TOKAJ-HEGYALJA EGYETEM

INFORMÁCIÓBIZTONSÁGI SZABÁLYZAT

A szabályzatot a Tokaj-Hegyalja Egyetem Szenátusa
a 26/2025-2026 (10.10.) sz. határozatával fogadta el.

Hatálybalépés napja: 2026. január 1.

Tartalomjegyzék

A Tokaj-Hegyalja Egyetem (a továbbiakban: Egyetem) Szenátusa a nemzeti felsőoktatásról szóló 2011. évi CCIV. törvény (a továbbiakban: Nftv.), az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.), az Európai Parlament és a Tanács (EU) 2016/679 rendelete (általános adatvédelmi rendelet, a továbbiakban: GDPR), valamint Magyarország kiberbiztonságára vonatkozó mindenkor hatályos jogszabályok – így különösen a Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény, a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről szóló 7/2024. (VI. 24.) MK rendelet– rendelkezéseire figyelemmel, továbbá az Egyetem működésének biztonságos, jogszerű és átlátható információkezelése, valamint elektronikus információs rendszereinek védelme érdekében az alábbi Információbiztonsági Szabályzatot (a továbbiakban: IBSZ vagy Szabályzat) alkotja és adja ki.

1. Bevezetés, általános rendelkezések

1.1. A szabályzat célja

Az Információbiztonsági Szabályzat (a továbbiakban: IBSZ, vagy Szabályzat) célja, hogy egységes, magas szintű szabályozási keretet biztosítson a Tokaj-Hegyalja Egyetem (a továbbiakban: Egyetem) számára az információk, valamint az elektronikus információs rendszerek (a továbbiakban: EIR-ek) bizalmasságának, sértetlenségének és rendelkezésre állásának védelmére.

A Szabályzat meghatározza azokat az alapelveket, követelményeket és felelősségi köröket, amelyek biztosítják:

- az Egyetem által használt EIR-ek és az azokban kezelt adatok biztonságos működését,
- az EIR-ek által nyújtott vagy azokon keresztül elérhető szolgáltatások védelmét,
- valamint a mindenkor hatályos jogszabályi előírásoknak való megfelelést.

A Szabályzat célja továbbá, hogy:

- világos iránymutatást adjon az Egyetem munkavállalói, hallgatói és külső partnerei számára az információk és EIR-ek biztonságos használatáról,
- elősegítse az információbiztonsági tudatosságot és a felelős adatkezelést,
- meghatározza az informatikai biztonsággal kapcsolatos felelősségi köröket és elvárásokat,
- valamint megalapozza az Egyetem információbiztonsági rendszerének működését és folyamatos fejlesztését.

1.2. A szabályzat hatálya

<u>Személyi hatály</u>

Jelen szabályzat személyi hatálya kiterjed az Egyetem összes munkavállalójára, oktatóira, hallgatóira, megbízottjára, valamint minden olyan személyre, aki az Egyetem informatikai rendszereit és hálózatait, EIR-jeit használja. Ide tartoznak továbbá azok a külső partnerek és szolgáltatók is, akik az Egyetem informatikai rendszereihez hozzáféréssel rendelkeznek, vagy informatikai szolgáltatásokat nyújtanak az Egyetem számára.

Tárgyi hatály

Jelen szabályzat tárgyi hatálya kiterjed az Egyetem valamennyi informatikai eszközére, rendszerére, hálózatára és adatára, EIR-jére függetlenül azok fizikai elhelyezkedésétől vagy tulajdonjogától. A szabályzat hatálya kiterjed az Egyetem által üzemeltetett vagy bérelt, valamint a felhasználók saját tulajdonában lévő, de az Egyetem hálózatához vagy rendszereihez csatlakoztatott eszközökre is.

A jelen szabályzattal összefüggő adatvédelmi és adatbiztonsági szabályok tekintetében a Tokaj-Hegyalja Egyetem Belső adatkezelési és adatbiztonsági szabályzata irányadó.

1.3. Információbiztonsági politika (IBP)

A Tokaj-Hegyalja Egyetem elkötelezett az információbiztonság magas szintű biztosítása mellett, amelynek célja az adatok és informatikai rendszerek védelme, valamint az Egyetem működésének biztonságos és zavartalan fenntartása. Az információbiztonság alapelvei közé tartozik a bizalmasság, amely biztosítja, hogy az adatokhoz kizárólag az arra jogosult személyek férhessenek hozzá, a sértetlenség, amely garantálja az adatok megbízhatóságát és pontosságát, valamint a rendelkezésre állás, amely biztosítja, hogy az információk és informatikai rendszerek a megfelelő időben és a megfelelő személyek számára elérhetők legyenek. A védelem minden releváns fenyegetést figyelembe vesz, kiterjed a rendszer valamennyi elemére, folyamatosan fenntartható, és arányos a kockázatokkal, biztosítva, hogy a védelmi intézkedések költsége összhangban álljon a potenciális károkkal. Az Egyetem biztosítja az információbiztonsági célok eléréséhez és fenntartásához szükséges, kockázatokkal arányos humán, pénzügyi és technológiai erőforrásokat.

Az Egyetem információbiztonsági rendszere összhangban áll a vonatkozó jogszabályi és szabályozási követelményekkel, különös tekintettel az Európai Unió általános adatvédelmi rendeletére (GDPR), az információs önrendelkezési jogról és az információszabadságról szóló törvényre, valamint a kiberbiztonságra vonatkozó hatályos magyar jogszabályokra. A belső szabályzatok és eljárások célja a folyamatos megfelelés biztosítása és az ellenőrzések rendszeres végrehajtása.

Az Egyetem kizárólag jogtiszta szoftvereket használ, és ugyanezt az elvárást támasztja minden együttműködő partnerével szemben.

Minden munkavállalónak, hallgatónak és partnernek kötelessége betartani az informatikai biztonsági előírásokat, valamint az adatvédelemre vonatkozó speciális szabályokat az Egyetem szolgáltatásainak igénybevétele során. Az informatikai rendszerek használatakor minden érintettől elvárt a körültekintő és felelősségteljes magatartás, amely biztosítja a rendszerek biztonságos és megfelelő működését.

Az Egyetem folyamatosan fejleszti információbiztonsági rendszerét, alkalmazkodva a változó technológiai és fenyegetettségi környezethez, valamint a jogszabályi előírásokhoz. A Szabályzat és az ahhoz kapcsolódó eljárások rendszeres felülvizsgálaton esnek át.

1.4. A szabályzat kezelése és felülvizsgálata

A Szabályzat előkészítésének és szakmai tartalmának kialakítása az Információbiztonsági Felelős (a továbbiakban: IBF) feladata, aki e munkát az információbiztonsági szerepköröket betöltő személyekkel együttműködésben végzi.

A Szabályzat jóváhagyása és hivatalos kiadása az Egyetem Szenátusának hatásköre.

A Szabályzat szakmai előkészítéséről, a kihirdetéséről, valamint a szabályzat személyi hatálya alá tartozók tájékoztatásáért az Információbiztonság Szabályozásáért Felelős Vezető (a továbbiakban: ISZFV) köteles gondoskodni.

A Szabályzat hatálya alá tartozó személyek kötelesek a dokumentum tartalmát megismerni.

Az egyes munkavállalói vagy megbízási körökben – ahol ezt a munkakör vagy feladat ellátása indokolja – az Egyetem külön nyilatkozat megtételét is előírhatja.

