SZEGEDI TUDOMÁNYEGYETEM

INFORMATIKAI BIZTONSÁGI SZABÁLYZATA

Szeged, 2026. március 30.

SZ-7/2025/2026.

Tartalom

A Szegedi Tudományegyetem Szenátusa a Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény és a Magyarország kiberbiztonságáról szóló törvény végrehajtásáról szóló 418/2025. (XII. 23.) Korm. rendelet, valamint a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről szóló 7/2024. (VI. 24.) MK rendelet alapján, figyelemmel az Európai Parlament és a Tanács (EU) 2022/2555 irányelvére (NIS2) az alábbi Információbiztonsági szabályzatot alkotta meg.

I. A SZABÁLYZAT CÉLJA

1. § A szabályzat célja, hogy az Szegedi Tudományegyetem (a továbbiakban: SZTE, Egyetem) elektronikus információs rendszereinek, adatvagyonának és informatikai szolgáltatásainak biztonságát egységes elvek mentén szabályozza, biztosítva azok megbízható, biztonságos és jogszerű működését.

2. § Az SZTE az adatvédelemre és információbiztonságra vonatkozó hazai és nemzetközi jogszabályoknak való megfelelés érdekében jelen szabályzatban meghatározza azokat a követelményeket, eljárásokat és felelősségi köröket, amelyek a fenti célok megvalósításához szükségesek. Ennek keretében:

a) meghatározza az SZTE információbiztonsági célkitűzéseit és az ezek eléréséhez szükséges alapelveket,
b) kijelöli a szerepköröket, felelősségeket és döntési jogköröket,
c) keretet ad az információbiztonsági programok, projektek, védelmi intézkedések és ellenőrzések megtervezéséhez, végrehajtásához és felügyeletéhez,
d) biztosítja az információbiztonsági tevékenységek és az SZTE szabályzatainak, utasításainak és folyamatainak összhangját.

II. A SZABÁLYZAT HATÁLYA

3. § A szabályzat személyi hatálya kiterjed az SZTE valamennyi szervezeti egységére, valamennyi foglalkoztatottjára, valamennyi az Egyetemmel hallgatói, valamint doktorjelölti jogviszonyban álló személyre (a továbbiakban: hallgatók), továbbá minden olyan természetes vagy jogi személyre, aki az SZTE Elektronikus Információs Rendszereihez (a továbbiakban: EIR) hozzáfér, azokat működteti vagy karbantartja, illetve az információbiztonsági programok és projektek megvalósításában részt vesz.

4. § A szabályzat tárgyi hatálya kiterjed az SZTE által használt vagy üzemeltetett informatikai rendszerekre, hálózatokra, adatbázisokra, alkalmazásokra, eszközökre és minden olyan digitális platformra, amely az SZTE működését közvetlenül vagy közvetetten támogatja, valamint a felhőalapú szolgáltatásokra és innovatív megoldásokra, ahol az SZTE üzemeltetést nem végez, de az Egyetem felhasználója azokban adatot kezel vagy információt oszt meg.

5. § A Szabályzat kiemelten vonatkozik:
a) az SZTE valamennyi EIR-jére, rendszerelemére és rendszerszolgáltatására;
b) az információbiztonsági programokra és projektekre;
c) az ellátási lánc információbiztonságát érintő tevékenységekre;
d) a kockázatkezelési folyamatokra és azok dokumentációjára;

e) a biztonsági teljesítménymérésre, felügyeletre és jelentéstételre;
f) a vezetői szintű információbiztonsági beszámolási és döntéshozatali mechanizmusokra;
g) az informatikai és információbiztonsági fejlesztésekre, továbbfejlesztésekre.

III. ÉRTELMEZŐ RENDELKEZÉSEK

6. § Ezen szabályzat alkalmazásában:

1. *Adatgazda:* az a személy, aki az adatok kezeléséért felel, ismeri az adatok tulajdonságait, dönt a hozzáférési jogosultságokról. Egy alkalmazáson belül több adatgazda is lehet.
2. *Alkalmazásgazda:* Az alkalmazásgazda az a szakmai kompetenciával rendelkező, felhasználói területi kulcsfelhasználó munkatárs, aki az adott alkalmazás teljes funkcionalitását, felhasználói üzleti logikáját ismeri, valamint a rendszer funkcióit rendszeresen alkalmazza. Támogatja az érintett rendszert használó szakterületi munkatársakat a rendszer napi használatában, valamint segítséget nyújt a változtatási igények megfogalmazásában.
3. *Biztonsági esemény:* nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat, amely az elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, és amelynek hatására az elektronikus információs rendszer által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elveszhet, illetve megsérülhet.
4. *Érzékeny adat:* az olyan adat, amit csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetnek meg, használhatnak fel, illetve rendelkezhetnek a felhasználásáról;
5. *Információbiztonsági incidens:* olyan esemény, amely veszélyezteti az elektronikus információs rendszereken tárolt, továbbított vagy kezelt adatok vagy az e rendszerek által kínált vagy azokon keresztül elérhető szolgáltatások rendelkezésre állását, sértetlenségét vagy bizalmasságát.
6. *Információbiztonsági incidenskezelés:* minden olyan tevékenység és eljárás, amelynek célja az információbiztonsági incidens megelőzése, észlelése, elemzése és elszigetelése vagy az információbiztonsági incidensre való reagálás és az információbiztonsági incidenst követően a működés helyreállítása.
7. *Kritikus adat:* a személyes adat vagy valamely jogszabállyal védett adat.
8. *Kockázatelemzés:* e szabályzat vonatkozásában kockázatelemzés alatt kizárólag az elektronikus információs rendszereket érintő kockázatértékelést értjük.

