéssel és az ezt követő védelmi intézkedésekkel folytonosan biztosítani kell az előírások betartatását.

5. A szabályozási ciklus úgy érvényesíthető, hogy adminisztratív intézkedéssel biztosítani kell a szabályozás, érvényesítés, ellenőrzés és a védelmi intézkedések/szankcionálás ismétlődő, ciklikus folyamatát.

2.2.2. További céljaink és elveink:

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

1. A felelősségeket az információbiztonság területén hangsúlyozottan elhatároljuk és az egyes szolgáltatásokban érdekelt személyekhez kötjük.

2. Hangsúlyozottan törekszünk a törvényi és jogszabályi megfelelőségre különös tekintettel a személyes adatok kiemelt védelmére. Az Adatvédelmi tisztviselő (továbbiakban: DPO ez irányú állásfoglalásait figyelembe vesszük.
3. Törekszünk a mobilitás és a biztonság közötti ellentét kiegyensúlyozott kezelésére. 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.
4. A védelem mellett biztosítjuk az oktatási és kutatási tevékenységhez szükséges szabad információáramlást.
5. A felhasználói jogosultságok természetes személyhez kötöttek és nem ruházhatók 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.
6. Elérendő cél, hogy a szolgáltató rendszerek üzemzavarait ne a felhasználók, hanem automatikus szolgáltatás monitorozó komponensek jelezzék.

2.3. Az információbiztonság szervezeti kérdései

2.3.1. Az információbiztonság belső szervezete: Az információbiztonsággal kapcsolatos felelősség megoszlik az IMF, IBF, az ISZI igazgatója, az egyes szervezetek vezetői és a felhasználók között. A felelősségmegosztás elveit az alábbiakban tárgyaljuk.

2.3.2. Az informatikai és információbiztonsági kérdésekben a legfőbb döntéshozó az Informatikai Menedzsment Fórum (IMF), melynek állandó tagjai:

- ISZI igazgatója
- Jogi, Igazgatási és Humánpolitikai Főigazgató
- Az ISZI igazgatójának helyettesítésére kijelölt személy
- Elektronikus Információs Rendszer Biztonságáért Felelős Személy (IBF)

2.3.3. A Kancellár vagy ISZI igazgatójának előzetes jóváhagyásával az IMF tagjai bármely egyéb szakterület képviselőit, szükség esetén külső feleket is bevonhatnak eseti jelleggel.

2.3.4. A Kancellár nevezi ki az SZTE Elektronikus Információs Rendszer Biztonságáért Felelős Személyét (IBF), aki a feladat ellátásához szükséges szakképzettséggel és hatáskörrel rendelkezik. A feladat szerződött partnerrel kiszervezett funkcióként is ellátható. Az IBF nem lehet függelmi kapcsolatban az informatikai szolgáltatásokat nyújtó szervezeti egységek vezetőivel.

2.3.5. 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.

2.3.6. 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.

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

2.3.8. Információbiztonsági koordináció (érintett felekkel egyeztetés): Az informatikai rendszerek IBSZ megfelelőségi vizsgálatát, illetőleg az ezzel kapcsolatos tanácsadást az ISZI igazgatója, illetve az általa kijelölt személyek végzik. Az IBSZ-nek való megfelelőség vizsgálatát az IMF, az ISZI igazgatója, az IBF vagy a rendszert üzemeltető szervezeti egység vezetője (üzemeltető szervezet vezetője) kezdeményezheti.

2.3.9. Az információbiztonsági felelősségek allokációja: Azon informatikai rendszerek esetében, amelyeknek nem volt sikeres IBSZ megfelelőségi 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 ISZI igazgatója felelős az információbiztonsági események, incidensek tanulságai és a pozitív példák megjelenítéséért.

2.3.10. Új információ-feldolgozó rendszerek elfogadási eljárása: Új informatikai rendszerek, szolgáltatások bevezetési kérelméhez csatolni kell a rendszer, szolgáltatás vázlatos leírását és a tervezett SLA-t. Ezen anyagok alapján az ISZI igazgatója a szolgáltatás engedélyezése előtt javaslatot tehet az IBSZ aktualizálására, az új szolgáltatás IBSZ besorolásának, paramétereinek megállapítására. Új szolgáltatás csak az IBSZ-ben foglalt követelményeknek megfelelően indítható. A szolgáltatás indítási kérelem automatikusan IBSZ megfelelési nyilatkozatnak is tekintendő.

2.4. Titoktartási nyilatkozatok

2.4.1. Az információbiztonsági szabályok betartásával és betartatásával kapcsolatban a *3. számú mellékletben* részletezett titoktartási nyilatkozatot írnak alá az egyetemi külső (üzleti, tudományos, non-profit stb.) partnerek.

2.4.2. A rendszer üzemeltetői a rendszer üzemeltetése során különféle személyes, illetőleg bizalmas adatokhoz férnek hozzá, ezért az ilyen rendszerek üzemeltetőitől is titoktartási nyilatkozatot kérhet az egyetemnek a szolgáltatásért felelős szervezeti egységének vezetője, amennyiben ezt a munkaszerződése nem tartalmazza.

2.4.3. A munkavégzés során a munkavégzők (például külső partner cég alkalmazottai) részére átadott, illetve tudomásukra jutott adatvédelmi szempontból érzékeny információkat is védeni kell, ezért ők is titoktartási nyilatkozatra kötelezettek.

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

2.5. 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.

Informatikai biztonsági témakörben a Nemzeti Kibervédelmi Intézettel (NKI) való kapcsolattartási feladatok ellátása elsődlegesen az ISZI feladata és felelőssége, ide értve az NKI figyelmeztetések, riasztások figyelemmel kíséretét is.

Személyes adatok érintettsége esetén a Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) felé történő adatszolgáltatási kötelezettségek teljesítése a Jogi, Igazgatási és Humánpolitikai Főigazgatóság (JIHF) és a DPO feladata és felelőssége.

2.6. Az információbiztonság független felülvizsgálata

Az információbiztonsági vizsgálatot az IBF látja el. A független audit szükségességéről és módjáról esetileg az IMF, az ISZI igazgatója vagy az IBF dönt. Az ilyen vizsgálat az „A" osztályú rendszerek esetén legalább 3 évente kötelező.

Az információbiztonsági vizsgálatok eredménye alapján az IBF feladata a védelmi intézkedési javaslatok kidolgozása az ISZI és szükség esetén további területek bevonásával. Amennyiben személyes adatok érintettsége merül fel a vizsgálat bármely szakaszában az ISZI-nek be kell vonnia a JIHF-et. A vizsgálatok eredményének és a védelmi intézkedési javaslatok előterjesztése az IMF felé az IBF feladata és felelőssége. A védelmi intézkedési javaslatokról az IMF dönt.

A védelmi intézkedések implementálásának nyomon követése és az IMF rendszeres tájékoztatása az IBF feladata.

2.7. Külső felekkel kapcsolatos rendelkezések

2.7.1. 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 a DPO-tól, információbiztonsági kérdésekben pedig az IBF-től vagy az ISZI igazgatójától.

2.7.2. Ügyfelekkel kapcsolatos információbiztonsági feladatok (jogosultság kiadás felhasználóknak): Az „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.

2.7.3. Partnerekkel, harmadik féllel kötött megállapodások biztonsági kérdései: Minden partnerrel, harmadik féllel kötött IT tartalmú megállapodás, szerződés, megrendelés esetében a megállapodásban rögzítendők az adatvédelmi és az információbiztonsági feltételek és előírások, az alábbiak szerint:

- A szerződés mellékleteként csatolandó az SZTE Informatikai Biztonsági Szabályzat (IBSZ) aktuális verziója, amit a partner / harmadik fél magára nézve kötelezőnek ismer el.
- Vagy a fenti megoldás helyett: a szerződésbe átemelendők az IBSZ külső felekre és az adott szerződésre releváns pontjai.

2.7.4. Új technológiai megoldások bevezetésekor először az egyetemi hálózati rendszeradminisztrátorral, az IBF-fel és az ISZI igazgatójával mindig előzetesen véleményeztetni kell az ajánlati kiírás, a szerződés, vagy a megrendelés szövegét (vagy annak szakmai részét) annak biztosítására, hogy a megfelelő információbiztonsági követelmények kerüljenek be a szövegezésbe, és hogy az új megoldások megfelelően illeszkedjenek a meglévő infrastruktúrába, és annak működését, rendelkezésre állását, biztonságát ne veszélyeztessék. Az előzetes véleményezés eredményét az IMF elé kell terjeszteni.

2.8. Az információvagyon menedzsmentje

2.8.1. Információs vagyonleltár: Az információs vagyon az üzemetetési dokumentációkban leírtak alapján meghatározott. Az intézmény IBSZ szerinti „A”,

2.8.2. „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.

2.8.3. Az információs vagyon tulajdonjoga: Az intézmény IBSZ szerinti „A”, „B” és

2.8.4. „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.

2.8.5. Az információs vagyon használatának szabályai:

- 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.
- Az SLA-k rögzítik az egyes szolgáltatásokkal kapcsolatos információvagyon, jogosultságkezelési és használati szabályokat. Minden fajta változtatás az SLA-k változtatási rendjének megfelelően végezhető.
- 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.

2.8.6. 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.

- 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.
- 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.

2.8.7. 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.

2.9. Emberi erőforrással kapcsolatos biztonsági kérdések

2.9.1. Alkalmazás előtti tennivalók: Az SZTE-en a felvételt a Jogi, Igazgatási és Humánpolitikai Főigazgatóság végzi. Erkölcsi bizonyítvány szükséges az „A”, „B” és „C” rendszerek üzemeltetői és fejlesztői esetében.