A Szabályzat felülvizsgálatát és frissítését az alábbi esetekben kell elvégezni:

- **Jelentős változások esetén:** Amennyiben az Egyetem működésében, szervezeti felépítésében, alaptevékenységében, informatikai rendszereiben vagy a vonatkozó jogszabályi környezetben olyan lényeges változás történik, amely a szabályzat módosítását indokolttá teszi.
- Új kockázatok és technológiák megjelenésekor: Ha új biztonsági kockázatok, fenyegetettségek vagy technológiai fejlődés teszi szükségessé a reagálást.
- **Rendszeres időközönként:** Legalább kétévente egyszer, a szabályzat naprakészségének és relevanciájának biztosítása érdekében.

A szabályzat módosítására javaslatot tehet bármely, a 2. **Szervezeti keretek és felelősségi** körök pontban meghatározott információbiztonsági szerepkört betöltő személy. A módosítások előkészítéséért és végrehajtásáért az IBF felel, míg az új verzió jóváhagyása és hivatalos kiadása az Egyetem Szenátusának hatásköre.

1.5. A szabályzat során használt fogalmak

Informatikai eszközök: Számítógépek (asztali számítógép, laptop, mobil eszközök), szerverek, hálózati eszközök (routerek, switchek, tűzfalak), nyomtatók, szkennerek, adathordozók (USB kulcsok, külső merevlemezek), mobiltelefonok, tabletek és minden egyéb, az Egyetem tulajdonában lévő vagy általa használt informatikai eszköz.

Informatikai rendszerek: Az Egyetem által használt szoftverek, alkalmazások, adatbázisok, levelezőrendszerek, ügyviteli rendszerek, tanulmányi rendszerek, könyvtári rendszerek, weboldalak, portálok és minden egyéb informatikai rendszer.

EIR (Elektronikus Információs Rendszer): Az Egyetem feladatai ellátásához használt, informatikai eszközökből, hálózatokból, szoftverekből és adatokból álló, egységként kezelt rendszer, amelynek célja az információk előállítása, feldolgozása, továbbítása, tárolása és megjelenítése.

Alkalmazás: Jelen Szabályzat alkalmazásnak tekint minden olyan szoftvert, informatikai rendszert vagy szolgáltatást (ideértve különösen a helyben üzemeltetett és a felhőalapú/SaaS megoldásokat, webes rendszereket, portálokat, valamint külső szolgáltató által hosztolt alkalmazásokat), amelyet az Egyetem az információk előállítására, feldolgozására, tárolására vagy szolgáltatására használ.

Bizalmasság: Az információvédelem alapelve, amely biztosítja, hogy az információkhoz csak az arra jogosult személyek férhessenek hozzá.

Sértetlenség: Az információvédelem alapelve, amely biztosítja, hogy az adatok pontosak, teljesek és jogosulatlanul nem módosíthatók.

Rendelkezésre állás: Az információvédelem alapelve, amely biztosítja, hogy az adatok és rendszerek a jogosult felhasználók számára a szükséges időben elérhetők legyenek.

Hozzáférési jogosultság: Az a meghatározott jogosultsági szint, amely alapján a felhasználó adatokat érhet el vagy műveleteket végezhet az informatikai rendszerekben.

Felhasználó: Az Egyetem minden munkavállalója, hallgatója, külső partnere vagy megbízottja, aki az Egyetem elektronikus információs rendszereihez hozzáférést kap.

Szolgáltató / harmadik fél: Olyan külső szervezet vagy személy, aki az Egyetem megbízásából szolgáltatást nyújt, és ennek során hozzáférhet az Egyetem adataihoz vagy rendszereihez.

Kockázat: Az információbiztonsági sérülékenységek kihasználásával járó fenyegetések által okozott károk vagy veszteségek bekövetkezésének valószínűsége és mértéke.

Sérülékenység: Az információbiztonságban meglévő olyan gyengeség vagy hiba, amely egy fenyegetés kihasználásával informatikai biztonsági incidenshez vezethet.

Informatikai Biztonsági esemény: Nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat, amely az elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idézhet elő.

Informatikai Biztonsági incidens: Olyan biztonsági esemény, amelynek hatására az elektronikus információs rendszer által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül.

Informatikai vészhelyzet: Olyan állapot, amikor az informatikai szolgáltatások jelentős része nem elérhető, a helyreállítás rövid időn belül nem lehetséges, az üzletmenet folytonosság biztosítása sérül.

MFA/2FA (Multi-Factor Authentication / Two-Factor Authentication): Többlépcsős hitelesítési mechanizmus, amely legalább két, egymástól független azonosítási tényező (pl. jelszó, token, SMS-kód, mobilalkalmazás-értesítés, biometrikus azonosító) együttes alkalmazásával biztosítja a felhasználó hitelesítését.

Hálózatok: Az Egyetem teljes hálózati infrastruktúrája, beleértve a vezetékes és vezeték nélküli hálózatokat, az internetkapcsolatot, a belső hálózatot és a távoli hozzáférést biztosító rendszereket.

Távoli hozzáférés: Olyan hozzáférés, amely az Egyetem informatikai rendszereihez, hálózati eszközeihez vagy szolgáltatásaihoz az Egyetem belső hálózatán kívülről, az interneten keresztül történik. A távoli hozzáférés történhet felhasználói, adminisztratív, üzemeltetői vagy távsegítségnyújtási célból. A hozzáférés kizárólag biztonságos, titkosított csatornán történhet.

Vezeték nélküli hozzáférés: Az Egyetem hálózati erőforrásaihoz való hozzáférés Wi-Fi hálózaton keresztül. A vezeték nélküli hozzáférések biztonságát hitelesítési és titkosítási eljárásokkal, valamint hálózati szegmentációval kell biztosítani.

Mobil eszközök: Mobil eszköznek minősül minden olyan hordozható eszköz, amely képes az Egyetem EIR-jeihez való kapcsolódásra (pl. laptop, okostelefon, táblagép).

Adatok: Az Egyetem által kezelt valamennyi adat, függetlenül annak formátumától (szöveges, képi, hang-, videóanyag), tárolási helyétől (elektronikus vagy papír alapú) és bizalmassági szintjétől (bizalmas, nem bizalmas, stb.).

Üzletmenet-folytonosság: Az a képesség, amely biztosítja az Egyetem kritikus feladatainak és szolgáltatásainak folyamatos vagy gyorsan helyreállítható működését katasztrófa, hiba vagy incidens esetén.

Katasztrófaterv: Az Egyetem által jóváhagyott dokumentum, amely meghatározza a rendkívüli események, természeti vagy technikai katasztrófák esetén követendő eljárásokat és felelősségi köröket az informatikai rendszerek helyreállítására.

Logolás / naplózás: Az elektronikus információs rendszerek működésének, hozzáféréseinek és eseményeinek olyan rögzítése, amely lehetővé teszi az utólagos ellenőrzést és az incidensek kivizsgálását.

Mentés: Az adatok biztonsági másolatának készítése az adatvesztés megelőzése érdekében.

2. **Szervezeti keretek és felelősségi körök**

Az Egyetem hatékony információvédelmi és információbiztonsági irányítási rendszerének alapja a világosan meghatározott szervezeti keret, valamint az egyértelműen kijelölt biztonsági szerepkörök és felelősségi szintek, amelyek az alábbiak szerint kerültek kialakításra.