IV. INFORMÁCIÓBIZTONSÁGI POLITIKA

7. § A Szegedi Tudományegyetem elkötelezett az információbiztonsági megfelelőség és a nemzetközi szabványok szerinti működés mellett. Az SZTE célja, hogy teljesítse a kiberbiztonsági jogszabályokban foglalt információbiztonsági követelményeket, különös tekintettel a kritikus szolgáltatások védelmére, a kockázatkezelésre, az incidenskezelésre és az üzletmenet-folytonosság biztosítására.

8. § A megfelelőség biztosítása érdekében az SZTE az alábbi feladatokat látja el:

a) Elvégzi az informatikai biztonsági szabályzat és folyamatok rendszeres felülvizsgálatát és frissítését a jogszabályi változásoknak megfelelően.
b) Alkalmazza a belső kontrollmechanizmusokat, önértékeléseket és auditokat.
c) Teljesíti a Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény (a továbbiakban: Kiberbiztonsági tv.) és a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről szóló 7/2024. (VI. 24.) MK rendelet által előírt kockázatelemzési, incidenskezelési, képzési és jelentési kötelezettségeket.
d) Naprakészen tartja a megfelelőségi dokumentációkat, nyilvántartásokat és tanúsítványokat, valamint elérhetővé teszi azokat az ellenőrző hatóságok számára.
e) Megszervezi vezetői szinteken és kulcsterületeken a célzott megfelelőségi képzéseket, amelyek segítik a szabályozási környezet megértését és a gyakorlati alkalmazását.

9. § Az SZTE fokozatosan felszámolja a szigetszerű, decentralizált rendszereket, és helyettük integrált, központilag menedzselt szolgáltatásokat vezet be, amelyek megfelelnek a korszerű információbiztonsági és üzemeltetési követelményeknek. Az infrastruktúra egységesítési törekvés kiemelten az alábbi területeken valósul meg:

a) **Hálózati architektúra**: Az SZTE campusain és telephelyein egységes, biztonságos hálózati struktúra kerül kialakításra, amely támogatja a központi felügyeletet, a szegmentálást, valamint a behatolásmegelőzést és észlelést.
b) **Szerver- és tárolórendszerek (adathordozók védelme)**: A fizikai és virtuális szerverek konszolidációja révén csökken a redundancia, nő az energiahatékonyság, és javul az adatbiztonság. A tárolási megoldások központi menedzsmenttel, titkosítással és biztonsági mentési protokollokkal működnek.
c) **Alkalmazás- és szolgáltatásmenedzsment**: Az SZTE informatikai szolgáltatásait – például levelezés, fájlmegosztás, tanulmányi rendszerek – egységes platformokon keresztül biztosítja, amelyek központilag frissíthetők, monitorozhatók és auditálhatók.
d) **Eszközmenedzsment**: A végfelhasználói eszközök (pl. számítógépek, mobiltelefonok, nyomtatók) egységes nyilvántartásba kerülnek, és központi eszközfelügyeleti rendszer biztosítja a konfigurációs, biztonsági és frissítési szabályok betartását.

10. § Az egységesítés célja az informatikai rendszerek üzemeltetési hatékonyságának növelése, a biztonsági kockázatok csökkentése, valamint a gyorsabb incidensreakció. Az integrált szolgáltatásmenedzsment révén az Informatikai Szolgáltatási Igazgatóság (a továbbiakban: ISZI) átlátható, mérhető és szabályozható módon biztosítja az SZTE digitális működésének stabilitását.

11. § Az infrastruktúra egységesítésének megvalósítása szakaszosan történik, az érintett szervezeti egységek bevonásával, és az ISZI koordinációjával. A folyamat során kiemelt figyelmet kap az adatvédelem, a szolgáltatás-folytonosság és a felhasználói élmény megőrzése.

V. ALAPELVEK

12. § Az SZTE információbiztonsági működését az alábbi alapelvek határozzák meg:

a) **Bizalmasság**: az elektronikus információs rendszerben tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról.
b) **Sértetlenség**: az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az az elvárt forrásból származik, azaz hiteles, valamint a származás ellenőrizhetőségét, bizonyosságát, azaz letagadhatatlanságát is, illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható.
c) **Rendelkezésre állás**: az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak.
d) **Helyreállíthatóság:** Katasztrófa vagy egyéb incidens esetén a kritikus információs vagyoneszközök és rendszerek helyreállíthatóak.
e) **Teljeskörű védelem**: A védelem minden rendszerelemre, rétegre és eszközre kiterjed.
f) **Zárt védelem**: A védelmi intézkedések szabályozott, szerves egészet alkotnak.
g) **Kockázatarányos védelem**: A védelmi szint a kockázatokkal arányos.
h) **Folyamatos védelem**: A védelem a rendszer teljes életciklusa alatt fennáll.
i) **Kivételkezelés:** A szabályzatban és a kapcsolódó eljárásrendekben nem szereplő, egyedi esetek kezelése az SZTE vezetésének döntése alapján történik.

VI. SZERVEZETI STRUKTÚRA ÉS FELELŐSSÉGI KÖRÖK

13. § Az Egyetem az informatikai infrastruktúra egységes, biztonságos és fenntartható üzemeltetését az Informatikai Szolgáltatási Igazgatóság (a továbbiakban: ISZI) segítségével biztosítja.

14. § Az SZTE információbiztonsági irányításában részt vevő szerepkörök feladatait és döntési jogköreit az alábbi felsorolás foglalja össze. A felelősségi és hatásköri rend egyértelmű meghatározása biztosítja az információbiztonsági programok, intézkedések és folyamatok átláthatóságát, elszámoltathatóságát és ellenőrizhetőségét.