2.9.2. Az alkalmazás alatti tennivalók:

- 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) a szolgáltatásért felelős szervezeti egység vezetője 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 SZTE vonatkozó előírásainak megfelelően szankcionálható.

2.9.3. Elbocsátás vagy munkakör-változás:

- 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 szervezeti egység 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.

- Amennyiben az SZTE az informatikai rendszerek felhasználóinak azonosítását központilag valósítja meg, úgy a dolgozó munkaviszonyának megszűnése esetén ebben a rendszerben is tiltani kell a felhasználói fiókját, így biztosítva az ehhez kapcsolódó informatikai rendszerekben is a hozzáférés megszűntetését.
- A szerződő harmadik félnek kötelezettséget kell vállalnia, hogy minden esetben, ha a szerződésben érintett, illetve az SZTE informatikai rendszereihez hozzáférő munkavállalóinál jogviszonyváltozás áll be, arról azonnali hatállyal tájékoztatja a SZTE szerződésben rögzített kapcsolattartóját. A kapcsolattartó feladata jeleznie az ISZI felé a személyi változást és ezzel egyidőben a jogosultságok felülvizsgálatának szükségességét, amennyiben az releváns.
- 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.
- Az alumni rendszerben a végzett hallgató megtarthatja a korábbi hálózati azonosítóját, és a hozzáférést az SZTE biztosítja.

2.10. Fizikai és környezeti biztonság

2.10.1. 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.

2.10.2. Fizikai belépési szabályozás: Az „A" kategóriájú rendszerek komponenseit tartalmazó szolgáltató helyiségekbe (géptermek, kábelrendezők) 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.

2.10.3. 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 (mentőeszköz / tároló, fejlesztői rendszer, felügyelő terminál, stb.) csak beléptető rendszerrel védett munkaszobában és irodában helyezhető el.
- 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 az ISZI előzetes írásos tájékoztatása valamint a folyamatban történő bevonása mellett.

2.10.4. Külső és környezeti károk elleni védelem:

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

2.10.5. 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.

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

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

2.10.8. 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.

2.10.9. 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 ISZI által felügyelt területnek minősülnek. Azokban munkát végezni, vagy a megközelíthetőségüket korlátozni csak a rendszerkomponens üzemeltetőjének előzetes írásos engedélyével lehet.

2.10.10. 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.
- Minden elvégzett karbantartást visszakereshető módon dokumentálnia szükséges az adott rendszer üzemeltetőjének. Amennyiben rendkívüli karbantartási feladat válik szükségessé, az ISZI-t tájékoztatni szükséges, lehetőség szerint a karbantartási feladat végrehajtása előtt, de mindenképp a karbantartási igény megjelenésének napján. Amennyiben felmerül annak a lehetősége, hogy a karbantartás kihathat egyéb olyan rendszerekre is, melynek üzemeltetése más üzemeltető felelősségi körébe tartozik, a karbantartás megkezdése előtt tájékoztatni kell az ISZI-t és a karbantartás csak az ISZI írásos jóváhagyásával kezdhető meg.

2.10.11. 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.

2.10.12. 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 GF és az MI bevonásával. Az „A”, „B” és „C” kategóriás eszközök selejtezésénél gondoskodni kell az azon tárolt adatok selejtezés előtti fizikai megsemmisítéséről.

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

2.11. Kommunikáció és üzemelés menedzsment

2.11.1. Működési folyamatok és felelősségek:

- Amennyiben egy szervezeti egység informatikai szolgáltatás bevezetését tervezi, akkor szolgáltatás-indítási kérelemmel fordul az ISZI igazgatójához, és ezzel elismeri megfelelési szándékát az egyetemi IBSZ kritériumainak. A szolgáltatás-indítási kérelmet az ISZI igazgatója adathiány vagy IBSZ sértés esetén elutasítja. Az ISZI igazgatója mérlegeli a szolgáltatás indítás körülményeit, szem előtt tartva a racionális erőforrás gazdálkodást, ami alapján javaslatot tesz az indítani kívánt szolgáltatás transzformációjára, vagy elutasítja a kérelmet. Az elutasítást részletesen indokolnia kell az ISZI igazgatójának, nem kizárva az esetleges módosított újbóli kérelem beadását. Vitás kérdésekben az IBF-fel szakmai konzultáció kezdeményezhető.

- Minősített („A”, „B” ill. „C” osztályú rendszerek) esetében az IBSZ megfelelést az ISZI vagy az IBF esetileg vizsgálhatja és az esetleges hiánypótlásra az üzemeltető szervezet vezetőjét felszólíthatja, aki vagy saját hatáskörben intézkedik, vagy az SZTE illetékes fórumához (Rektor, Kancellár 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 Működés-folytonosság szempontjából kritikusnak tekintett 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 ISZI igazgatója és az IBF is.

2.11.2. 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 adatvédelmi kérdésekre is, melyek összhangban állnak az SZTE szabályzataival.
- Az információbiztonsági követelmények érvényre juttatásának érdekében a szolgáltatást igénylőnek a szerződés megkötése előtt be kell vonnia az ISZI-t.
- A jogi és adatvédelmi követelmények érvényre juttatásának érdekében a szolgáltatást igénylőnek a szerződés megkötése előtt be kell vonnia a JIHFet és a DPO-t.
- A működési környezetben történő változások a szerződések felülvizsgálatának szükségességét eredményezhetik. A Belső Ellenőrzési Osztály feladata a külső felekkel kötött szerződések éves felülvizsgálatának kezdeményezése a szerződés szempontjából releváns szakterületek bevonásával.
- Az „A” és a „B” kategóriájú IT szolgáltatások esetében az SZTE szolgáltatásonként egykapus ügyintézést és érdekképviseletet alkalmaz. Az ilyen szolgáltatók esetében (felhatalmazás alapján) az ügyfélkapcsolatra és szerződéskötésre jogosult az üzemeltetésért felelős szervezeti egység vezetője.

2.11.3. 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.
- Az adatvédelmi követelmények meghatározásai a JIHF és DPO feladata és felelőssége.

2.11.4. 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 ISZI igazgatója jogosult illetve köteles az ilyen levelező rendszernek a haladéktalan kitiltására illetve hálózati kapcsolatának megszüntetésére. A károkozás tényét az ISZI 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).

2.11.5. Biztonsági mentések:

- A rendszerek mentésével szembeni követelmények meghatározása az ISZI feladata az érintett szakterületek bevonásával annak érdekében, hogy olyan mentési követelmények teljesüljenek a gyakorlatban, melyek a szakterületek működésének megfelelőek. A jogszabályoknak megfelelő megőrzési idők meghatározása a JIHF feladata és felelőssége.
- 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 elfogadhatók.
- 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 szolgáltatási napra ki kell terjedniük.
- Az „A" osztályú rendszerek esetében az alkalmazásokban tárolt intézményi adatokat minden munkanap végén 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 ISZI igazgatója ellenőrizheti.

2.11.6. Hálózatbiztonság menedzsmentje: Az intézmény teljes területére kiterjedő alapinfrastruktúra (számítógépes és telefonhálózat) védelme egységes koncepció és megvalósítás mellett történik. Az irányelvek és módszerek meghatározását és a szükséges operatív beavatkozásokat a telekommunikációs hálózat üzemeltetésével megbízott 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).

2.11.7. 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 ISZI 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.

2.11.8. Információcsere:

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

2.11.9. Monitorozás:

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

2.12. Hozzáférés szabályozás

2.12.1. 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 birtokolhat.
- A jogosultság kezelést napra készen tartani és dokumentálni kell.

2.12.2. 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.

2.12.3. 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.

2.12.4. 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.

2.12.5. 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 naplóznia kell az egyes szolgáltatások dokumentációja szerint, illetve minimum 1 hónapig.

2.12.6. 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 adatokhoz 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 publikálandó adatok hozzáférési jogosultságát.

2.12.7. Mobil számítógép használat és telefonos munkavégzés:

- Az „A” osztályú rendszerekhez történő menedzsment hozzáférés kizárólag dedikált hálózatból (intranet, VPN) lehetséges. 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. Az ilyen megoldások megvalósítására kizárólag az ISZI 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.
- Az SZTE-n belül lehetőség van a saját eszközök alkalmazására is („Bring Your Own Device", BYOD), melyek használatakor az SZTE érzékeny adatainak tárolása a felhasználó felelőssége, a biztonságos tárolási megoldással kapcsolatban az ISZI nyújt segítséget a felhasználók számára. A felhasználóknak az eszközön kerülni kell az olyan kifogásolható anyagok tárolását, feldolgozását vagy továbbítását, amelyek sértik a törvényt vagy a közízlést, mint például: betiltott filmek, publikációk; pornográfiát, pedofíliát, erőszakot hirdető cikkek, publikációk; kalóz letöltésből származó média anyagokat; a jó ízlés határait sértő anyagokat.

2.13. Információs rendszerek beszerzése, fejlesztése és karbantartása

2.13.1. 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 változtathatók olyan irányba, hogy a rendszer biztonsági szintje csökkenjen.
- Új technológiai megoldások esetén először az egyetemi hálózati rendszeradminisztrátorral, az IBF-fel és az ISZI igazgatójával mindig előzetesen véleményeztetni kell a megvalósítandó technológiát és a meghatározott biztonsági követelményeket annak biztosítására, hogy a megfelelő védelmi intézkedések kerüljenek megvalósításra, és hogy az új megoldások megfelelően illeszkedjenek a meglévő infrastruktúrába, és annak működését, rendelkezésre állását, biztonságát ne veszélyeztessék. Az előzetes véleményezés eredményét az IMF elé kell terjeszteni

2.13.2. Rendszerek tervezése:

- 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.

2.13.3. 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 a munkakörük ellátáshoz nem szükséges (éles üzemű szolgáltató rendszerben fejlesztés nem történhet).

2.13.4. 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.