- Biztonsági szerepkör: Információbiztonság Szabályozásáért Felelős Vezető (ISZFV)
  - **A hozzárendelt felelősség:** Általános vezetői és az információbiztonság tervezéséhez, szervezéséhez, irányításához, kockázatokkal arányos megvalósításához, felügyeletéhez, folyamatos fenntartásához és továbbfejlesztéséhez szükséges erőforrások biztosításáért való felelősség.
  - **Szerepkör betöltője az Egyetemen:** Kancellár
- Biztonsági szerepkör: Kockázatkezelésért Felelős Vezető
  - **A hozzárendelt felelősség:** A kockázatok szervezeti szintű áttekintésének és elemzésének, valamint a kockázatmenedzsment szervezeten belüli egységes működésének biztosításáért való felelősség.
  - **Szerepkör betöltője az Egyetemen:** Kancellár
- Biztonsági szerepkör: Információbiztonsági Felelős (IBF)
  - A hozzárendelt f**elelősség:** Az információbiztonsági tevékenységek tervezéséért, felügyeletéért és ellenőrzéséért való felelősség.
  - **Szerepkör betöltője az Egyetemen:** Informatikai Szervezet vezetője
- Biztonsági szerepkör: Adatgazda
  - **A hozzárendelt felelősség:** A felelősségi körébe tartozó információk és adatok besorolásának meghatározása és felülvizsgálata; az adatokhoz való hozzáférési jogosultsági elvek, felhasználói szerepkörök és hozzáférési szintek meghatározása és jóváhagyása; valamint a területén kezelt információk Szabályzatnak megfelelő védelmének és kezelésének biztosítása.
  - **Szerepkör betöltője az Egyetemen:** Szervezeti egységek vezetői, projektvezetők, Alkalmazásnyilvántartásban kijelölt adatgazdák
- Biztonsági szerepkör: Alkalmazásgazda
  - **A hozzárendelt felelősség:** Az adott alkalmazás konfigurációjának, felhasználói szerepköreinek és jogosultságainak beállítása és karbantartása az Adatgazda által meghatározott és jóváhagyott jogosultsági elvek alapján; az alkalmazás rendeltetésszerű és biztonságos használatának támogatása.

- Sz**erepkör betöltője az Egyetemen:** Az Alkalmazásnyilvántartásban kijelölt felelős személy(ek).

- Biztonsági szerepkör: Üzemeltetésért felelős
  - **A hozzárendelt felelősség:** Az Egyetem központi informatikai infrastruktúrájának és alapvető szolgáltatásainak üzemeltetéséért való felelősség, ideértve különösen a szerverek, virtualizációs környezetek, adattárolók, hálózati eszközök, tűzfalak, címtárszolgáltatások, az Egyetem Microsoft 365 környezete, a felhasználói fiókok és csoportok infrastruktúra-szintű kezelése, valamint a VPN- és WiFi-hozzáférések üzemeltetése.
  - **Szerepkör betöltője az Egyetemen:** Informatikai vezető-helyettes
- Biztonsági szerepkör: Biztonsági vezető
  - **A hozzárendelt felelősség:** Fizikai biztonsággal kapcsolatos tevékenységek ellátásáért való felelősség.
  - **Szerepkör betöltője az Egyetemen:** Üzemeltetési vezető
- Biztonsági szerepkör: Humánerőforrás menedzsmentért felelős
  - **A hozzárendelt felelősség:** Foglalkoztatottak be- és kiléptetéséért, a személyi ügyekhez kapcsolódó tevékenységek koordinálásáért való felelősség. Információbiztonsági képzések lebonyolításáért és adminisztrációjáért való felelősség.
  - **Szerepkör betöltője az Egyetemen:** HR vezető
- Biztonsági szerepkör: Informatikai beszerzésekért felelős
  - **A hozzárendelt felelősség:** Informatikai erőforrások, eszközök és szolgáltatások beszerzésének lebonyolításáért való felelősség.
  - **Szerepkör betöltője az Egyetemen:** Informatikai Szervezet vezetője, és helyettese

Az Egyetem az általa használt elektronikus információs rendszereket és alkalmazásokat egységes Alkalmazásnyilvántartásban tartja nyilván. Az Alkalmazásnyilvántartás jelöli, hogy az adott alkalmazás önálló EIR-nek minősül-e vagy egy EIR részét képezi, továbbá tartalmazza az adott EIR/alkalmazás kijelölt Adatgazdáját, Alkalmazásgazdáját és Üzemeltetésért felelősét. Az Alkalmazásnyilvántartásban önálló EIR-ként megjelölt rendszerekhez Rendszerbiztonsági Terv (RBT), a nem EIR-nek minősülő, de az Alkalmazásnyilvántartásban megjelölt alkalmazásokhoz alkalmazásbiztonsági adatlap készítendő.

Az Alkalmazásnyilvántartás létrehozásáért, tartalmának meghatározásáért és naprakészen tartásáért az Információbiztonsági Felelős (IBF) felel, az érintett Adatgazdák és Alkalmazásgazdák közreműködésével.

Az Információbiztonság Szabályozásáért Felelős Vezető a felelősségét nem, de az egyes – különösen a döntés előkészítéssel összefüggő – feladatok végrehajtását delegálhatja a jelen Szabályzat keretében, fentiekben meghatározott biztonsági szerepköröket betöltő személyek felé.

Az Információbiztonsági Felelős köteles ellenőrizni az IBSZ szabályainak betartását és az előírt intézkedések végrehajtását. Ezt a feladatellátás, a szabályzat felülvizsgálata és a rendszeres biztonsági helyzetértékelés során végzi, és szükség esetén tájékoztatja az Információbiztonság Szabályozásáért Felelős Vezetőt.

2.1. Az információbiztonsági engedélyezési eljárás

Az Egyetem Információbiztonság Szabályozásáért Felelős Vezetője jogosult és köteles gondoskodni arról, hogy minden, információbiztonsággal kapcsolatos tevékenység és intézkedés kizárólag:

- megfelelő felhatalmazással rendelkező személy(ek) által,
- a döntéshez szükséges és indokolt információk birtokában,
- a biztonsági kockázatok és követelmények figyelembevételével,
- szabályozott keretek között

kerüljön jóváhagyásra és végrehajtásra.