15. § Kancellár: az Egyetem működtetését végző vezető, aki biztosítja az elektronikus információs rendszer működésének feltételeit.

a) **Felelősség/feladat**: Felelős az információbiztonsági célok teljesüléséért, gondoskodik a belső szabályozók kiadásáról és biztosítja az információbiztonsági célok eléréséhez szükséges erőforrásokat.

b) **Hatáskör/jogosultság**: Jelen szabályzatot a Szenátus elé terjeszti és gondoskodik a kapcsolódó szabályozók kiadásáról, valamint rendelkezik az erőforrások felett.

16.§ Informatikai Szolgáltatási Igazgatóság: az SZTE informatikai rendszereit kezelő szervezet: gondoskodik az informatikai rendszerek stratégiai és operatív kezeléséről.

a) **Felelősség/feladat:** Részt vesz az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában.
b) **Hatáskör/jogosultság:** Rendszeradminisztrátor szintű hozzáféréssel rendelkezik a kritikus rendszerekhez és jogosult a hozzáférések kezelésére és technikai változtatások végrehajtására.

17. § Elektronikus információs rendszer biztonságáért felelős személy (a továbbiakban: EIRBF): Ellátja a kockázatelemzési feladatokat az EIR-ekre vonatkozóan, elvégzi jelen szabályzat és kapcsolódó szabályozók felülvizsgálatát, valamint a gyakorlati megvalósulás ellenőrzését.

a) **Felelősség/feladat:** Előkészíti és elfogadását követően megküldi a kiberbiztonsági hatóság részére a szervezet információbiztonsági szabályzatát**,** véleményezi az elektronikus információs rendszerek biztonságát érintő szabályozókat, segíti a biztonsági intézkedések kidolgozását, bevezetését és felügyeletét. Ellenőrzi az elektronikus információbiztonságra vonatkozó szabályok betartását, felülvizsgálja egyetemi szabályozók jogszabályokkal való összhangját, a tapasztalatokról biztonsági helyzetértékelést készít az Egyetem vezetése számára. Felülvizsgálja az auditok során esetlegesen keletkező információbiztonsági intézkedési tervek végrehajtását, rendszeresen beszámol a vezetés részére az információbiztonság helyzetéről. Feladatai ellátása során együttműködik az érintett szervezeti egységekkel, valamint kapcsolatot tart a jogszabályban kijelölt kiberbiztonsági hatóságokkal és incidenskezelő szervezettel, továbbá működteti a kockázatmenedzsment keretrendszert.
b) **Hatáskör/jogosultság:** Hozzáférést kérhet minden releváns biztonsági dokumentációhoz és rendszerhez a feladatvégrehajtáshoz szükséges legkisebb jogosultsággal, valamint javaslattételi jogkörrel rendelkezik a szabályzatmódosítások és információbiztonsági intézkedések vonatkozásában.

18. § Stratégiai és Fejlesztési Főigazgatóság (a továbbiakban: SFF): az általa kiadott **s**zabályozó dokumentumok nyilvántartása, rendszerbe illesztése, hatáskörébe tartozó kontroll tevékenységek (auditok) megszervezése, végrehajtása, javítási intézkedések megvalósulásának kontrollja.

19. § Jogi és Igazgatási Igazgatóság (a továbbiakban: JII): az egyetemi szintű szabályozók kiadása, nyilvántartása, valamint a jogszabályi megfelelés támogatása.

20. § Adatvédelmi tisztviselő (a továbbiakban: DPO): Támogatást nyújt az adatvédelmi megfelelés biztosítása érdekében.

21. § Adatgazda: A felelősségi körébe tartozó információs vagyonelemek tekintetében gyakorolja a szakmai döntési jogkört, gondoskodik azok osztályozásáról, valamint a hozzáférési jogosultságok meghatározásáról és engedélyezéséről. Az adatosztályozás és az elektronikus információs rendszerek biztonsági osztályba sorolása alapján meghatározza az alkalmazandó védelmi intézkedéseket.

22. § Szerződéses partnerek: Együttműködnek a szerződéses biztonsági követelmények betartásában, valamint részt vesznek az incidenskezelésben.

VII. KOCKÁZATMENEDZSELÉS ÉS BIZTONSÁGI OSZTÁLYBA SOROLÁS

23. § A Szegedi Tudományegyetem a kockázatmenedzsment rendszerének részeként az információbiztonság fenntartása érdekében rendszeres kockázatelemzést végez, amelynek célja az informatikai rendszerek, adatok és szolgáltatások biztonságát veszélyeztető tényezők azonosítása, értékelése és kezelése (Értékelés, engedélyezés és monitorozás). A kockázatelemzés során figyelembe kell venni a fenyegetések valószínűségét, a lehetséges hatásokat, valamint az érintett rendszerek és adatok kritikus jellegét. A Kancellár kijelöli a kockázatmenedzsment folyamat felelőseit, névvel és felelősségi körrel. Megjelöl egy kockázatkezelésért felelős vezetőt, valamint minden lényeges EIR esetében tisztázza az engedélyező szerepkört

24. § A kockázatelemzést kritikus rendszerek esetén évente, nem kritikus rendszerek esetén 2 évente el kell végezni, illetve minden jelentős informatikai változás, új rendszer bevezetése vagy biztonsági incidens után meg kell ismételni. Az elemzés eredménye alapján az ISZI meghatározza a szükséges védelmi intézkedéseket, prioritásokat és erőforrásokat, amelyekkel csökkenthetők vagy kezelhetők a feltárt kockázatok.

25. § A kockázatelemzés eredményeire építve az SZTE biztonsági osztályozást alkalmaz az informatikai rendszerekre, adatokra és szolgáltatásokra. Az osztályozás célja, hogy azonosítsa az egyes elemek biztonsági szintjét, és meghatározza az alkalmazandó védelmi intézkedéseket. A biztonsági osztályozás figyelembe veszi:

a) az adat jellegét (pl. személyes, különleges, kutatási, pénzügyi),
b) az adatkezelés célját és jogalapját,
c) a rendszer üzleti és oktatási kritikusságát,
d) a jogszabályi és szerződéses kötelezettségeket.