2.13.5. 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.

2.13.6. Fejlesztési és tesztelési folyamatok biztonsága:

- Minden „A” és „B” osztályú alkalmazás fejlesztési tevékenységét a szolgáltató éles alkalmazás-példánytól és annak adatbázisától elkülönülten kell végezni fejlesztői környezetben. 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.

2.13.7. 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.

2.14. Információbiztonsági események menedzsmentje

2.14.1. 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 ISZI központi tájékoztató csatornáinak (kör e-mail, belső portál, honlap) használatára is.
- A Szabályzat személyi hatálya alá tartozó felhasználóknak kötelessége az informatikai szolgáltatások igénybevétele közben tapasztalt biztonsági gyengeségek jelentése (a rendszer működőképességének fenntarthatósága érdekében) a rendszer üzemeltetőjének. Ennek elmulasztása vagy a gyengeség kihasználása biztonsági eseménynek minősül.
- Biztonsági esemény anonim módon a ithelp@szte.hu e-mail címre küldhető, melyhez az ISZI munkatársának van közvetlen hozzáférése, aki szükség esetén értesíti az IBF-t.
- Az adatvédelmi incidensekről a JIHF és a DPO közvetlenül is tájékoztatható a dpo@szte.hu email címen.
- A szerződött félnek az SZTE saját munkavállalóihoz hasonlóan kötelessége betartani jelen Szabályzatot. Kötelességük jelenteni minden észlelt hibát és biztonsági incidenst a szerződés szerinti kapcsolattartónak, akinek haladéktalanul jeleznie kell azt az ISZI-nek.
- A biztonsági esemény észleléséről az adott rendszer üzemeltetőjének kötelessége írásban értesíteni az ISZI-t és az IBF-et.
- Amennyiben az adatvédelmi incidensről szóló bejelentés közvetlenül a JIHF-hoz vagy DPO-hoz érkezik be, értesíteniük kell az ISZI-t és az IBF-et, hogy megvizsgálják az incidens informatikai vonatkozásait.

- A biztonsági esemény kivizsgálásáról az üzemeltetőnek az IBF-et a tájékoztatnia kell, valamint szükség esetén a biztonságieseménykivizsgálásába bevonni. Az incidensről és az incidens kivizsgálásának eredményéről az IBF feladata tájékoztatni az IMF-et, aki dönt a külső felekkel, beleértve a hatóságokkal való kommunikáció szükségességéről és módjáról. A kommunikáció megkezdése előtt az SZTE vezetésének jóváhagyása szükséges. .
- Amennyiben személyes adatok érintettségének lehetősége merül fel, úgy az adott rendszer üzemeltetőjének kötelessége haladéktalanul tájékoztatnia és a vizsgálatba bevonnia a JIHF-et és a DPO-t. Amennyiben az incidens az érintettek és a hatóság (NAIH) tájékoztatását igényli, a DPO feladata az SZTE vezetésének bevonása, valamint a vonatkozó jogszabálynak megfelelő tájékoztatás végrehajtása.
- Biztonsági esemény vagy gyengeség bejelentése esetén a bejelentő köteles csatolni mindazon adatokat, amik az esemény megítéléséhez legjobb tudása szerint szükségesek (pl. időpont, tapasztalt jelenség, naplóbejegyzés, stb.)

2.15. Működés-folytonosság biztosítása

2.15.1. A működés-folytonosság információbiztonsági vetülete:

- A működés-folytonosság szempontjából kritikus rendszerek meghatározása az ISZI feladata az érintett szakterületek által meghatározott rendelkezésre állási követelmények alapján.
- Az „A” és „B” osztályú rendszerek közül működés-folytonosság szempontjából kritikusnak tekintett rendszerek működés-folytonosságának, rendelkezésre állásának biztosítása az üzemeltető feladata. Ez kiterjed az adott szolgáltatás (alkalmazás) feltételrendszerének körültekintő meghatározására, a felelős incidenskezelésre, a szükséges funkcionális és biztonsági javítások telepítésére, rendszeres biztonsági mentések készítésére, és időnkénti mentés visszatöltési tesztek végzésére.

2.15.2. Működés-folytonosság szempontjából kritikusnak tekintett „A” osztályú rendszereknél kötelezően készítendő BCP (Üzletmenet folytonossági terv) és DRP (Katasztrófa utáni helyreállítási terv), melyeknek elkészítéséért az üzemeltető a felelős. A BCP hatókörét a felhasználó területek vezetőivel kell egyeztetni, ugyanis elegendő azt csak a kritikusabb folyamatokra kidolgozni.

2.15.3. Működés-folytonosság szempontjából kritikusnak tekintett „A” osztályú rendszereknél nem szükséges BCP akcióterveket kidolgozni (csak DRP elegendő), ha a következő feltételek teljesülnek:

- Az üzemeltetőnek meg kell határoznia az általa vállalt maximális visszaállítási időt, és a biztonsági mentések gyakoriságát. A vállalt maximális visszaállítási idő a DRP részeként kell dokumentálva legyen arra az esetre ha egy rendszer nulláról újra felépítendő (például: ha tűz miatt megsemmisülnek a hardver elemek).
- A felhasználóknak meg kell határozniuk az általuk elvárt maximális visszaállítási időt (Recovery Time Objective, RTO) és az adatvesztés maximális időtartamát (Recovery Point Objective, RPO), mint igényeket az üzemeltető felé. Ezen igények a maximálisan tolerálható időket kell tükrözzék, amennyit a kapcsolódó folyamat (az SZTE működése) még egy ilyen szélsőséges esetben kibír, azaz üzleti hatása még elfogadható.

- Amennyiben az üzemeltető által vállalt visszaállítási idő megfelel a felhasználók által elvárt maximális visszaállítási idő (RTO) igénynek (azaz a vállalt visszaállítási idő rövidebb vagy ugyanakkora mint az igény), és a mentési gyakoriság is megfelel az adatvesztés maximális időtartama (RPO) igénynek (a mentés gyakoribb vagy ugyanakkora mint az időtartam) akkor DRP akciótervek készítése elegendő, és a BCP akciótervek készítésétől el lehet tekinteni.
- Minimum egy DRP akciótervet készíteni a fenti esetben is kötelező, amely a rendszer nulláról való felépítését írja le lépésről lépésre.

2.15.4. Működés-folytonosság szempontjából kritikusnak tekintett „B" osztályú rendszerek esetében a BCP és DRP készítése csak ajánlott, de nem kötelező. Működés-folytonosság szempontjából kritikusnak tekintett „C" és „D" osztályú rendszereknél pedig egyáltalán nem szükséges.

2.15.5. A BCP akciótervek végrehajtója mindig a felhasználói (üzleti) oldal (hiszen ez egyetemi folyamatok működtetését jelenti rendszerek kiesése esetén), de a BCP tervek kidolgozása közös feladat, ami üzemeltetői és felhasználói együttműködést igényel Az üzemeltető felelőssége bevonni a feladatba a kulcsfelhasználókat és koordinálni a tervek elkészítését.

2.15.6. A DRP akciótervek végrehajtója mindig az üzemeltetői (IT) oldal, és a DRP akciótervek kidolgozása is kizárólag üzemeltetői feladat, azonban a megfelelő megoldás kidolgozásához információt kell kapjanak a felhasználói igényekről. Ugyanis az alkalmazandó technológiát és módszereket nagyban befolyásolja a felhasználók által elvárt maximum visszaállítási idő (RTO) és az adatvesztés maximális időtartama (RPO).

2.16. Megfelelőség

2.16.1. Jogszabályi megfelelőség:

- Az adott szolgáltatást nyújtó szervezet vezetőjének felelőssége a mindenkori jogszabályi megfelelőség 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 a következők:

a. 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról.

b. 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (adatvédelmi törvény)

Az adott szolgáltatást nyújtó szervezet vezetőjének kötelessége tájékozódni az újabb jogszabályok megjelenéséről. A közérdekű adatok kezelésével, adatvédelmével kapcsolatos jogszabályok az SZTE honlapján is publikálásra kerülnek.

2.16.2. Megfelelés IBSZ-nek, szabványoknak és műszaki előírásoknak:

- Az adott szolgáltatást nyújtó szervezeti egység vezetőjének felelőssége a mindenkori IBSZ-nek, a kötelező érvényű szabványoknak és műszaki előírásoknak való megfelelőség biztosítása a nyújtott szolgáltatások vonatkozásában.
- Az adott szolgáltatást nyújtó szervezet vezetőjének kötelessége tájékozódni a kötelező érvényű szabványok és műszaki előírások meglétéről.

2.16.3. 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 IBF jogosult ellenőrizni.
- Egy adott szolgáltatás paramétereinek és egyéb feltételeinek súlyos megsértése esetén az ISZI igazgatója külön rendkívüli biztonsági ellenőrzést és felülvizsgálatot rendelhet el.
- A felülvizsgálatok eredményei alapján az ISZI 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.

2.17. Záró rendelkezések

2.17.1 A jelen Szabályzat és annak függelékei 2021. év május hó 31. napján lépnek hatályba a Szabályzat kihirdetésével. Kihirdetésnek minősül az Egyetem központi honlapján (https://.u-szeged.hu/) történő közzététel. A Szabályzat a következő linken érhető el folyamatosan: https://u-szeged.hu/szabalyzatok

2.17.3 Az Egyetem Karai és egyéb, a szabályzatban nevesített informatikai szolgáltató egységei e Szabályzat hatálybalépését követő 60 napon belül kötelesek saját Szabályzataikat felülvizsgálni és a szükséges módosításokat átvezetni.

2.17.4 A Rektor és a Kancellár gondoskodik arról, hogy e Szabályzatot és mellékleteit, az oktatók, kutatók, más beosztású alkalmazottak és a hallgatók megismerhessék. A Szabályzatot az Egyetem szervezeti egységeiben, az egyetem honlapján az érdekeltek számára hozzáférhetővé kell tenni.