2.1.1. Engedélyezéshez kötött tevékenységek és jogkörök

Az információbiztonsággal kapcsolatos engedélyezéshez kötött tevékenységeket az alábbi kategóriákba soroljuk, a hozzájuk tartozó jóváhagyási jogkörökkel együtt:

- Nem Delegálható Engedélyezési Jogkörök (Információbiztonság Szabályozásáért Felelős Vezető kizárólagos hatásköre)
  a) a biztonsági szerepköröket betöltő személyek kinevezése és megbízása, valamint indokolt esetben kinevezésük vagy megbízásuk visszavonása,
  b) új távoli vagy vezeték nélküli hozzáférési megoldás bevezetése, meglévő használatának felfüggesztése, kivezetése vagy kiváltása,
  c) az Egyetem rendelkezésében lévő EIR használatának megszüntetése, kivezetése vagy kiváltása,
  d) új EIR beszerzése és fejlesztése,
  e) új, az Egyetem rendszereibe integrált, vagy magas kockázatú adatokat kezelő felhasználói szoftver beszerzése,
  f) az informatikai fejlesztés elfogadása, átvétele, bevezetésének elrendelése,
  g) üzletmenet-folytonossági intézkedések végrehajtásának elrendelése (ideértve a helyettesítő eljárásokat és helyreállító tevékenységeket), valamint kieséssel járó hibajavítás jóváhagyása,
  h) információbiztonsági képzési programok lebonyolításának jóváhagyása,
  i) szervezeti információk nyilvánosságra hozatala, közzététele,
  j) kockázatkezelési intézkedések végrehajtása,
  k) cselekvési, biztonsági, és intézkedési tervek jóváhagyása,

- Az Információbiztonság Szabályozásáért Felelős Vezető által delegált jóváhagyások

  ISZFV jelen Szabályzatban meghatározott alábbi engedélyezési jogköröket általános jelleggel, folyamatos hatállyal delegálja:

  - az Adatgazda részére:
    l) az adott EIR-ben használt felhasználói szerepkörök és az ezekhez tartozó adathozzáférési szintek, jogosultsági elvek meghatározásának és az egyedi jogosultsági igények TARTALMI jóváhagyása (annak eldöntése, hogy ki, milyen adatokhoz, milyen célból és milyen szerepkörben férhet hozzá);
  - az Alkalmazásgazdák részére:

m) az adott alkalmazás felhasználói fiókjainak és hozzáférési jogosultságainak beállítása az Adatgazda által meghatározott szerepkörök és jóváhagyott jogosultsági igények alapján.
n) az adott EIR biztonsági és működési paramétereinek kezelésére vonatkozó engedélyek kiadása (például jelszóházirend, naplózás, mentési és archiválási szabályok, rendszerbeállítások),
o) egyedi azonosítás és hitelesítés alóli kivétel igénye,

- az Üzemeltetésért Felelős személy(ek) részére:
  p) csoportszintű hozzáférés beállítására vonatkozó igény,
  q) Egyetemi adatot tartalmazó rendszerelem kiszállítása,

- Az Üzemeltetésért felelős személy hajtja végre, az Információbiztonság Szabályozásáért Felelős Vezető általános felhatalmazása alapján:
  r) az Egyetem központi informatikai infrastruktúrájához kapcsolódó felhasználói fiókok kezelése az Adatgazda által meghatározott és jóváhagyott jogosultsági elvek alapján.
  s) azonosítók és hitelesítő eszközök kiosztása,
  t) rendszeres biztonsági mentések ütemezése és ellenőrzése,
  u) felhasználói szoftvertelepítés (a szükséges biztonsági ellenőrzés végrehajtását követően).

2.1.2. Az Engedélyezési Eljárás Menete **és a Szereplők Felelőssége**

Az engedélyezési eljárás célja, hogy minden, az Egyetem információbiztonságát érintő változtatás, fejlesztés vagy tevékenység (különösen a felhasználói fiókok és jogosultságok kiadása, módosítása vagy visszavonása, valamint az EIR-t, alkalmazást, hálózati vagy infrastruktúra-elemet érintő módosítás) ellenőrzött, dokumentált és felelős döntés alapján valósuljon meg.

Igény benyújtása

- Igényt bármely felhasználó, Adatgazda, Alkalmazásgazda vagy az Üzemeltetésért felelős kezdeményezhet. Az igényt minden esetben írásban kell rögzíteni.
- Az igénynek legalább az alábbiakat kell tartalmaznia:
  - az igény pontos leírása,
  - az érintett rendszer(ek), alkalmazás(ok), szolgáltatás(ok) megjelölése,
  - az igény indoklása és várható előnyei,
  - a tervezett időzítés és esetleges leállási hatás.

Tartalmi Jóváhagyás

- Amennyiben az igény adatokhoz való hozzáférést, felhasználói szerepkört vagy jogosultsági szintet érint, az érintett adatkör Adatgazdája tartalmilag hagyja jóvá az igényt, a felhasználó feladatkörét és szerepét (pl. adminisztratív, oktatói, hallgatói, külső partner) és az ahhoz arányosan illeszkedő jogosultsági szintet figyelembe véve.
- Ha az igény elsődlegesen egy EIR vagy alkalmazás működését, funkcióit vagy beállításait érinti, az Alkalmazásgazda készít javaslatot, és szükség esetén egyeztet az érintett Adatgazdával.

- Ha az igény elsődlegesen az informatikai infrastruktúrát (pl. szerver, hálózat, VPN, WiFi, címtár, Microsoft 365) érinti, az Üzemeltetésért felelős készít javaslatot, és jogosultságot érintő hatás esetén az érintett Adatgazdát is be kell vonni.
- Azokban az esetekben, amikor a 2.1.1. pont szerint nem delegálható engedélyezési jogkör érintett, az Információbiztonság Szabályozásáért Felelős Vezető (ISZFV) jóváhagyása kötelező.

Információbiztonsági szempontú értékelés

- Jelentősebb biztonsági kockázattal járó igények (pl. új EIR vagy alkalmazás bevezetése, külső szolgáltató igénybevétele, érzékeny adatkört érintő lényeges változtatás) esetén az Információbiztonsági Felelős (IBF) információbiztonsági szempontból véleményezi a kérelmet.
- Az ISZFV jogosult előírni, hogy egy adott igényt az IBF kötelezően értékeljen (különösen, ha az igény kockázatnövekedéssel járhat).
- Az IBF véleményezése során:
  - azonosítja a főbb információbiztonsági kockázatokat,
  - javaslatot tesz szükség esetén kiegészítő védelmi intézkedésekre.
- Az IBF véleményét írásban rögzíti, és rendelkezésre bocsátja az engedélyezésre jogosult személy számára

Engedélyezés

- Amennyiben a kérelem nem érinti a 2.1.1. pontban meghatározott, nem delegálható engedélyezési jogköröket, a tartalmi jóváhagyást végző személy (pl. Adatgazda, Alkalmazásgazda, Üzemeltetésért felelős) döntése egyben engedélynek minősül, külön engedélyezési lépésre nincs szükség.
- A 2.1.1. pontban meghatározott, nem delegálható engedélyezési jogköröket érintő ügyekben a tartalmi jóváhagyást követően az Információbiztonság Szabályozásáért Felelős Vezető (ISZFV) jogosult és köteles a végső engedély kiadásáról dönteni, a tartalmi javaslat és – ha készült – az IBF véleménye alapján.
- Az engedélyezés – a szervezet által alkalmazott gyakorlatnak megfelelően – történhet papír alapon (aláírt nyomtatvány) vagy elektronikusan.

Végrehajtás

- Az engedélyezett tevékenység végrehajtásáért:
  - alkalmazás- / EIR-szinten az Alkalmazásgazda,
  - infrastruktúra-szinten az Üzemeltetésért felelős,
  - illetve a döntésben kijelölt egyéb végrehajtó felel.
- Jogosultságok kiadása, módosítása vagy visszavonása esetén az Alkalmazásgazda az alkalmazás-/EIR-szintű, az Üzemeltetésért felelős pedig az infrastruktúra-szintű (pl. címtár, hálózati, M365) beállításokat hajtja végre az Adatgazda döntése alapján.