26. § A kockázatelemzés lezárását követően a dokumentumok a szükséges intézkedések megtétele érdekében megosztásra kerülnek az érintettekkel, és minden esetben megküldésre kerülnek:

a) az EIRBF,
b) az ISZI,
c) a Kancellár.

részére.

27. § A biztonsági osztályozás alapján az SZTE három fő védelmi szintet különböztet meg:

a) **Alap biztonsági osztály**: általános informatikai rendszerek, nyilvános adatok.
b) **Jelentős biztonsági osztály**: érzékeny adatok, belső használatú rendszerek.
c) **Magas biztonsági osztály**: különleges személyes adatokat kezelő, valamint az SZTE működését közvetlenül jelentősen befolyásoló rendszerek.

28. § (1) Az „alap” biztonsági osztály esetében legfeljebb csekély káresemény következhet be, mivel:

a) az elektronikus információs rendszerben jogszabály által nem védett adat vagy legfeljebb kis mennyiségű személyes adat sérülhet,
b) a szervezet üzleti vagy ügymenete szempontjából csekély értékű, vagy csak belső (szervezeti) szabályzóval védett adat vagy rendszer sérülhet,
c) a lehetséges társadalmi-politikai hatás a szervezeten belül kezelhető, vagy
d) a közvetlen és közvetett anyagi kár a szervezet éves költségvetésének vagy nettó árbevételének 1%-át nem haladja meg.

(2) A „jelentős” biztonsági osztály esetében közepes káresemény következhet be, mivel:

a) nagy mennyiségű személyes adat, illetve különleges személyes adat sérülhet,
b) személyi sérülések esélye megnőhet (ideértve például a káresemény miatti ellátás elmaradását, a rendszer irányítatlansága miatti veszélyeket),
c) a szervezet üzleti vagy ügymenete szempontjából érzékeny folyamatokat kezelő rendszer, információt képező adat vagy egyéb, jogszabállyal (orvosi, ügyvédi, biztosítási, banktitok stb.) védett adat sérülhet,
d) a káresemény lehetséges társadalmi-politikai hatásai a szervezettel szemben bizalomvesztést eredményezhetnek, a jogszabályok betartása vagy végrehajtása elmaradhat, vagy a szervezet vezetésében személyi felelősségre vonást kell alkalmazni, vagy
e) a közvetlen és közvetett anyagi kár meghaladja a szervezet éves költségvetésének vagy nettó árbevételének 1%-át, de nem haladja meg annak 10%-át.

(3) A „magas” biztonsági osztály esetében nagy káresemény következhet be, mivel:

a) különleges személyes adat nagy mennyiségben sérülhet,
b) emberi életek kerülnek közvetlen veszélybe, személyi sérülések nagy számban következhetnek be,
c) nemzeti adatvagyon helyreállíthatatlanul megsérülhet,
d) az ország, a társadalom működőképességének fenntartását biztosító kritikus infrastruktúra rendelkezésre állása nem biztosított,
e) az SZTE üzleti vagy ügymenete szempontjából nagy értékű, üzleti titkot vagy különösen érzékeny folyamatokat kezelő rendszer vagy információt képező adat tömegesen vagy jelentősen sérülhet,
f) súlyos bizalomvesztés állhat elő az SZTE-vel szemben, alapvető emberi vagy a társadalom működése szempontjából kiemelt jogok is sérülhetnek, vagy
g) a közvetlen és közvetett anyagi kár meghaladja az SZTE éves költségvetésének vagy nettó árbevételének 10%-át.

29. § Az EIR-ek biztonsági osztályba sorolása

(1) Az SZTE minden EIR-jét biztonsági osztályba sorolja annak érdekében, hogy megfelelő biztonsági kontrollintézkedéseket rendelhessen az adott eszközhöz, figyelembe véve az SZTE működésére, erőforrásaira és külső kapcsolataira gyakorolt potenciális káros hatásokat.

(2) A biztonsági osztályba sorolás a hatályos jogszabályok, szabványok és belső szabályzatok alapján történik.

(3) A biztonsági osztályba sorolás az információbiztonsági kockázatok értékelésével kezdődik, amely során három alapelv mentén történik a minősítés:

a) Bizalmasság: az információ jogosulatlan hozzáférés elleni védelme.
b) Sértetlenség: az információ pontosságának és teljességének megőrzése.
c) Rendelkezésre állás: az információ és az informatikai rendszerek elérhetősége.

(4) A besorolási szintek legalább az alábbiak szerint strukturálódnak:

a) Alap: csak csekély működési vagy pénzügyi hatással járó kockázat.
b) Jelentős: jelentős kihatás az üzletmenetre, adatvédelemre vagy szabályozói megfelelésre.
c) Magas: súlyos, akár nemzetbiztonsági szintű kockázatok, amelyek rendszerszintű zavart vagy működésképtelenséget okozhatnak.

30. § A rendszerbiztonsági tervben (RBT) dokumentált biztonsági osztály

(1) A biztonsági osztályba sorolás eredményét az RBT tartalmazza, amelyben a következőket kötelező dokumentálni:

a) a kiválasztott biztonsági osztály és a hozzárendelt besorolási szint (alacsony, közepes, magas),
b) a biztonsági követelmények indoklása mindhárom alapelv szerint (bizalmasság, sértetlenség, rendelkezésre állás),
c) a kockázatértékelés módszertana,
d) a felelős személyek aláírása és dátuma.