Kelt: Szegeden, 2021. év május hó 31. napján

Prof Dr Rovó László s. k. **Dr. Fendler Judit s. k.**

rektor kancellár

1. melléklet: Titoktartási nyilatkozat üzleti partnerek részére

Titoktartási nyilatkozat

amely létrejött egyrészről a

Szegedi Tudományegyetem
(székhelye: 6720 Szeged, Dugonics tér 13.)
(továbbiakban, mint *SZTE*), másrészről a(z)

……..…….
(székhelye: ……..……..)
(a továbbiakban, mint *Üzleti partner*) 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
   e) amely köztudomású;
   f) amelyet nem az együttműködés megsértésével hoztak nyilvánosságra;
   g) amely nyilvánosságra hozatali korlátozás nélkül a másik Fél birtokában volt már azelőtt, hogy a nyilvánosságra hozó Féltől megkapta volna;
   h) amelyet a használó Fél olyan harmadik Féltől kapott, aki jogszerűen szerezte meg, vagy hozta létre azt, és akit nem köt a nyilvánosságra hozatali tilalom;
   i) amelyet az egyik Fél a másik Fél bizalmas információjának felhasználása nélkül maga hozott létre; vagy
   j) 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.
5. Üzleti partner vállalja, hogy az együttműködés tartalmára vonatkozó bármely információ megszerzésével érintett munkatársával titoktartási nyilatkozatot irat alá, mely titoktartási nyilatkozat legalább az együttműködésben meghatározott megkötéseket kell tartalmazza.

Dátum: Szeged, ……

……	……
SZTE	*Üzleti partner*

1. függelék
Informatikai Felhasználói Szabályzat

Tartalomjegyzék

1. Bevezetés 36
   1.1. A szabályzat célja, hatálya, alapelvei 36
   1.2. A szabályzat közzététele 36
   1.3. A szabályzat megismertetése 36
   1.4. Fogalmak 36
2. Felhasználókra vonatkozó szabályzatok, eljárásrendek 38
   2.1. Központi szintű szabályzatok 38
   2.2. Üzemeltetői szintű, helyi eljárásrendek, rendelkezések 38
3. Felhasználói szabályok 38
   3.1. Felhasználói nyilatkozat 38
   3.2. Rendeltetésszerű használat 39
   3.3. Tilalmak 39
   3.4. Felhasználói magatartás 39
   3.5. A felhasználó jogai 40
4. Felhasználói szabályok megsértése 41
   4.1. Felhasználók szankcionálása 41
   4.2. Anyagi felelősség 41
   4.3. Jogosultságok megszerzésére irányuló kísérlet 41
   4.4. Biztonsági rendszer feltörése 41
   4.5. A jogosultságok átadása 41
   4.6. Személyes jövedelemszerzés 42
   4.7. Meg nem engedett egyéb tevékenység 42

1. Bevezetés

1.1. A szabályzat célja, hatálya, alapelvei

A Szegedi Tudományegyetem (SZTE) számítógépes hálózata (SZTENET) az egyetemen folyó oktatás, kutatás, hazai és nemzetközi kapcsolattartás, továbbá az ügyvitel és a gyógyítás elengedhetetlenül fontos infrastrukturális része. A szabályozás feladata, hogy használatában olyan eljárásokat írjon elő, amelyek a lehető legjobban biztosítják az SZTE közössége számára az infrastruktúra fenti célokra való, rendeltetésszerű használhatóságát. Ezen belül meghatározza a felhasználók feladatait, kijelöli felelősségük határait.

1.1.1. A szabályzat személyi 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.

1.1.2. A szabályzat tárgyi hatálya kiterjed a teljes SZTENET-re. Az SZTENET az egyetem számítógépes hálózata, melynek részét képezik aktív és passzív hálózati eszközök, továbbá minden a hálózatra kötött számítástechnikai berendezés függetlenül attól, hogy az mely egyetemi egység tulajdonában vagy használatában van. A hálózatra nem csatlakoztatott számítástechnikai berendezések nem részei az SZTENET-nek.

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

1.2. A szabályzat közzététele

A Szabályzat az SZTE honlapján mindenki által hozzáférhető.

1.3. A szabályzat megismertetése

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

1.4. Fogalmak

1.4.1. Az **SZTENET** az SZTE számítógépes hálózata. Részét képezik a következő típusú eszközök: passzív adatátviteli vonalak (hálózati összeköttetések, amelyek részben egyetemi tulajdonúak, részben béreltek) és csatlakozók, aktív hálózati elemek (repeaterek, bridge-ek, switchek, routerek, terminál szerverek), továbbá minden hálózatra kötött számítógépes munkaállomás (PC, workstation, terminál, hálózati nyomtató, mobil eszköz) 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 földrajzilag kiterjedt, felépítése a fokozatosan és folyamatosan történő

fejlesztések miatt bonyolult. Szervesen kapcsolódik a város kutató, oktató és közművelődési intézményeinek hálózataihoz. Nem zárt rendszer, kapcsolódik a hazai oktatási, kutatási, könyvtári és közgyűjteményi hálózathoz (HBONE), ezen keresztül más hazai és nemzetközi hálózatokhoz. Regionális szerepköre van a közép- és felsőfokú oktatás, kutatás számára a hazai és nemzetközi hálózatok elérhetőségének biztosításában. A felhasználó oktatók, kutatók, hallgatók és ügyintézők nagyszámú közössége heterogén igényeket és szolgáltatásokat vár, ezek kiszolgálása csak kompromisszumokkal lehetséges. Jelenleg és várhatóan a jövőben is a rendelkezésre álló erőforrások (munkahelyek száma, kiépítettsége, szerverek kapacitásai, sávszélességek) szűkösek, a közösség közérdeke, hogy ezeket az alapvető célokra használjuk.

A hazai és nemzetközi kapcsolatok, információ áramlás szempontjából különösen jelentős szerepe van a HBONE Szeged-Budapest vonalának, amelyet a szegedi oktatási és kutatási régió, kisebb mértékben a középfokú oktatás közösen használ.

Az SZTENET üzemeltetését az Informatikai és Szolgáltatási Igazgatóság (ISZI) és az üzemeltető egységek (tanszék, tanszékcsoport, intézet, klinika, kar, központi oktatási egység, központi egység, hivatal, kollégium, hallgatói önkormányzat, egyetemi érdekképviselet) megosztva végzik. A hallgatók számára tanrendi gyakorlati foglalkozásokra, önálló tanulmányi munkáik végzésére, továbbá kapcsolattartásra és információszerzésre az SZTE biztosítja a lehetőséget (hallgatói laboratóriumok és szolgáltatások formájában).

1.4.2. Egy rendszer vagy számítástechnikai eszköz **üzemeltető**je 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 egyetem rektora üzemeltetőt jelölhet ki. Az üzemeltető egységek köre lefedi a karokat és az SZTE központi gazdálkodásirányítási és igazgatási egységeit. Az üzemeltető egységek aktuális nyilvántartását az egyetemi hálózati rendszeradminisztrátor vezeti.

1.4.3. Az üzemeltető az eszközökhöz **üzemeltető személyzet**et jelöl ki. Az üzemeltető egység üzemeltető személyeit az egység vezetője jelöli ki, ill. bízza meg. Az üzemeltető személyzetben egyes eszközökhöz, eszközcsoporthoz az üzemeltetési szerepköröket meg kell különböztetni.

1.4.4. Az **egyetemi hálózati rendszeradminisztrátor** az Informatikai és Szolgáltatási Igazgatóság (ISZI) vezetője által megbízott személy, aki az SZTENET gerinchálózat kiépítettségét ismeri. Hozzájárulása nélkül a hálózatra új technológiai megoldással működő eszköz nem köthető, és ilyen új szolgáltatás nem indítható. Új technológiai megoldások bevezetésekor véleményező szerepe van, azzal a céllal, hogy az új megoldások megfelelően illeszkedjenek a meglévő infrastruktúrába, és annak működését, rendelkezésre állását, biztonságát ne veszélyeztessék

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

2. Felhasználókra vonatkozó szabályzatok, eljárásrendek

2.1. Központi szintű szabályzatok

A felhasználók számára alapvetően a következő szabályzatok, eljárásrendek tartalmaznak előírásokat az informatikai rendszerek, eszközök használatára vonatkozóan:

- Informatikai Felhasználói Szabályzat (jelen dokumentum) (központi szabályozó dokumentum)
- Informatikai Biztonsági Szabályzat (IBSZ) (központi szabályozó dokumentum)

Ezek a központi szabályzatok az SZTE valamennyi szervezeti egységére egyformán érvényesek.

2.2. Üzemeltetői szintű, helyi eljárásrendek, rendelkezések

Az üzemeltető szervezeti egységek saját hatáskörükben helyi eljárásrendeket dolgozhatnak és hirdethetnek ki, amik alapján az általuk üzemeltetett rendszerek használhatóak. Ezek közül a felhasználókat is érintő eljárásrendek a következők:

- Eszközök adminisztrációjának eljárásrendje
- Felhasználók és jogosultságok adminisztrációjának eljárásrendje
- Incidensek, problémák (rendszerhibák) adminisztrációjának eljárásrendje

Amennyiben a szervezeti egységek sajátosságai indokolják, az IBSZ-t ki lehet egészíteni helyi rendelkezésekkel is, ekkor ezek az IBSZ mellékletét képezik.

3. Felhasználói szabályok

3.1. Felhasználói nyilatkozat

Az SZTE tulajdonában vagy tartós használatában lévő számítógépes infrastruktúra minden felhasználója köteles az Informatikai Felhasználói Szabályzat szerint végezni munkáját. A felhasználói tevékenység megkezdésével a felhasználó elismeri a hálózati és lokális szolgáltatásokra vonatkozó szabályok, a használt eszközre vagy szolgáltatásra vonatkozó korlátozások ismeretét, betartását.