Dokumentálás és nyilvántartás

- Minden kérelem, értékelés és döntés kötelezően dokumentálandó és legalább 3 évig megőrzendő.
- A dokumentációban rögzíteni kell:
  - kérelem azonosítóját, benyújtóját, benyújtás dátumát,
  - a tartalmi jóváhagyást végző személy(ek) megnevezését (pl. Adatgazda),

    - az IBF értékelését és javaslatát (ha készült),
    - az engedélyező személy nevét, beosztását és döntésének dátumát,
    - a végrehajtás tényét, időpontját és a végrehajtásért felelős személy(ek) adatait.
- A dokumentumokat elektronikus nyilvántartásban (pl. központi iktatás, jegykezelő rendszer vagy megosztott központi tárhely) kell tárolni a visszakereshetőség és az auditálhatóság biztosítása érdekében.

3. Adminisztratív biztonsági intézkedések

3.1. Felhasználók jogai és kötelezettségei

Az Egyetem valamennyi munkavállalója, hallgatója és külső partnere, aki hozzáférést kap az Egyetem informatikai erőforrásaihoz, a jelen Szabályzat szempontjából felhasználónak minősül. Minden felhasználó köteles a rá vonatkozó előírásokat megismerni és maradéktalanul betartani.

A felhasználók jogai:

- Rendeltetésszerű használat: A felhasználók jogosultak az Egyetem által biztosított informatikai eszközök és szolgáltatások rendeltetésszerű használatára az oktatási, kutatási, tanulmányi és adminisztratív feladataik ellátása során.
- Hozzáférési jogosultság: Minden felhasználó jogosult a munkakörének vagy tanulmányi státuszának megfelelő, számára kijelölt erőforrásokhoz való hozzáférésre.
- Jelentési jog: A felhasználók jogosultak az informatikai rendszer biztonságával, működésével kapcsolatos problémákat észrevételezni és jelenteni.
- Támogatás: A felhasználók jogosultak segítséget kérni az informatikai rendszerek használatához, és az informatikai incidensek kezeléséhez.

A felhasználók kötelezettségei:

- Szabályzatok betartása: A felhasználók kötelesek az informatikai erőforrásokat kizárólag a jogszabályoknak, az Egyetem szabályzatainak és a rendeltetésszerű használatnak megfelelően igénybe venni.
- Bizalmasság és integritás: A felhasználók kötelesek betartani a hozzáférési és jogosultsági szabályokat. Tilos az illetéktelen információk megszerzése vagy rendszerek megkerülése, illetve a bizalmas adatok és személyes információk védelmére vonatkozó előírások megszegése.
- Azonosító eszközök védelme: A felhasználók kötelesek jelszavaikat és hitelesítő eszközeiket bizalmasan kezelni, és azokat harmadik személynek nem adhatják át.
- Eseménykezelés: A felhasználók kötelesek haladéktalanul bejelenteni, ha biztonsági eseményt, jogosulatlan hozzáférést vagy adatszivárgás gyanúját észlelik.
- Vagyonvédelem: A felhasználók kötelesek óvni az Egyetem tulajdonában álló eszközöket a rongálódástól, elvesztéstől vagy jogosulatlan használattól.

3.2. **Tiltott tevékenységek és visszaélések megelőzése**

Az Egyetem informatikai erőforrásainak használata során a felhasználók kötelesek tartózkodni minden olyan magatartástól, amely a rendszerek biztonságát, más felhasználók jogait vagy az Egyetem működését veszélyezteti.

Tiltott tevékenységnek minősül különösen:

- Jogosulatlan hozzáférés: Tilos bármely olyan információhoz, adathoz, rendszerhez vagy szolgáltatáshoz hozzáférni, amelyhez a felhasználó nem rendelkezik hivatalos jogosultsággal.
- Védelmi rendszerek megkerülése: Tilos a biztonsági mechanizmusok és védelmi rendszerek (pl. tűzfalak, vírusirtók, szűrőprogramok) kijátszása, megkerülése, kikapcsolása vagy módosítása.
- Jogosulatlan szoftverhasználat: Tilos engedély nélküli szoftverek telepítése, futtatása, vagy a szoftverhasználatra vonatkozó szerzői jogi előírások megsértése.
- Kártékony kódok terjesztése: Tilos olyan kódok (pl. vírusok, trójaiak) létrehozása, továbbítása vagy birtoklása, amelyek károsíthatják az EIR-eket.
- Támadások indítása: Tilos az Egyetem vagy harmadik fél hálózatát, rendszereit, informatikai szolgáltatásait célzó támadások végrehajtása.
- Személyes adatokkal való visszaélés: Tilos a személyes adatok jogellenes gyűjtése, feldolgozása, közzététele vagy más módon történő felhasználása.
- Erőforrás kihasználása: Tilos az Egyetem által biztosított erőforrások jogszabályba ütköző vagy az Egyetem tevékenységétől idegen célú felhasználása.
- Egyéb veszélyeztetés: Tilos bármely olyan cselekmény, amely az Egyetem jó hírnevét, adatvagyonát vagy informatikai rendszereinek sértetlenségét veszélyezteti.

Az Egyetem jogosult a tiltott tevékenységek megelőzése érdekében ellenőrzési, naplózási és vizsgálati intézkedéseket alkalmazni. A szabályok megsértése fegyelmi, munkajogi vagy jogi következményekkel járhat.

3.3. **Informatikai erőforrások és szolgáltatások használati szabályai**

Az Egyetem által biztosított informatikai erőforrások és szolgáltatások (például e-mail rendszer, internet-hozzáférés, hálózati tárhely, alkalmazások) elsődlegesen a munkaköri, oktatási, kutatási, tanulmányi és adminisztratív feladatok ellátását szolgálják.

3.3.1. Elektronikus levelezés

- Rendeltetésszerű használat: Az Egyetem által biztosított e-mail fiókok használata kötelező a hivatalos ügyintézéshez és kommunikációhoz. Az e-mail rendszer nem használható tömeges, kéretlen reklámanyag vagy spam küldésére, illetve jogellenes tartalom terjesztésére.
- Bizalmasság: A felhasználók kötelesek gondoskodni e-mail fiókjuk jelszavának védelméről és a bizalmas információk megfelelő titkosításáról.
- Védelmi mechanizmusok: Tilos az e-mail rendszerbe épített vírus- és spamvédelem megkerülése vagy kikapcsolása, valamint gyanús mellékletek megnyitása.
- Személyes célú használat: A munkahelyi e-mail címet elsődlegesen az Egyetem működésével, oktatási-kutatási tevékenységével és hivatali ügyeivel összefüggő kommunikációra lehet használni. Az e-mail fiók eseti jellegű, csekély mértékű,

magáncélú használata megengedett, amennyiben az nem sérti az Egyetem jogos érdekeit, nem jár többletköltséggel, nem akadályozza a munkavégzést, és megfelel a vonatkozó jogszabályoknak. Tilos ugyanakkor a munkahelyi e-mail cím magáncélú internetes szolgáltatásokhoz (pl. hírlevél-feliratkozás, webáruház, közösségi média vagy egyéb online fiók) való használata regisztráció céljából, kivéve, ha az közvetlenül az Egyetem tevékenységéhez kapcsolódik.