(2) A biztonsági osztályozás dokumentálása és rendszeres felülvizsgálata kötelező. Az osztályozás alapján meghatározott védelmi intézkedéseket az ISZI, és az EIRBF közösen hajtja végre, és azok betartását folyamatosan ellenőrzi.

VIII. INCIDENSKEZELÉS

31. § A SZTE információbiztonsági incidenskezelési folyamatának célja, hogy gyorsan, hatékonyan és dokumentált módon reagáljon minden olyan eseményre, amely veszélyezteti az SZTE informatikai rendszereinek, adatvagyonának vagy szolgáltatásainak biztonságát. Az incidenskezelés során kiemelt szempont a szolgáltatások folytonosságának fenntartása, az adatvesztés megelőzése, valamint a jogszabályi megfelelés biztosítása.

32. § Információbiztonsági incidensnek minősül minden olyan esemény, amely során:

a) jogosulatlan hozzáférés történik informatikai rendszerhez vagy adathoz,
b) adatvesztés, adatvédelmi szabálysértés vagy meg nem engedett adatmanipuláció következik be,
c) túlterheléses támadás (DoS), zsarolóvírus vagy egyéb kártékony kód jelenik meg,
d) biztonsági szabályzat megsértése történik, akár szándékosan, akár gondatlanságból.

33. § Az incidenseket minden érintett – foglalkoztatott, hallgató, külső partner – köteles haladéktalanul, de legkésőbb 24 órán belül jelenteni az EIRBF-nek. A bejelentés történhet elektronikus úton, telefonon, személyesen.

34. § Az incidenskezelési folyamat lépései:

a) **Bejelentés és regisztráció**: Az incidens rögzítése az információbiztonsági nyilvántartásban.
b) **Elsődleges értékelés**: Az ISZI biztonsági csoportja megvizsgálja az esemény súlyosságát, hatókörét és sürgősségét.
c) **Vizsgálat és elemzés**: Az incidens technikai és szervezeti hátterének feltárása, az érintett rendszerek és adatok azonosítása.
d) **Intézkedések**: Azonnali védelmi lépések megtétele (pl. hozzáférés felfüggesztése, rendszerleválasztás, adatmentés).
e) **Kommunikáció**: Az érintettek tájékoztatása, szükség esetén hatóságok (pl. Nemzeti Kibervédelmi Intézet (NKI), Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) értesítése.
f) **Helyreállítás**: A normál működés visszaállítása, az adatok és szolgáltatások biztonságos újraindítása.
g) **Dokumentálás és utóértékelés**: Az incidens részletes dokumentálása, tanulságok levonása, javaslatok a jövőbeni megelőzésre.

35. § Feladatok szerepkörök szerinti bontásban:

(1) A Kancellár (felső vezetés) feladatai:

a) A biztonsági eseménykezelési folyamatok jóváhagyása és stratégiai szintű támogatása.
b) Döntéshozatal a jelentős biztonsági események, krízishelyzetek és azok következményeinek kezeléséről.
c) Az SZTE külső érintettek (hatóságok, tulajdonos, média) felé történő képviseletének biztosítása.
d) Jogosult stratégiai iránymutatás és kríziskommunikációs utasítások kiadására.

(2) Az EIRBF feladatai:

a) A biztonsági eseménykezelési eljárások kidolgozása, dokumentálása és megismertetése.
b) A biztonsági eseménykezelési folyamatok koordinációja, a biztonsági események értékelésének, minősítésének és lezárásának felügyelete.
c) A biztonsági események kezelésére irányuló oktatások, tesztek és gyakorlatok szakmai támogatása.
d) Jogosult biztonsági eseménykezelési eljárások elindítására, módosítására és szabályzatmódosítás kezdeményezésére.
e) Jogosult a vezetés rendszeres tájékoztatására a biztonsági eseményekről, trendekről, kockázatokról.

(3) Az ISZI feladatai:

a) Az EIR-eket érintő biztonsági események technikai kezelésének operatív irányítása az elfogadott eljárásrendek szerint.
b) Technikai elemzések, naplófájlok értékelésének, hálózati/szegmentációs lépéseknek és helyreállítási tevékenységeknek a koordinálása.
c) A technikai dokumentáció (naplózás, vizsgálati jegyzőkönyvek, helyreállítási lépések) vezetésének felügyelete.

d) Jogosult az eseménykezelési terv technikai részének aktiválására, az IT-feladatok kiosztására és nyomon követésére.
e) Jogosult hozzáférni az érintett rendszerekhez vizsgálat és helyreállítás céljából, vizsgálatokat kezdeményezni, javaslatot tenni elhárítási lépésekre.

(4) A JII és a DPO feladatai:

a) A biztonsági események jogi és adatvédelmi szempontú értékelése.
b) Hatósági bejelentési kötelezettségek (pl. Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH), ágazati hatóság) fennállásának vizsgálata, a bejelentések előkészítésének koordinálása, kivéve azon hatóságokat, amelyekkel a kapcsolatot az EIRBF tartja.
c) Jogosult javaslatot tenni a bejelentési kötelezettség teljesítésére, és kapcsolatot tartani a hatóságokkal a vezetés felhatalmazása alapján.
d) Az incidenskezelés során különös figyelmet kell fordítani a személyes adatokkal kapcsolatos eseményekre, amelyek esetén a GDPR előírásai szerint 72 órán belül adatvédelmi incidensként jelentést kell tenni a NAIH felé, amennyiben az incidens valószínűsíthetően kockázatot jelent az érintettek jogaira és szabadságaira.

(5) A Műszaki Igazgatóság feladata a fizikai és környezeti védelem biztosítása.

36. § (1) Az SZTE szervezeti egységei kötelesek rendszeresen tesztelni és gyakorolni az incidenskezelési eljárásokat annak érdekében, hogy biztosítsák a felkészültséget és a gyors reagálást.