3.2. Rendeltetésszerű használat

A felhasználók a számítógépes infrastruktúrát csak rendeltetésszerűen használhatják. Az üzemeltető, hálózatot érintő esetekben az ISZI vezetője külön engedélye nélkül az eszközöket csak az egyetemi oktatásra, kutatásra, ügyvitelre, az ezekhez kapcsolódó tevékenységekre, valamint a hallgatók tanulmányaik folytatására vehetik igénybe. Különösen **engedélyhez kötött** külső hálózati kapcsolatok létesítése, a hálózaton átalakítások végrehajtása, a felhasználó számára jövedelmet hozó, nem a munkaköréhez tartozó munkavégzés. Csak személyre és csak időszakra engedélyezhető hálózatra dolgozó program fejlesztése, tesztelése. **Nem engedélyezhető** még saját tulajdonú eszközön sem a szórakozás (hálózati játékprogramok futtatása, hálózati forgalmat jelentősen növelő szórakoztató kép- és hanganyagok továbbítása), továbbá olyan tevékenység folytatása vagy szolgáltatás indítása, amely az SZTENET erőforrásait igénybe veszi és nem egyetemi célokat szolgál. Különösen nem engedélyezhető azonosító rendszer nélkül üzemeltetett, de a hálózati szolgáltatásokra konfigurált eszköz jogosulatlan személy használatába átadása (pl. PC mail, web kliens), kapcsolt vagy bérelt vonali csatlakozás létesítése, szerver üzemeltetése jogosulatlan személyek számára, kereskedelmi tevékenység. Ezen szabályzat előírásainak megszegését támogató szoftver nem telepíthető.

3.3. Tilalmak

3.3.1. **Tilos** más felhasználók tevékenységének zavarása, illetéktelen jogosultságok és adatok megszerzése, jogosultságok (felhasználói azonosító, mount jelszó stb.) bárkinek történő átadása, a szoftverek és a hardver elemek megrongálása, működőképességük veszélyeztetése, eszközök jogosulatlan megbontása vagy önkényes átkonfigurálása, szegmensek tartós megszakítása vagy átépítése, a szoftver licence-jogok megsértése (szerzői joggal védett szoftverek másolása).

3.3.2. A felhasználó **nem kísérelheti meg** a számára, ill. a besorolása szerinti felhasználói csoport számára nem engedélyezett erőforrások, szolgáltatások, jogosultságok, kvóták megszerzését. Minden szolgáltatás csak arra a célra vehető igénybe, amelyre azt létrehozták. Különösen nem megengedhető pl. mail, telnet használata nagyméretű adattömegek hálózati átvitelére, mozgatására.

3.4. Felhasználói magatartás

3.4.1. A felhasználó köteles együttműködni a kijelölt helyi és egyetemi üzemeltető személyzettel. Az **üzemeltető személyzet utasításait** még ellenkező véleménye mellett is végre kell hajtania. Ilyenkor utólag élhet panasszal az üzemeltetőnél.

3.4.2. Meghibásodás esetén a hiba elhárítását jogosulatlanul megkezdeni tilos. A kijelölt üzemeltető személyzetet **kell értesíteni** (lehetőleg a hibajelenség minél pontosabb leírásával). A kijelölt üzemeltető személy jogosult a hibák kijavítására intézkedni.

3.4.3. A felhasználó **köteles** az eszköz használatával kapcsolatos fontos események, hibák jelentésére az üzemeltető által előírt formában. Különösen köteles tartozékok, elemek hiányát, szoftver vírus fertőzések gyanúját, felfedezett biztonsági lyukakat, problémákat jelenteni. Köteles más felhasználók figyelmeztetésére a szabályzatok betartására, a nem rendeltetésszerű, ill. a szabályzatokkal ellentétes használat jelentésére.

3.4.4. A lokálisan is elérhető adatok, információk csak a **lokális forrásból** használhatóak (pl. központilag járatott news, levelezési listák, újságok). Engedélyhez kötött az SZTENET-en kívülről ajánlott on-line szolgáltatások (nfs mount, X szervíz stb.) igénybevétele. A felhasználó munkája végzéséhez elegendő, de **erőforráskímélő** eszközök használatára törekedjen (pl. többfunkciós kliens helyett csak a kívánt funkciót nyújtó kliens használata), az üzemeltető erre vonatkozó ajánlásait fogadja el. A több felhasználó által használt eszközök (memória, processzor, tároló- és vonali kapacitásban) erőforrás igényes használatát lehetőleg olyan **időszak**ban gyakorolja, amikor ez más felhasználók munkáját kevésbé zavarja, illetve tartsa be az üzemeltető személyzet ezzel kapcsolatos előírásait.

3.4.5. A saját informatikai eszköz (BYOD) használatakor a felhasználótól elvárt az alábbi javaslatok megvalósítására való törekedés.

- A felhasználónak javasolt a számítógép biztonságos környezet előírásainak való megfeleltetése, így a rendszeresen frissített operációs rendszer, az aktív, rendszeresen frissített vírusvédelem használata és tűzfal alkalmazása.
- Az SZTE érzékeny adatait saját eszközön lehetőség szerint csak titkosítva tároljon a felhasználó. A munkavégzéshez már nem használt adatok kerüljenek másolásra a hálózatra, és törlésre a saját eszközről. Biztonságos tárolási megoldásról a felhasználó az ISZI segítségét kérheti.
- A BYOD eszközön való munkavégzéskor, a tevékenység befejezése vagy megszakításakor, az eszközt ne hagyja a felhasználó felügyelet nélkül, úgy hogy az alkalmazott rendszerből ne jelentkezne ki, vagy az eszközt ne zárolná olyan megoldással, hogy annak feloldásához azonosító adat (jelszó, pin kód) megadása kellene.

3.5. A felhasználó jogai

3.5.1. A felhasználónak joga van tájékoztatást kapni a helyi felhasználói szabályokról, a felelős üzemeltetők személyéről, feladat- és hatásköréről.

3.5.2. A felhasználónak joga van pontos tájékoztatást kapni a felhasználandó gép biztonsági minősítéséről, az elérhető szolgáltatásokról és azok igénybevételének módjáról.

3.5.3. A felhasználó kérheti az üzemeltetőktől a számára megítélt erőforrások biztosítását.

3.5.4. A felhasználó az eszköz által biztosított szolgáltatásokat a felhasználói csoportba sorolástól függően igénybe veheti.

3.5.5. A felhasználó elvárhatja az üzemeltető személyzettől - a felhasználási mód szerinti besorolástól függően - az eszközön tárolt anyagainak, információinak megőrzését, illetéktelen felhasználók hozzáférésének megakadályozását. Az információk megőrzési idejéről a felhasználókat tájékoztatni kell.

3.5.6. A felhasználó panaszt tehet az üzemeltető személyzet intézkedései ellen az üzemeltetőnél.

4. Felhasználói szabályok megsértése

A felhasználói szabályok megsértése esetén a felhasználó az IBSZ 1.6.9 pontjában leírtakra tekintettel szankciókkal sújtható.

4.1. Felhasználók szankcionálása

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.

4.2. Anyagi felelősség

A szabályzatok, illetve az elvárható gondosság be nem tartásából, a nem rendeltetésszerű használatból, rongálásból, az ezekből eredő üzemzavar előidézéséből adódó károkért a felhasználó anyagi felelősséget is visel. Az üzemeltető a felhasználót ezzel együtt az általa üzemeltetett eszközök használatában korlátozhatja, illetve teljesen kizárhatja, súlyosnak minősíthető károkozásért hallgató esetében fegyelmi eljárás, munkavállaló esetében munkáltatói intézkedés kezdeményezhető.

4.3. Jogosultságok megszerzésére irányuló kísérlet

A felhasználó arra irányuló, sikeres vagy sikertelen kísérlete, hogy a számára, ill. a besorolása szerinti felhasználói csoport számára nem engedélyezett erőforrásokat, szolgáltatásokat, jogosultságokat (felhasználói azonosító, dial-up, mount jog stb.), kvótákat megszerezze, a betöréssel ill. a lopással azonos megítélés alá tartozik, így cselekménye súlyosnak minősítendő, az SZTENET használatából való kizárással büntetendő.

4.4. Biztonsági rendszer feltörése

Biztonsági rendszer feltörése - abban az esetben is, ha ez más vétséggel nem is párosul - az SZTENET használatából való kizárással büntetendő és hallgató esetében fegyelmi eljárás, munkavállaló esetében munkáltatói intézkedés indítandó. Belső és külső felhasználó esetében egyaránt meg kell tenni azokat az intézkedéseket, amelyek az Internet közösséget hasonló támadásoktól a későbbiekben esetleg megvédik.

4.5. A jogosultságok átadása

A jogosultságok átadásából, más személyekkel való megosztásából eredő vétségeket az üzemeltető első esetben figyelmeztetéssel, ismétlődő esetben az SZTENET használatából való kizárással vagy felfüggesztéssel bünteti. Amennyiben a jogosultságok átadása egyéb vétségek elkövetésére, vagy jogosulatlan hozzáférésre is alkalmat ad, a felhasználót ki kell zárni az SZTENET használatából.

4.6. Személyes jövedelemszerzés

Abban az esetben, ha a vétség engedély nélküli személyes jövedelemszerzésre irányuló munkavégzés, ebben való közreműködés, ilyen célra törekvő hirdetés, vagy az SZTENET-en keresztül elérhető információk árusítása, a büntetés az SZTENET használatából való felfüggesztés.