3.3.2. Internet használat

- **Rendeltetésszerű használat:** Az Egyetem által biztosított internet hozzáférés elsősorban a munkavégzéshez, kutatáshoz és oktatáshoz szükséges források elérésére szolgál.
- Tiltott tartalom: Tilos az Egyetem hálózatán jogellenes, pornográf, obszcén, rágalmazó vagy gyűlöletkeltő tartalom letöltése, megtekintése, terjesztése vagy tárolása. Tilos továbbá a szerzői jogokat sértő tartalmak letöltése, másolása vagy megosztása.
- Káros tevékenységek: Tilos olyan tevékenységek végzése, amelyek károsítják az Egyetem rendszereit, hálózatát vagy jó hírnevét (pl. illegális letöltő oldalak, szerencsejáték vagy más jogellenes tevékenységek).
- A hálózat terhelése: A hálózat tartós, nagy sávszélességű igénybevételével járó, nem oktatási vagy kutatási célú tevékenységek (pl. nagy mennyiségű szórakoztató tartalom folyamatos letöltése) tilosak. Munkavégzéshez szükséges, tartósan nagy forgalmú tevékenységet az Üzemeltetésért felelőssel előzetesen egyeztetni kell.
- **Forgalom ellenőrzése**: Az Egyetem az általa üzemeltetett hálózatok és informatikai rendszerek forgalmát biztonsági és üzemeltetési okokból – különösen a jogosulatlan hozzáférések, kártékony kódok, hálózati támadások, szolgáltatás-kiesést okozó terhelések megelőzése és kivizsgálása érdekében – jogosult ellenőrizni és szűrni.
  A forgalom-ellenőrzés és naplózás elsősorban forgalmi és naplóadatokra (pl. forrás- és célcím, időpont, protokoll, forgalom mennyisége) terjed ki, a kommunikáció tartalmának megismerése kizárólag kivételes esetben, jogszerű céllal és a vonatkozó adatvédelmi és munkajogi szabályok betartásával végezhető.

3.3.3. Saját eszközök használata

- Engedélyezés és fe**lelősség:** Az Egyetem belső hálózatához saját tulajdonú eszközzel (laptop, okostelefon, tablet, stb.) csatlakozni kizárólag a felhasználó saját felelősségére, és a jelen szabályzat 4.5.1 Mobil eszközök használata pontban meghatározott biztonsági feltételek mellett lehetséges.
- **Biztonsági ellenőrzés:** Az Egyetem hálózatára csatlakozó saját eszközök esetében a felhasználók kötelesek elfogadni, hogy az Egyetem alapvető biztonsági ellenőrzéseket végezhet (pl. hálózati forgalom monitorozása, hozzáférés korlátozása).
- Adatkezelés: Az Egyetem rendszereiből származó bizalmas adatok saját eszközön történő tartós, nem védett tárolása tilos.
- Támogatás: Az Egyetem informatikai támogatást kizárólag az Egyetem tulajdonában lévő eszközökre biztosít, a saját eszközök biztonságáért és üzemképességéért a felhasználó a felelős.
- Az Egyetem által kockázatosnak minősített elektronikus információs rendszerekhez (EIR), valamint bármely rendszerhez rendszergazdai vagy azzal egyenértékű adminisztratív jogosultsággal történő hozzáféréshez saját tulajdonú eszköz nem

használható. Ilyen hozzáférés kizárólag az Egyetem által biztosított, menedzselt eszközről engedélyezhető.

4. Logikai biztonság

Az Egyetem biztosítja, hogy az információvagyonhoz és az azt kezelő EIR-ekhez, az EIR-ek rendszerelemeihez és az EIR-ek által nyújtott vagy azokon keresztül elérhető szolgáltatásokhoz való hozzáférés szabályozott, dokumentált és a szükséges mértékre korlátozott legyen. A hozzáférés-kezelés elsődleges célja az információk bizalmasságának, sértetlenségének és rendelkezésre állásának megőrzése az illetéktelen hozzáférés, módosítás, közzététel vagy megsemmisítés megakadályozásával.

A fizikai hozzáférésekre vonatkozó szabályokat az 5.1. Fizikai hozzáférés-szabályozás pont tartalmazza.

A hozzáférések felügyeletével kapcsolatos szabályok és kötelezettségek megismertetéséről és annak dokumentálásáról az Egyetem a 11. Személyi biztonság pontban meghatározottak szerint gondoskodik.

4.1. Azonosítás és hitelesítés elvei

Az Egyetem adataihoz, elektronikus információs rendszereihez (EIR-ek) való hozzáférés kizárólag megfelelő azonosítás és hitelesítés útján történhet. Az azonosítás és hitelesítés célja, annak biztosítása, hogy az informatikai rendszerekhez és az azokban tárolt adatokhoz kizárólag az arra jogosult személyek férhessenek hozzá.

Alapelvek

- Egyedi azonosítás: Minden felhasználónak egyedi azonosítóval (felhasználónév) kell rendelkeznie. Közös vagy megosztott fiókok használata kizárólag kivételes esetben, Információbiztonság Szabályozásáért Felelős Vezető engedélyével történhet.
- Hitelesítés: Az azonosítást minden esetben hitelesítési eljárásnak kell követnie, amely lehet jelszavas, kétfaktoros (2FA), vagy más, az adott rendszerhez illeszkedő módszer.
- Privilegizált fiókok: A magasabb szintű hozzáféréssel rendelkező fiókok esetében minden esetben kötelező a többtényezős hitelesítés alkalmazása, amennyiben azt az adott rendszer támogatja.
- **Csoportszintű hozzáférés:** Csak akkor engedélyezhető, ha a rendszer nem teszi lehetővé az egyéni azonosítást, és a hozzáférés kizárólag adatmegtekintésre szolgál, nem tesz lehetővé módosítást.
- Anonim hozzáférés: Alapértelmezetten tilos, kivéve, ha azt az adott rendszer rendszerbiztonsági terve kifejezetten engedélyezi.
- Új EIR-ek: Fejlesztés vagy beszerzés esetén az azonosítási és hitelesítési követelmények teljesülését előzetesen vizsgálni kell, és amennyiben lehetséges, azok érvényesítését elvárásként kell megfogalmazni.
- Legkisebb jogosultság elve: A felhasználók és rendszerek kizárólag a feladataik ellátásához szükséges információkhoz, informatikai erőforrásokhoz (EIR-ekhez) és funkciókhoz férhetnek hozzá, a lehető legszűkebb hozzáférési jogosultsági szinten. Ez magában foglalja az adatok olvasási, írási, módosítási és törlési jogát, valamint a rendszerek funkcióinak használati lehetőségét, kizárólag a releváns üzleti folyamatokhoz kapcsolódóan.

A legkisebb jogosultság elvét minden olyan rendszerben érvényesíteni kell, ahol a jogosultságok technikailag szabályozhatók. Központilag szabályozott vagy külső szolgáltató által üzemeltetett rendszerek (pl. országos tanulmányi, adatszolgáltató vagy SaaS-alkalmazások) esetében a felhasználók csak olyan szerepkörökhöz, modulokhoz vagy funkciókhoz kaphatnak hozzáférést, amelyek a szolgáltató által biztosított jogosultsági modell keretein belül elérhetők.

4.1.1. Jelszópolitika

Az Egyetem elkötelezett aziránt, hogy az Elektronikus Információs Rendszerekhez (EIR-ekhez) és az azokban tárolt adatokhoz való hozzáférést hatékonyan szabályozza. Ennek alapvető eleme a biztonságos jelszavak használata és kezelése, amely megakadályozza a jogosulatlan hozzáférést, az információk sérülését, közzétételét vagy elvesztését. Ez a jelszópolitika minden Egyetemmel jogviszonyban álló személyre, valamint minden olyan EIR-re vonatkozik, amely jelszavas hitelesítést alkalmaz.