(2) Az incidenskezelési folyamatot az EIRBF évente felülvizsgálja és szükség esetén frissíti. az új fenyegetések, technológiai változások és jogszabályi előírások alapján.

IX. ÜZLETMENET-FOLYTONOSSÁG ÉS KIBERREZILIENCIA

37. § A Szegedi Tudományegyetem elkötelezett amellett, hogy működését – különösen az oktatási, kutatási és egészségügyi szolgáltatásokat– információbiztonsági incidensek, technológiai hibák vagy külső támadások esetén is zavartalanul, vagy minimális megszakítással fenntartsa. Ennek érdekében az SZTE az alábbi üzletmenet-folytonossági és kiberreziliencia stratégiát alkalmazza, amely biztosítja a kritikus rendszerek gyors helyreállítását, az adatvesztés minimalizálását és a szolgáltatások újraindítását.

38. § Az üzletmenet-folytonosság keretében:

a) azonosítja a kritikus informatikai rendszereket, adatokat és szolgáltatásokat,
b) meghatározza az elfogadható kiesési időt (Maximum Allowable Downtime – MAD) és az adatvesztési toleranciát (Recovery Point Objective – RPO),
c) kidolgozza a helyreállítási eljárásokat (Disaster Recovery Plan – DRP),
d) rendszeresen teszteli és frissíti a folytonossági terveket.

39. § A kiberreziliencia (Cyber Resilience) az SZTE azon képességét jelenti, hogy proaktívan felkészüljön, reagáljon és alkalmazkodjon a kibertérből érkező fenyegetésekhez, valamint képes legyen a normál működés gyors visszaállítására. Ennek érdekében:

a) folyamatosan monitorozza az informatikai rendszereket és hálózatokat,

b) alkalmazza a megelőző védelmi intézkedéseket (pl. behatolásmegelőző rendszerek, biztonsági mentések, redundáns infrastruktúra),
c) biztosítja az egyetemi polgárok és érintettek felkészítését és a vészhelyzeti eljárások ismeretét,
d) együttműködik nemzeti és nemzetközi kiberbiztonsági szervezetekkel (pl. NKI).

40. § Az üzletmenet-folytonossági és kiberreziliencia terveket az alkalmazásgazdák dolgozzák ki az EIRBF és az ISZI támogatásával. A terveknek tartalmazniuk kell:

a) a kritikus rendszerek és szolgáltatások listáját,
b) a helyreállítási prioritásokat és felelősöket,
c) a kommunikációs protokollokat vészhelyzet esetén (rendszer és kommunikációvédelem),
d) az alternatív működési lehetőségeket (pl. távoli hozzáférés, felhőalapú szolgáltatások).

41. § Az üzletmenet-folytonossági és kiberreziliencia tervek végrehajtásáért az EIRBF és az Alkalmazásgazda közösen felelősek. Az elkészült terveket évente felül kell vizsgálni tesztelésükkel egybekötve, és minden jelentős technológiai vagy szervezeti változás esetén frissíteni kell. A tervek tesztelési eredményeit dokumentálni kell, és a tapasztalatokat be kell építeni a jövőbeli fejlesztésekbe.

X. INFORMÁCIÓBIZTONSÁGI TUDATOSSÁG ÉS KÉPZÉS

42. § A Szegedi Tudományegyetem információbiztonsági kultúrájának alapja a szervezeti szintű tudatosság és a rendszeres képzés.

43. § Az SZTE az alábbi képzési és tudatosságnövelő intézkedéseket alkalmazza:

a) Külön utasításban meghatározott keretek között minden foglalkoztatott köteles évente legalább egyszer információbiztonsági képzésen részt venni. A képzés kiterjed a jogszabályi előírásokra, a belső szabályozókra, a gyakori fenyegetésekre (pl. adathalászat, zsarolóvírusok), valamint a helyes reagálási és bejelentési protokollokra.
b) A hallgatók számára az információbiztonsági tudatosságot növelő képzést biztosít, elérhetővé teszi az alapvető biztonsági irányelveket és útmutatókat az egyetemi platformokon.
c) A vezetői szinteken célzott, szerepkör-specifikus képzéseket tart, különös tekintettel a döntéshozatali felelősségre, a kockázatkezelésre és az incidenskezelésre.
d) A külső partnerek és beszállítók számára – amennyiben hozzáférnek az SZTE informatikai rendszereihez vagy adatvagyonához – biztonsági tájékoztatást biztosít.

44. § A képzések formája lehet személyes oktatás, e-learning, interaktív teszt vagy esettanulmány-alapú szimuláció.

45. § (1) A képzések eredményességét az EIRBF rendszeresen értékeli és az eredmények alapján szükség esetén módosító javaslatot tesz a tematikára.

(2) A képzési részvétel dokumentálása, a nyilvántartás vezetése, valamint a hiányzók pótlólagos oktatásának megszervezése kötelező, amelyről a Humánpolitikai Igazgatóság gondoskodik.

46. § Az információbiztonsági tudatosság növelése érdekében az SZTE elérhetővé teszi és kommunikálja a jó gyakorlatokat, az aktuális fenyegetéseket és figyelmeztetéseket belső hírlevelek, illetve portálüzenetek formájában. A cél egy olyan biztonságtudatos szervezeti kultúra kialakítása, amelyben minden érintett aktívan hozzájárul az információbiztonság fenntartásához.

XI. HOZZÁFÉRÉS-KEZELÉS

47. § A Szegedi Tudományegyetem információbiztonsági stratégiájának egyik alappillére a hozzáférés-kezelés, amely biztosítja, hogy az informatikai rendszerekhez, adatokhoz és szolgáltatásokhoz kizárólag jogosult, hitelesített felhasználók férjenek hozzá. A hozzáférés-kezelés célja az adatok bizalmasságának, sértetlenségének és rendelkezésre állásának megőrzése, valamint a jogosulatlan hozzáférések megelőzése.