4.7. Meg nem engedett egyéb tevékenység

Meg nem engedett egyéb tevékenység (játékprogramok hálózati futtatása, más felhasználók zavarása, üzemzavar okozása stb.) figyelmeztetéssel, ismétlődő esetben az SZTENET használatából való felfüggesztéssel büntetendő.

2. függelék
Informatikai Üzemeltetési Szabályzat

Tartalomjegyzék

1. Bevezetés 44
   1.1. A szabályzat célja, hatálya, alapelvei 44
   1.2. A szabályzat rendszeres felülvizsgálata (a bekezdés szövege új) 44
   1.3. A szabályzat közzététele (a bekezdés forrása az IBSZ) 44
   1.4. A szabályzat megismertetése (bekezdés forrása az IBSZ) 45
   1.5. Üzemeltetői szintű, helyi eljárásrendek, rendelkezések (a bekezdés szövege új) 45
2. Üzemeltetési szabályok 45
   2.2. Az üzemeltetés szervezeti felépítése, alapfeladatok 45
3. Üzemeltetői szabályok 47
   3.1. Az üzemeltető személyzet 47
   3.2. Üzemeltetői jogosultságok 49
   3.3. Az eszközök felhasználási módja 50
4. Üzemeltetési szabályok megsértése, eljárásrendek 51
   4.1. Üzemeltető személyek 51
   4.2. Felhasználók 51
   4.3. Anyagi felelősség 52
   4.4. Jogosultságok megszerzésére irányuló kísérlet 52
   4.5. Biztonsági rendszer feltörése 52
   4.6. A jogosultságok átadása 52
   4.7. Személyes jövedelemszerzés 52
   4.8. Meg nem engedett egyéb tevékenység 52

1. Bevezetés

1.1. A szabályzat célja, hatálya, alapelvei

1.1.1. A Szegedi Tudományegyetem (SZTE) számítógépes hálózata (SZTENET) az egyetemen folyó oktatás, kutatás, hazai és nemzetközi kapcsolattartás, továbbá az ügyvitel és a gyógyítás elengedhetetlenül fontos infrastrukturális része.

A szabályozás célja, hogy üzemeltetésben, működtetésében és fejlesztésében olyan eljárásokat írjon elő, amelyek a lehető legjobban biztosítják az SZTE közössége számára az infrastruktúra fenti célokra való, rendeltetésszerű használhatóságát. Ezen belül meghatározza az üzemeltetők feladatait, kijelöli felelősségük határait.

E szabályzat több pontjában is az Informatikai Biztonsági Szabályzat pontjait ismerteti, az üzemeltetésnél releváns pontokat kiemelve és ha szükséges akkor tovább részletezve.

1.1.2. A szabályzat tárgyi hatálya kiterjed a teljes SZTENET-re. Az SZTENET az egyetem számítógépes hálózata, melynek részét képezik aktív és passzív hálózati eszközök, továbbá minden a hálózatra kötött számítástechnikai berendezés függetlenül attól, hogy az mely egyetemi egység tulajdonában vagy használatában van. A hálózatra nem csatlakoztatott számítástechnikai berendezések nem részei az SZTENET-nek.

1.1.3. A szabályzat személyi hatálya kiterjed az SZTE informatikai szolgáltatásokat nyújtó valamennyi szervezeti egységére, és ezen belül az SZTENET valamennyi üzemeltető személyére.

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

1.1.5. Az SZTENET-ben lehetőség van bármely olyan technikai megoldás befogadására, amely a meglévő szolgáltatásokat nem veszélyezteti, üzembiztonsága az elvárható szintet nyújtja és jelen IBSZ követelményeinek megfelel, azonban ennek validálásához minden új technológiai megoldás esetén gondoskodni kell a megfelelő szakértők bevonásáról, és a véleményük kikéréséről (lásd kifejtve későbbi fejezetben).

1.2. A szabályzat rendszeres felülvizsgálata

A szabályzatot az IMF évente felülvizsgálja, és a felülvizsgálatról készült jegyzőkönyvet vagy jelentést a Szenátusnak tájékoztatásul megküldi. Amennyiben a szabályzatban módosítás szükséges, úgy módosítási javaslatait a Szenátus felé megteszi. A módosított szabályzatot a Szenátus hagyja jóvá és helyezi hatályba.

1.3. A szabályzat közzététele

A Szabályzat az SZTE honlapján mindenki által hozzáférhető.

1.4. A szabályzat megismertetése

Az egyes szervezeti egységek vezetői kötelesek gondoskodni arról, hogy minden informatikai szolgáltatást nyújtó szervezeti egység és üzemeltető személyzet megismerje ezt a szabályzatot.

1.5. Üzemeltetői szintű, helyi eljárásrendek, rendelkezések

1.5.1. Az üzemeltető szervezeti egységek kötelesek kidolgozni és kihirdetni mindazon helyi eljárásrendeket, amelyek alapján az általuk üzemeltetett „A", „B" és „C" osztályú rendszerek használhatóak. Ezek minimum a következők:

- Eszközök adminisztrációjának eljárásrendje (bevételezés, leltárba vétel, személyhez rendelés, igénylés, jóváhagyás, kiadás, visszavétel, selejtezés, leltározás)
- Felhasználók és jogosultságok adminisztrációjának eljárásrendje (igénylésre jogosultak köre, igénylés módja, igénylés elbírálása, beállítás, zárolás, visszavonás, ellenőrzés)
- Incidensek, problémák (rendszerhibák) adminisztrációjának eljárásrendje (bejelentés, eszkalálás, megoldás, lezárás, monitorozás)
- Változáskezelés adminisztrációjának eljárásrendje (fejlesztési igények, jóváhagyások, hibajavítások, konfigurációs beállítások, paraméterezés, patch-elés, tesztelés, élesbe állítás)

1.5.2. Megkülönböztetünk **hálózati szolgáltatás**okat (számítógépes munkahelyről igénybe vehető szerver szolgáltatások, amelyek hálózati forgalommal járnak, pl. mail, web, ftp, gopher, nfs-mount, mirror) és lokális szolgáltatásokat (amelyek esetleg hálózati szolgáltatáson keresztül érhetőek el, pl. szövegszerkesztő). Jelen szabályzat a lokális szolgáltatásokra nem tartalmaz előírásokat, ez az üzemeltető jogköre.

2. Üzemeltetési szabályok

2.1. Az üzemeltetés szervezeti felépítése, alapfeladatok

2.1.1. Tevékenysége során az ISZI az alábbi kiemelt feladatokat látja el az egész SZTE vonatkozásában:

- az Egyetem egészére kiterjedő, oktatáshoz, kutatáshoz valamint az egyetemi adminisztrációhoz kapcsolódó hálózati alapinfrastruktúra, az egyetemi gerinchálózat, a hazai és nemzetközi hálózati kijárat, az egyetemi hálózati központ géptermének valamint az itt elhelyezett eszközöknek, a telekommunikációs központnak és hálózatnak az üzemeltetése, az informatikai és kommunikációs hálózat fejlesztése;
- együttműködés a hazai és nemzetközi kutatói informatikai hálózatokat fejlesztő és üzemeltető szervezetekkel, külső hálózati partnerekkel (szolgáltatókkal, illetve az akadémiai közösséggel), közreműködés a felsőoktatás informatikai hálózatának fejlesztési, finanszírozási terveinek kidolgozásában, az erre alapított szervezetek és bizottságok munkájában;

- a hálózatüzemeltetéshez, a mindenkor aktuális egyetemi címtartomány kezeléséhez kapcsolódó központi adminisztrációs és üzemeltetési feladatok ellátása, az egyetemi hálózat védelme a nem megengedett, rosszindulatú tevékenységekkel szemben;
- az Egyetem központi és kiemelt funkciót biztosító informatikai szolgáltatások számára adatközponti és szerver erőforrások kialakítása, az ezekhez szükséges magas fizikai rendelkezésre állás biztosítása;
- az Egyetem központi infrastruktúra szolgáltatásainak üzemeltetése és fejlesztése, hozzájárulás az oktatási, kutatási és medikai szakterületek alkalmazásainak szolgáltatásbiztosításához, beleértve ezen szakrendszerek teljes körű üzemeltetését, karbantartását, fejlesztését;
- erőforrásai felhasználásával hozzájárulás az Egyetem oktatási, kutatási, gyógyítási alapszolgáltatásainak folyamatos megújításához, közreműködés a társadalmi, gazdasági, technológiai, piaci igényekhez igazodó egyetemi szolgáltatások biztosításában;
- az Egyetem informatikai erőforrásainak működtetésével, használatával kapcsolatos egyetemi szabályzatok elkészítése, karbantartása és betartatása, az informatikai feladatok ellátásában és a szolgáltatások biztosításában közreműködő munkatársak tevékenységének szakmai irányítása és felügyelete;
- egyetemi szintű, központi hálózati, eszköz és vírusvédelmi megoldások létrehozása és üzemeltetése, az egyetemi szintű szoftverbeszerzések koordinációja;
- külön meghatározott szabályok szerint minden egyetemi polgár részére egyenlő esélyű hozzáférési lehetőség biztosítása az Egyetem és a kapcsolódó központi, országos és nemzetközi információs rendszerek informatikai szolgáltatásaihoz;
- felügyeleti, üzemeltetési, fejlesztési hatáskörében a meglévő adminisztrációs, gazdálkodási, humánerőforrás kezelési, fekvő és járóbeteg ellátási, tanulmányi és tudásbázis alapú informatikai szakrendszerekre épülő Vezetői Információs és Irányítási Rendszer létrehozása és üzemeltetése;
- az Egyetem által felhalmozott információs adatvagyon védelme, ennek biztosítására egyetemi szintű Információbiztonsági Irányítási Rendszer kialakítása, működtetése és fejlesztése;
- az informatikai és szolgáltatási feladatok magas szintű támogatását biztosító ügyfélkapcsolati rendszer, ügyfélszolgálat létrehozása, működtetése és fejlesztése

2.2. Az SZTENET üzemeltetése:

2.2.1. Az SZTENET üzemeltetését az ISZI és az üzemeltető egységek (tanszék, tanszékcsoport, intézet, klinika, kar, központi oktatási egység, központi egység, hivatal, kollégium, hallgatói önkormányzat, egyetemi érdekképviselet) megosztva végzik. Az ISZI és az egységek által üzemeltetendő eszközök körét, a kapcsolódási pontokat az SZTENET mindenkori állapotának megfelelően, az üzemeltetők számára is hozzáférhető módon nyilván kell tartani. Az SZTENET fejlesztésénél figyelemmel kell lenni arra, hogy az egységek (elsősorban a karok) saját igényeiknek megfelelő, de más egységekre nézve nem hátrányos fejlesztési lehetőségekhez jussanak.