Az adott Alkalmazásgazda, illetve az Üzemeltetésért felelős személy köteles az alábbi jelszókövetelményeket technikai eszközökkel érvényesíteni, amennyiben az adott rendszer ezt lehetővé teszi. Amennyiben a rendszer nem támogatja a beállításokat, a felhasználók kötelesek az alábbi szabályokat betartani.

Jelszókövetelmények

A jelszavaknak meg kell felelniük az alábbi minimális követelményeknek:

- Karakterszám: A jelszónak legalább 10 karakter hosszúságúnak kell lennie. Kiemelt vagy adminisztratív jogosultsággal rendelkező fiókok esetében törekedni kell legalább 12 karakter hosszúságú jelszavak használatára.
- Karaktertípusok: A jelszónak kötelezően tartalmaznia kell kisbetűt (a-z), nagybetűt (A-Z) és számot (0-9). Speciális karakter használata nem kötelező, de javasolt.
- Komplexitás: A jelszó nem lehet könnyen kitalálható, és nem tartalmazhatja a felhasználónév, a személyes adatok (pl. név, születési dátum), vagy az Egyetem nevének egy részét. Kerülni kell a szótárban megtalálható szavak vagy egyszerű számsorok használatát.
- Jelszótörténet: A felhasználó nem állíthat be olyan jelszót, amely megegyezik az utolsó öt (5) korábbi jelszavával.
- Jelszó Lejárat:
    - Azokon az Elektronikus Információs Rendszereken (EIR-eken), ahol a 4.1. Azonosítás és hitelesítés elvei pontban meghatározottak szerint kötelező a többtényezős hitelesítés (MFA) alkalmazása, ott nincs előírt időszakos jelszóváltási kötelezettség. Ezen rendszerek esetén a jelszó lejáratát az Egyetem az MFA nyújtotta többletvédelem figyelembevételével határozza meg, a felhasználói kényelem és a biztonság egyensúlyának optimalizálása érdekében.
    - Azokon az EIR-eken azonban, ahol nem kötelező a többtényezős hitelesítés alkalmazása, a felhasználói jelszavakat legalább 180 naponta meg kell változtatni.

Jelszókezelési Eljárások

A felhasználók felelősek jelszavaik biztonságos kezeléséért és titokban tartásáért.

Titoktartás:

- A jelszavakat szigorúan bizalmasan kell kezelni. Tilos azokat másokkal megosztani, függetlenül attól, hogy a másik személy az Egyetem munkavállalója vagy külső partner.
- Tilos a jelszavakat felírni, felragasztani a monitorra, billentyűzetre, vagy bármilyen olyan helyre, ahol illetéktelenek hozzáférhetnek.
- Digitális formában, pl. jelszókezelő szoftverben történő tárolás esetén az adatoknak titkosítottnak és jelszóval védettnek kell lenniük.

Kezdeti Jelszavak:

- Az újonnan létrehozott felhasználói fiókokhoz generált kezdeti jelszavaknak véletlenszerűnek és komplexnek kell lenniük.
- Az első bejelentkezés alkalmával a felhasználó köteles megváltoztatni a kezdeti jelszót.

Jelszó Visszaállítása:

- A jelszó elfelejtése vagy kompromittálódásának gyanúja esetén az Alkalmazásgazda, vagy az Üzemeltetésért felelős személy jogosult a jelszó visszaállítására.
- A visszaállított jelszónak meg kell felelnie a meghatározott jelszókövetelményeknek.

Jelszóval kapcsolatos incidensek kezelése

- Amennyiben a felhasználó gyanús tevékenységet észlel fiókjával kapcsolatban, vagy úgy véli, hogy jelszava illetéktelen kezekbe került (kompromittálódott), köteles a jelszavát haladéktalanul megváltoztatni és az eseményt azonnal jelezni közvetlen felettesének és az Üzemeltetésért felelősnek.
- A jelszóval kapcsolatos gyanús eseményeket informatikai biztonsági eseményként kell kezelni. Az incidens további kivizsgálása, a szükséges intézkedések meghatározása és a rendszer(ek) biztonságos állapotának helyreállítása az Informatikai Katasztrófaterv 4. Informatikai incidensek kezelése pontban rögzítettek szerint történik, az Üzemeltetésért felelős és az Információbiztonsági Felelős (IBF) bevonásával.

4.2. Felhasználói fiókok kezelése

A felhasználói fiókok kezelése az Elektronikus Információs Rendszerek (EIR) biztonságos működésének és az adatokhoz való hozzáférés ellenőrzésének alapvető eleme. Az Egyetem célja, hogy a felhasználói fiókok létrehozása, módosítása, felfüggesztése és törlése szabályozott, átlátható és ellenőrizhető módon, az információbiztonsági elveknek megfelelően történjen.

4.2.1. Fióktípusok és jogosultsági szintek

Az Egyetem által használt EIR-ekben engedélyezett és tiltott fióktípusokat, azokhoz tartozó jogosultsági szinteket, valamint azok jellemzőit az adott EIR Rendszerbiztonsági terve határozza meg és dokumentálja. Kiemelt figyelmet kell fordítani a privilegizált fiókokra (pl.

rendszergazdai fiókok), amelyek esetében fokozott biztonsági követelmények és ellenőrzési mechanizmusok alkalmazása kötelező a megnövelt kockázat miatt.

4.2.2. Fiókkezelési eljárásrend

A Fiókkezelési eljárásrend célja, biztosítani, hogy az Egyetem informatikai rendszereiben használt felhasználói fiókok létrehozása, módosítása és megszüntetése szabályozott, dokumentált és ellenőrzött módon történjen, így megakadályozva az illetéktelen hozzáféréseket.

Fiók létrehozása

- Fiók létrehozása csak jóváhagyott igény alapján történhet.
- Az igénylőnek meg kell adnia:
  - az igényelt fiók típusát (saját, csoport, szolgáltatásfiók),
  - a szükséges jogosultsági szintet,
  - a hozzáférés indokát és időtartamát.
- A jóváhagyásról az adott EIR Rendszerbiztonsági tervében rögzített adatgazda dönt.
- A létrehozásról az Üzemeltetésért Felelős, vagy az adott Alkalmazásgazda gondoskodik.

Fiók módosítása

- Jogosultság módosításra szintén írásos vagy elektronikus igénybejelentés alapján kerül sor.
- Az IBF ellenőrizheti, hogy a módosítás arányos-e a feladatkörrel.
- A módosítást dokumentálni kell a nyomon követhetőség érdekében.

Fiók megszüntetése

- Munkaviszony, megbízás vagy hallgatói jogviszony megszűnésekor a felhasználói fiókot a megszűnés napján, de legkésőbb 24 órán belül le kell tiltani.
- A jogviszony megszűnését a Tanulmányi Osztály, a Humánerőforrás-menedzsmentért felelős, vagy az adott szervezeti egység köteles írásban jelezni az Adatgazda, az Üzemeltetésért Felelős és az Alkalmazásgazda felé.
- Az adatok archiválásáról a szervezeti egység vezetője és az Üzemeltetésért felelős közösen gondoskodik.
- Ideiglenes fiókok esetében a lejárati időt - ha az adott rendszer támogatja – kötelezően be kell állítani, így a lejárat után automatikusan deaktiválódnak.