48. § Az SZTE hozzáférés-kezelési rendszere az alábbi alapelveken nyugszik:

a) **Legkisebb jogosultság elve**: Minden felhasználó csak olyan mértékű hozzáférést kap, amely feltétlenül szükséges a feladatai ellátásához.
b) **Szerepkör-alapú hozzáférés**: A jogosultságok előre definiált szerepkörökhöz kerülnek hozzárendelésre, amelyek tükrözik az egyetemi munkakörök és funkciók sajátosságait.
c) **Azonosítás és hitelesítés**: Minden hozzáférés egyértelműen azonosított felhasználóhoz kötött, erős jelszavak, meghatározott rendszerek tekintetében kétfaktoros hitelesítés (MFA) és – ahol indokolt – biometrikus azonosítás alkalmazásával.
d) **Hozzáférési naplózás**: Minden meghatározott hozzáférési esemény naplózásra kerül, és a naplókat rendszeresen ellenőrizik a gyanús vagy rendellenes tevékenységek kiszűrése érdekében.

49. § A hozzáférési jogosultságokat az EIRBF, az ISZI és az adatgazda közösen kezeli. A jogosultságok kiadását, módosítását és visszavonását az adatgazda kezdeményezi az ISZI által üzemeltetett szakrendszeren keresztül. Az ISZI nyomon követhető módon hajtja végre az igénylés, jóváhagyás, aktiválás és deaktiválás lépéseit. A jogosultságokat legalább évente felül kell vizsgálni, különös tekintettel az inaktív, áthelyezett vagy kilépett felhasználókra.

50. § Külön szabályozás vonatkozik a következő hozzáférési típusokra:

a) **Vendég-hozzáférés**: Külső partnerek, vendégkutatók vagy ideiglenes felhasználók számára csak időkorlátos, célhoz kötött hozzáférés engedélyezhető, amelyet naplózni és rendszeresen felülvizsgálni kell.
b) **Távoli hozzáférés**: VPN-en vagy más biztonságos csatornán keresztül történő hozzáférés csak előzetes engedélyezéssel, titkosított kapcsolat mellett történhet.
c) **Adminisztratív hozzáférés**: Rendszergazdai jogosultságokat csak szigorúan ellenőrzött körben, külön naplózással és rendszeres auditálással lehet biztosítani.
d) **Azonosítás vagy hitelesítés nélkül engedélyezett hozzáférés:** Azonosítani szükséges azon felhasználói tevékenységeket, amelyek - a szervezeti célokkal és üzleti funkciókkal összhangban - az EIR-ben azonosítás vagy hitelesítés nélkül is végrehajthatók. A rendszerbiztonsági tervben dokumentálni és indokolni szükséges

azokat a felhasználói tevékenységeket, amelyek azonosítás vagy hitelesítés nélkül is végrehajthatók.

51. § A hozzáférés-kezelés során különös figyelmet kell fordítani a személyes adatokhoz való hozzáférésre, amelyet a GDPR előírásai szerint kell szabályozni. Az adatkezelési célhoz nem kapcsolódó hozzáférés tilos, és adatvédelmi incidensnek minősülhet.

52. § Az adatgazda rendszeresen teszteli a hozzáférés-kezelési mechanizmusokat, és a tapasztalatok alapján az EIRBF és az ISZI támogatásával fejleszti az eljárásokat. A hozzáférés-kezelés hatékonysága külső és belső ellenőrzések keretében kerül vizsgálatra, különös tekintettel a kritikus rendszerekre és érzékeny adatokra.

XII. KÜLSŐ PARTNEREKRE ÉS BESZÁLLÍTÓKRA VONATKOZÓ RENDELKEZÉSEK

53. § A Szegedi Tudományegyetem információbiztonsági védelmének kiterjesztése érdekében kiemelt figyelmet fordít a külső partnerekkel és beszállítókkal való együttműködés biztonsági feltételeire.

54. § Az SZTE az alábbi elveket és intézkedéseket alkalmazza a külső partnerek és beszállítók információbiztonsági kezelésére:

a) Valamennyi információs és kommunikációs technológia (IKT) tárgyú, külső partnerrel kötött szerződésnek tartalmaznia kell az információbiztonsági követelményeket, különös tekintettel az adatkezelésre, hozzáférésre, incidenskezelésre és auditálhatóságra.
b) A partnerek csak olyan mértékű hozzáférést kapnak, amely feltétlenül szükséges a szerződéses feladatok ellátásához (legkisebb jogosultság elve).
c) A hozzáférés időben korlátozott, célhoz kötött, és technikailag naplózott módon történik. A hozzáférési eseményeket az ISZI rendszeresen ellenőrzi.
d) Az SZTE külső partnerek számára igény szerint tájékoztatást biztosít, amely ismerteti az SZTE információbiztonsági szabályait, elvárásait és a lehetséges következményeket szabályszegés esetén.
e) Az SZTE fenntartja a jogot arra, hogy a külső partnerek információbiztonsági gyakorlatát auditálja, különösen akkor, ha az együttműködés érzékeny vagy kritikus adatokat érint.
f) A beszállítók által biztosított szoftverek, hardverek vagy szolgáltatások biztonsági megfelelőségét az ISZI előzetesen értékeli, és csak jóváhagyás után kerülhetnek bevezetésre.
g) A külső partnerek által okozott vagy érintett információbiztonsági incidenseket az SZTE saját incidenskezelési eljárásrendje szerint kezeli, és szükség esetén jogi lépéseket tesz.