2.2.2. Az ISZI üzemelteti az SZTENET és egyben a régió oktatási és kutatási célú kijáratát a HBONE-ra a Kormányzati Informatikai Fejlesztési Ügynökség (KIFÜ) megbízásából a KIFÜ által kihelyezett eszközökön keresztül. Az ISZI feladata, hogy érvényesítse azokat a szabályokat, amelyek a HBONE-ra és a rá kapcsolódó intézményekre vonatkoznak.

2.2.3. A hallgatók számára tanrendi gyakorlati foglalkozásokra, önálló tanulmányi munkáik végzésére, továbbá kapcsolattartásra és információszerzésre az SZTE biztosítja a lehetőséget (hallgatói laboratóriumok és szolgáltatások formájában).

2.2.4. Az ISZI a jelen szabályzatban előírt egyetemi nyilvántartásokat vezeti, az üzemeltetők felett a szakmai felügyeletet gyakorolja. Az SZTENET rendellenes működése, meghibásodása, egyes részeinek használhatatlansága esetén az ISZI más egységek üzemeltető személyzetét utasíthatja - a hiba elhárításához szükséges mértékben - az eszközeiken szükséges teendők végrehajtására.

2.2.5. Az egyetem egységei saját eszközeiket maguk üzemeltetik. Üzemeltető személyzetük a szabályzatban a feladatköröknél részletezett bejelentési, véleményeztetési, engedélyeztetési kötelezettségüket az ISZI üzemeltető személyzeténél teljesítik. Ahol a szabályzat másként nem rendelkezik, az engedélyezés joga az ISZI igazgatóját illeti meg. Az ISZI látja el az üzemeltetőket a munkájukhoz szükséges információkkal, adatokkal az üzemeltetők rendszeradminisztrátorain keresztül.

2.2.6. Az üzemeltetők a mindenkori technikai lehetőségeiknek megfelelő maximális mértékben kötelesek a jelen szabályzat előírásainak betartatását hardver és szoftver eszközökkel ellenőrizni és a szabálysértéseket megakadályozni.

2.2.7. Publikus szolgáltatás (pl. anonymous ftp, web, gopher, könyvtári katalógus, távoktatás) csak abban az esetben indítható, ha hardver vagy szoftver eszközökkel biztosítva van, hogy a szolgáltatást igénybe vevő külső felhasználó az SZTENET és a HBONE egyéb szolgáltatásaihoz nem fér hozzá.

2.2.8. Az ISZI az SZTENET működésének javítása, megbízhatóságának növelése érdekében ajánlásokat tehet, ill. saját hatáskörében olyan szabályokat írhat elő, amely a felhasználókat nem korlátozza a szolgáltatások igénybevételében, csupán annak formáit határozza meg (pl. kötelező cache, kötelező kliens használat, névkonvenciók betartása, egyes szolgáltatások kötelezően előírt dedikált szerveren keresztüli igénybevétele, firewall előírások).

3. Üzemeltetői szabályok

3.1. Az üzemeltető személyzet

3.1.1. Egy rendszer vagy számítástechnikai eszköz **üzemeltető**je 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 egyetem rektora üzemeltetőt jelölhet ki. Az üzemeltető egységek köre lefedi a karokat és az SZTE központi gazdálkodásirányítási és igazgatási egységeit. Az üzemeltető az eszközökhöz **üzemeltető személyzet**et jelöl ki.

3.1.2. Az üzemeltető egységek aktuális nyilvántartását az egyetemi hálózati rendszeradminisztrátor vezeti. Az üzemeltető az egyetemi hálózati rendszeradminisztrátor egyetértésével besorolja az eszközt a szabályzat szerinti **felhasználási mód**ba. A jelen szabályzatban az adott felhasználási módú eszközre kötelezően előírt feladatkörökhöz az üzemeltető köteles üzemeltető személyt kijelölni.

Az üzemeltető egység üzemeltető személyeit az egység vezetője jelöli ki, ill. bízza meg. Az üzemeltető személyzetben egyes eszközökhöz, eszközcsoporthoz az üzemeltetési szerepköröket meg kell különbözteni
Üzemeltető egységenként a rendszeradminisztrátori feladatkörön kívüli funkciókat a szervezeti egység méretétől, a feladatok mennyiségétől, az üzemeltetett eszközök felhasználási módjától és mennyiségétől függően több személy is betöltheti, illetve egy személy több funkciót is elláthat.

3.1.3. Az egyetemi hálózati rendszeradminisztrátor az Informatikai és Szolgáltatási Igazgatóság (ISZI) vezetője által megbízott személy, aki az SZTENET gerinchálózat kiépítettségét ismeri. Hozzájárulása nélkül a hálózatra új technológiai megoldással működő eszköz nem köthető, és ilyen új szolgáltatás nem indítható. Új technológiai megoldások bevezetésekor véleményező szerepe van, azzal a céllal, hogy az új megoldások megfelelően illeszkedjenek a meglévő infrastruktúrába, és annak működését, rendelkezésre állását, biztonságát ne veszélyeztessék. Jogkörének egy részét átadhatja valamely egység rendszeradminisztrátorának az átadott jogok és kötelezettségek pontos körülhatárolásával. Előírja azon adatok körét, kívánt mélységét és formáját, amelyek az eszközök egyetemi gerinchálózatra kapcsolásához szükségesek. Kiadja a hálózatra a csatlakoztatási paramétereket (cím, név, megengedett szolgáltatások, engedélyezett felhasználói kör). Ellátja a munkájuk végzéséhez szükséges információkkal a rendszeradminisztrátorokat. A rendszeradminisztrátoroktól jogosult megkérni azon adatokat, amelyek nyilvántartására az üzemeltető kötelezett (felhasználók, naplózás, szolgáltatások). Utasíthatja a rendszeradminisztrátorokat az SZTENET működését javító intézkedéseinek végrehajtására (proxy szerverek használata stb.).

Az egyetemi hálózati rendszeradminisztrátor elkészíti a jelen helyzetnek megfelelően az üzemeltetők nyilvántartását, ezek szolgáltatásainak, üzemeltető személyzetüknek feltüntetésével. A nyilvántartást folyamatosan aktualizálja az egységek rendszeradminisztrátorainak bejelentései alapján. A nyilvántartásnak mindenkor egyértelműen meg kell különböztetnie a központi (az ISZI hatáskörébe tartozó) és az egységek (karok) szolgáltatás-csoportjait. A nyilvántartásból a felhasználókat is érintő információkról a felhasználókat folyamatosan tájékoztatni kell.

Az egyetemi hálózati rendszeradminisztrátor kidolgozza azokat a formákat, módokat, ahogyan az engedélyeztetési, bejelentési kötelezettségeiket az egységek üzemeltető személyzetei teljesítik.

3.1.4. A **rendszeradminisztrátor** feladata a kezelésére bízott eszközök szoftveres karbantartása, a felhasználók szoftveres menedzselése, jogosultságainak beállítása, a szabályzatban megkívánt naplózási adatok előállítása. A rendszergazda szolgáltatja a rendszeradminisztrátor feladatainak ellátásához szükséges adatokat. A rendszergazda feladata továbbá, hogy minden lehetséges eszközzel megakadályozza a hálózati jogosultságokkal való visszaélés lehetőségét a kezelésében lévő eszközökön. Amennyiben az eszközt hallgatók is használják, félévenként elkészíti a hallgatói számítógép használati munkarendet, amelynek ismeretét és betartását az igénybe vevő hallgatók aláírásukkal igazolnak. A rendszeradminisztrátori feladatkörre minden üzemeltetőnek megbízást kell adnia (kari, könyvtári, kollégiumi stb. rendszeradminisztrátor).

3.1.5. A **support munkatárs** felügyeli az üzemeltető kezelésében lévő hardver és szoftver eszközök működését. Feladata a felhasználók munkájának segítése, információszolgáltatás az eszközökön használható szolgáltatásokról, felhasználói problémák megoldása, a bonyolultabb hardver és szoftver problémák jelentése szállítóknak illetve a rendszergazdának. Felügyeli a felhasználók tevékenységét abból a szempontból, hogy az eszközök rendeltetésszerű használata teljesüljön. Ellátja a vagyon- és tűzvédelmi feladatokat az üzemeltető által előírt formában.

3.1.6. A **postamester** feladata a felhasználók elektronikus levelezésének felügyelete, az azzal kapcsolatos problémák megoldása, illetve azon felhasználók kiszűrése, akik az elektronikus levelezést nem a rendeltetésének megfelelően (pl. nagyméretű adatok forgalmazására) használják. A postamester köteles minden eszközzel védeni a levéltitkot, nem használhatja ki a postamesteri jogosultságaiból adódó hozzáférési jogait a levéltitok megsértésére. A postamester köteles egy olyan e-mail címet megadni, amelyen neki az elektronikus levelezéssel kapcsolatos problémákat, észrevételeket jelenteni lehet. Az ezen szabályokat meg nem tartó üzemeltetőt az egyetemi hálózati rendszeradminisztrátor a postamester megváltoztatására, tartalmi problémák esetén az elektronikus levelezés szolgáltatás megszüntetésére szólíthatja fel.

3.2. Üzemeltetői jogosultságok

3.2.1. Az üzemeltető személyekre a felhasználói szabályok is érvényesek, azzal a módosítással, hogy számukra az üzemeltető helyett az ISZI látja el a felügyeletet (a szabályok betartásának figyelemmel kísérését). Munkakörénél fogva az üzemeltető személy a felhasználóknál bővebb jogosultságokkal rendelkezik. Bővebb jogosultságával nem élhet vissza, nem használhatja fel a felhasználók jogainak megsértésére függetlenül attól, hogy jelen szabályzatból eredő vagy más, általánosan elismert jogról van szó. Amennyiben az üzemeltető személy a felhasználói vagy üzemeltetői szabályokat sérti, vagy szándékosan visszaél bővebb jogosultságával, az üzemeltetésből ki kell zárni, egyéni felhasználási módú eszköz esetében az eszközt az SZTENET-ről el kell távolítani.

3.2.2. Tiszteletben kell tartania azokat a szabályokat, kialakult szokásokat, követnie kell azokat az eljárásmódokat, amelyek a hazai és nemzetközi akadémiai hálózatok közösségeiben elfogadottak. Érvényesítenie kell azokat a szabályokat, amelyeket az egyetem elfogad (pl. a HUNGARNET Egyesület, az NIIF Program, az Internet információs infrastruktúrára vonatkozó szabályai).

3.2.3. Adat- és titokvédelem: Az üzemeltetői jogosultságok által megszerezhető, ill. a tevékenységek naplózásával, a forgalom ellenőrzésével, továbbá más számítástechnikai eszközökkel gyűjtött információk csak az SZTENET működésének javítására, a rendellenes használat kiszűrésére, a szabálysértő magatartás felderítésére használhatók. Egyéb célokra való információgyűjtésre vagy felhasználásra az SZTE felső vezetése adhat utasítást. Azon személyeket, akik ezen információk gyűjtésére jogosultak, ill. az információk birtokába juthatnak, az üzemeltető jelöli ki a lehető legszűkebb körre szorítkozva.

3.3. Az eszközök felhasználási módja

Az üzemeltető az egyetemi hálózati rendszeradminisztrátorral egyetértésben egyes eszközöket, eszközcsoportokat felhasználási mód szerint kategóriákba sorol.

- "A" speciális biztonsági követelményű eszköz (pl. konfigurálható hálózati aktív eszköz, személyi, gazdasági, hallgatói nyilvántartó eszközcsoportok),
- "B" személyi azonosító rendszerrel ellátott eszköz (pl. többfelhasználós Unix szerver),
- "C" személyi vagy egyedi felhasználású eszköz (pl. oktató dolgozószobájában csak a saját használatában levő PC),
- "D" néhány felhasználós, személyi azonosító rendszer nélküli eszköz (pl. irodában, kollégiumi szobában elhelyezett PC),
- "E" teljesen szabad felhasználású eszköz (pl. tantermi, olvasótermi, folyosói PC).

A felhasználási módba való sorolás meghatározza, hogy az adott eszköz milyen típusú szolgáltatások futtatására alkalmazható, illetve milyen nyilvántartást kell ezzel az eszközzel kapcsolatosan vezetni.

3.3.1. Az **"E"** felhasználási módba tartozó eszközöknél a felhasználókra érvényes jogok és kötelezettségek a meghatározóak. Ezeknek az eszközöknek a hálózathoz való hozzáférését a biztonsági követelményeknek megfelelően szűrni kell, hardver és szoftver eszközökkel biztosítani kell, hogy csak az egyetem publikus szolgáltatásai legyenek rajtuk keresztül elérhetőek.

3.3.2. A **"D"** felhasználási módba tartozó eszközök esetében a felhasználási jogot az eszköz rendszergazdájától az eszköz nyilvántartási naplójába tett bejegyzéssel kell kérni, a felhasználó ezen teszi meg a felhasználói szabályok betartására vonatkozó írásos nyilatkozatát. A rendszergazda feladatkörhöz személyt kell rendelni (pl. irodavezető).

3.3.3. A **"C"** felhasználási módba tartozó eszközöknél a felhasználó (aki általában a rendszergazda is) nyilvántartása az eszköz nyilvántartásával összevontan kezelendő. A rendszergazda felelős az eszköz rendeltetésszerű használatáért, a jogosulatlan hozzáférés megakadályozásáért.

3.3.4. A **"B"** felhasználási módba tartozó eszközöknél a felhasználó egy igénylő lapon szolgáltat adatokat, igényel erőforrásokat, és írja alá a szabályzatok betartásáról szóló nyilatkozatot. Hallgatónak tanévenként meg kell újítania igényét. Az üzemeltető személyzet egy kijelölt tagja bírálja el a kéréseket, s veszi nyilvántartásba a felhasználót. A felhasználó nyilvántartása az operációs rendszer által nyújtott eszközökkel is lehetséges. A rendszeradminisztrátor és a rendszergazda feladatkörökhöz személyt kell rendelni. Hozzáférési jog nélkül az eszközön csak az egyetem lokális, publikus szolgáltatásai lehetnek elérhetőek (pl. guest, demo, anonymous user jogok csak ezekre szólhatnak).

3.3.5. Az **"A"** felhasználási módba tartozó eszközöknél a "B" mód előírásait, továbbá az SZTE „Adatvédelmi Szabályzatának" előírásait meg kell tartani. Ezen kívül szükséges a felhasználók tevékenységének naplózása (pl. log file segítségével). A felhasználó és üzemeltető személyek csak a munkájuk végzéséhez elengedhetetlen jogosultságokkal rendelkezhetnek. Bizalmas, titkos vagy törvényekben előírt adatvédelem alá eső adatok tárolása esetén az adatvédelemre az üzemeltetőnek szabályzatot kell alkotnia és ennek betartására az ellenőrzés módját elő kell írnia.

3.3.6. A felhasználási módtól függetlenül a lehetséges eszközökkel mindig biztosítani kell a felhasználók személyre, időpontra és a használt eszközre szóló azonosításának lehetőségét.

4. Üzemeltetési szabályok megsértése, eljárásrendek

A felhasználói szabályok megsértése esetén a felhasználó az IBSZ 1.6.9 pontjában leírtakra figyelemmel az alábbiakban részletezett szankciókkal sújtható.

4.1. Üzemeltető személyek

A szabályzatot sértő üzemeltető személy ellen munkáltatói intézkedés indítható. Amennyiben a szabálysértés más egyetemi szabályok sértésével együtt valósul meg, az egyetemi szabályzatok szerint kell eljárni. A szabályzatot súlyosan sértő üzemeltető személyt az üzemeltető köteles az üzemeltető személyzet tagjai köréből véglegesen kizárni.

4.2. 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.

4.3. Anyagi felelősség

A szabályzatok, illetve az elvárható gondosság be nem tartásából, a nem rendeltetésszerű használatból, rongálásból, az ezekből eredő üzemzavar előidézéséből adódó károkért a felhasználó anyagi felelősséget is visel. Az üzemeltető a felhasználót ezzel együtt az általa üzemeltetett eszközök használatában korlátozhatja, illetve teljesen kizárhatja, súlyosnak minősíthető károkozásért hallgató esetében fegyelmi eljárás, munkavállaló esetében munkáltatói intézkedés kezdeményezhető.

4.4. Jogosultságok megszerzésére irányuló kísérlet

A felhasználó arra irányuló, sikeres vagy sikertelen kísérlete, hogy a számára, ill. a besorolása szerinti felhasználói csoport számára nem engedélyezett erőforrásokat, szolgáltatásokat, jogosultságokat (felhasználói azonosító, mount jog stb.), kvótákat megszerezze, a betöréssel ill. a lopással azonos megítélés alá tartozik, így cselekménye súlyosnak minősítendő, az SZTENET használatából való kizárással büntetendő.

4.5. Biztonsági rendszer feltörése

Biztonsági rendszer feltörése - abban az esetben is, ha ez más vétséggel nem is párosul - az SZTENET használatából való kizárással büntetendő és hallgató esetében fegyelmi eljárás, munkavállaló esetében munkáltatói intézkedés indítandó. Belső és külső felhasználó esetében egyaránt meg kell tenni azokat az intézkedéseket, amelyek az Internet közösséget hasonló támadásoktól a későbbiekben esetleg megvédik.

4.6. A jogosultságok átadása

A jogosultságok átadásából, más személyekkel való megosztásából eredő vétségeket az üzemeltető első esetben figyelmeztetéssel, ismétlődő esetben az SZTENET használatából való kizárással vagy felfüggesztéssel bünteti. Amennyiben a jogosultságok átadása egyéb vétségek elkövetésére, vagy jogosulatlan hozzáférésre is alkalmat ad, a felhasználót ki kell zárni az SZTENET használatából.

4.7. Személyes jövedelemszerzés

Abban az esetben, ha a vétség engedély nélküli személyes jövedelemszerzésre irányuló munkavégzés, ebben való közreműködés, ilyen célra törekvő hirdetés, vagy az SZTENET-en keresztül elérhető információk árusítása, a büntetés az SZTENET használatából való felfüggesztés.

4.8. Meg nem engedett egyéb tevékenység

Meg nem engedett egyéb tevékenység (játékprogramok hálózati futtatása, más felhasználók zavarása, üzemzavar okozása stb.) figyelmeztetéssel, ismétlődő esetben az SZTENET használatából való felfüggesztéssel büntetendő.