55. § Az EIRBF rendszeresen kezdeményezi az SZTE külső partnerekkel kapcsolatos információbiztonsági gyakorlatának felülvizsgálatát és szükség esetén javaslatot tesz a szerződéses feltételek, eljárásrendek vagy technikai megoldások módosítására a jogszabályi és technológiai környezet változásainak megfelelően.

XIII. KARBANTARTÁS, FIZIKAI ÉS KÖRNYEZETI VÉDELEM

56. § Minden EIR üzemeltetője köteles a hardver komponensek karbantartási igényét felmérni és ezeket úgy ütemezni, hogy a rendszer tervezett élettartama ne rövidüljön és ne sérüljön az üzletmenet-folytonossága a karbantartási hiányosságok miatt.

57. § Fizikai és környezeti védelem magában foglalja a hardverek megóvását a fizikai behatásoktól, a környezeti veszélyektől és az illetéktelen hozzáféréstől. A fizikai védelemnek összhangban kell lennie a biztonsági osztályba sorolással.

XIV. FELÜLVIZSGÁLAT ÉS AUDIT - VEZETŐSÉGI ÁTVIZSGÁLÁS

58. § A Szegedi Tudományegyetem az információbiztonsági rendszerének hatékonysága és jogszabályi megfelelősége érdekében rendszeres felülvizsgálatot és auditálást végez. A cél, hogy a jelen szabályzat, a kapcsolódó eljárásrendek és technikai intézkedések folyamatosan igazodjanak a változó kockázati környezethez, a technológiai fejlődéshez, valamint a hazai és nemzetközi szabályozási elvárásokhoz.

59. § A szabályzat és az információbiztonsági dokumentációk felülvizsgálatát az EIRBF évente legalább egyszer kötelezően elvégzi, illetve minden jelentős szervezeti, technológiai vagy jogszabályi változás esetén soron kívül el kell végezni. A felülvizsgálat során az EIRBF és az ISZI közösen értékelik:

a) a jelen szabályzat aktualitását és gyakorlati alkalmazhatóságát,
b) a kockázatelemzési eredmények alapján szükséges módosításokat,
c) az incidenskezelési tapasztalatokból levont tanulságokat,
d) a felhasználói visszajelzéseket és auditmegállapításokat.

60. §. Az EIRBF két évente belső auditokat végez. Az audit célja, hogy objektív képet adjon a szabályzat betartásáról, a kontrollmechanizmusok hatékonyságáról, valamint az esetleges hiányosságokról és fejlesztési lehetőségekről.

61. § A belső auditok mellett az SZTE külső auditokra is felkészül, különösen akkor, ha tanúsítási eljárás, hatósági ellenőrzés vagy partneri megfelelőségi vizsgálat történik. A külső auditokat független, akkreditált szervezetek végzik, és az auditjelentések alapján az SZTE intézkedési tervet készít a feltárt hiányosságok megszüntetésére.

62. § Az auditfolyamat során kiemelt figyelmet kapnak:

a) a hozzáférés-kezelés és naplózás megfelelősége,
b) az adatkezelési és adatvédelmi gyakorlatok,
c) az incidenskezelési eljárások dokumentáltsága és reakcióideje,
d) az üzletmenet-folytonossági és kiberreziliencia tervek aktualitása,
e) a külső partnerekkel kapcsolatos biztonsági intézkedések.

63. § Az auditok eredményeiről az EIRBF összefoglaló jelentést készít, amely tartalmazza a megállapításokat, a javasolt intézkedéseket és a végrehajtásért felelős személyeket. Az auditjelentések és felülvizsgálati dokumentumok megőrzése, nyomon követése és hozzáférhetősége az EIRBF feladata.

XV. ZÁRÓ RENDELKEZÉSEK

64. § Jelen szabályzat az SZTE információbiztonsági működésének alapelveit, kereteit és stratégiai irányait határozza meg. Az általános elvek gyakorlati alkalmazása, valamint az egyes biztonsági területek részletes szabályozása érdekében külön eljárásrendek kerülnek kiadásra, amelyek kötelező érvényűek az érintett szervezeti egységek és szereplők számára.

65. § Az eljárásrendek célja, hogy a jelen szabályzatban rögzített elvek mentén pontosan meghatározzák:

a) az egyes folyamatokat (pl. incidenskezelés, hozzáférés-igénylés, adatmentés),
b) a technikai kontrollokat és konfigurációs követelményeket (pl. jelszó, házirend, titkosítási szabványok, naplózási paraméterek),
c) a szerepkör-specifikus feladatokat és felelősségi köröket (pl. rendszergazdák, adatgazdák, felhasználók),
d) a működési és dokumentációs kötelezettségeket (pl. nyilvántartások, bejelentési protokollok, auditálási elvárások).

66. § Ez lehetővé teszi, hogy az SZTE információbiztonsági rendszere rugalmasan alkalmazkodjon a technológiai fejlődéshez, a jogszabályi változásokhoz és az intézményi sajátosságokhoz, miközben biztosítja az egységes, átlátható és ellenőrizhető működést.

67. § Jelen szabályzatot a Szenátus 2026. év március hó 30. napján hozott SZ-108-VII/2025/2026. (III.30.) számú határozatával elfogadta.

68. § Jelen szabályzat 2026. év április hó 1. napján lép hatályba. A Szabályzat a következő linken érhető el folyamatosan: http://www.u-szeged.hu/szabalyzatok.

69. § Jelen szabályzat hatályba lépésével egyidejűleg hatályát veszti a Szenátus 2021. május 31. napján SZ-205-XIII/2020/2021. (V.31.) számú határozatával elfogadott Szegedi Tudományegyetem Informatikai Biztonsági szabályzata.

Kelt: Szegeden, 2026. március hó 30. napján

Prof. Dr. Rovó László s. k.
rektor

Dr. Fendler Judit s. k.
kancellár