4.2.3. Sikertelen bejelentkezési kísérletek kezelése

Az egyes EIR-ek Rendszerbiztonsági tervei rögzítik és dokumentálják a fiókzárolási házirendeket.

Adatvédelmi és információbiztonsági szempontból elvárás, hogy – amennyiben az adott EIR lehetőséget biztosít – a rendszer:

- automatikusan zárolja a felhasználói fiókot, ha egymást követően előre meghatározott, konfigurálható számú (legfeljebb 10) sikertelen bejelentkezési kísérlet történik (fiókzárolási küszöb),

- a zárolás automatikusan feloldódjon egy előre beállított, konfigurálható időtartam elteltével (fiókzárolás időtartama, jellemzően 15 perc és 24 óra között),
- vagy a zárolás feloldása kizárólag az Üzemeltetésért Felelős vagy más, erre kijelölt szerepkör adminisztrátori beavatkozásával történjen.

4.3. Hozzáférési jogosultságok felügyelete

Az Egyetem elkötelezett az információvagyonhoz és az azt kezelő rendszerekhez való hozzáférési jogosultságok folyamatos és hatékony felügyelete iránt, biztosítva ezzel az információbiztonsági elvek és a vonatkozó jogszabályi előírások betartását. A jogosultság felügyelet célja annak ellenőrzése, hogy minden hozzáférés kizárólag a szükséges mértékben, a legkisebb jogosultság elvét követve, a felhasználó aktuális feladatköréhez igazodva legyen engedélyezve.

4.3.1. **Rendszeres felülvizsgálat és ellenőrzés**

Az Egyetem biztosítja, hogy a hozzáférési jogosultságok, beleértve a felhasználói fiókokhoz (lásd: *4.2.2. Fiókkezelési eljárásrend*), csoportokhoz, illetve a rendszerszintű és alkalmazásspecifikus jogosultságokhoz rendelt jogokat is, rendszeres időközönként, de legalább évente felülvizsgálatra kerüljenek. A felülvizsgálat során ellenőrizni kell, hogy a jogosultságok továbbra is indokoltak, naprakészek, és összhangban vannak a felhasználók aktuális feladatkörével, valamint az Egyetem belső szabályozásával és az alkalmazandó jogszabályokkal. A felülvizsgálatok során feltárt eltéréseket és minden gyanús vagy jogosulatlan hozzáférési kísérletet haladéktalanul meg kell szüntetni és jelenteni kell az Információbiztonsági Felelős (IBF) részére.
A felülvizsgálat végrehajtásáért az adott alkalmazás Alkalmazásgazdája és Adatgazdája közösen, az ellenőrzésért az Információbiztonsági Felelős (IBF) felel.

4.3.2. Jogosultsági dokumentáció és nyilvántartás

Az összes hozzáférési jogosultságot, beleértve a felhasználói fiókokhoz, csoportokhoz és rendszerekhez rendelt jogokat, pontosan és részletesen dokumentálni kell (pl. jogosultsági mátrix, nyilvántartások). A dokumentációnak mindig tükröznie kell a ténylegesen érvényes jogosultságokat, és biztosítani kell annak hozzáférhetőségét, integritását és rendszeres frissítését.
A dokumentáció elkészítéséért és naprakészen tartásáért az adott alkalmazás Alkalmazásgazdája és az Adatgazdája, annak tartalmának ellenőrzéséért és felügyeletéért az Információbiztonsági Felelős (IBF) felel.

4.3.3. Feladatkörök szétválasztása

A visszaélések, hibák és jogosulatlan tevékenységek kockázatának minimalizálása érdekében biztosítani kell a kritikus informatikai feladatkörök és a hozzájuk tartozó jogosultságok szétválasztását. Ez magában foglalja többek között az adminisztrátori, fejlesztői, tesztelői és éles üzemeltetési jogosultságok, valamint az adatok, tranzakciók rögzítésével, jóváhagyásával, lekérdezésével kapcsolatos jogkörök elkülönítését, amennyiben ez technológiai és szervezeti szempontból megvalósítható.

4.4. Távoli és vezeték nélküli hozzáférés

Az Egyetem az Elektronikus Információs Rendszerekhez (EIR) való távoli és vezeték nélküli hozzáférés szabályait, valamint a kapcsolódási és konfigurációs követelményeket az EIR Rendszerbiztonsági tervében határozza meg és dokumentálja. A rendszerbiztonsági tervben meghatározott beállítások végrehajtásáért az Üzemeltetésért felelős egység felel.

4.4.1. Távoli hozzáférés

A távoli hozzáférés kizárólag biztonságos, titkosított adatátviteli csatornákon keresztül történhet (VPN – Virtual Private Network, TLS, SSH), és csak indokolt esetben, előzetes jóváhagyással engedélyezhető. Ez vonatkozik mind a felhasználói, mind az üzemeltetési célú (pl. távsegítség, rendszeradminisztráció) hozzáférésekre is.

A távoli hozzáféréshez használt vagy tervezett technológia biztonsági megfelelőségét az Információbiztonsági Felelős (IBF) jogosult megvizsgálni. Amennyiben a megoldás megfelelő biztonsági funkciókat biztosít, az Információbiztonság Szabályozásért Felelős Vezető az IBF javaslata alapján dönt annak engedélyezéséről. Ellenkező esetben a követelményeknek megfelelő rendszer alkalmazását kell elrendelni.

A távoli hozzáférésekre vonatkozó eseményeket részletesen naplózni kell a 7.2. Naplózás és monitorozás pontban meghatározottak szerint, lehetővé téve a biztonsági incidensek kivizsgálását és az elszámoltathatóságot.

4.4.2. Vezeték nélküli hozzáférés

A munkavégzés céljára, adminisztratív és belső üzemeltetési feladatok ellátására szolgáló vezeték nélküli hálózatoknak legalább jelszavas védelemmel, korszerű titkosítással kell rendelkeznie. E hálózatokhoz kizárólag az Egyetem által biztosított vagy felügyelt, menedzselt eszközök csatlakozhatnak.

Az Egyetem hallgatói és vendég Wi-Fi hálózataihoz saját tulajdonú eszközökkel is engedélyezett a csatlakozás, a 3.3.3. pontban és a jelen fejezetben meghatározott biztonsági feltételek mellett. A hallgatói és vendég hálózatoknak logikailag elkülönítetten kell működniük az Egyetem belső, adminisztratív hálózataitól, és nem biztosíthatnak közvetlen hozzáférést az Egyetem belső rendszereihez és adataihoz.

A vezeték nélküli hálózatok konfigurációja során biztosítani kell a csatlakozó eszközök azonosítását és a hálózati hozzáférések naplózását, valamint alkalmazni kell a biztonsági legjobb gyakorlatokat.

4.4.3. A biztonságos vezeték nélküli használat szabályai

A vezeték nélküli hálózatokhoz való hozzáférés során a felhasználóknak különös figyelmet kell fordítaniuk az információbiztonsági kockázatokra és a megfelelő védelmi intézkedésekre.
A biztonságos vezeték nélküli használat szabályai a következők:

a) A felhasználó köteles kizárólag jelszóval védett, megbízható hálózatokhoz csatlakozni.
b) A nyilvános vagy ismeretlen Wi-Fi hálózatok használatát – különösen érzékeny vagy bizalmas adatok elérésekor – kerülni kell.

c) A saját tulajdonú eszközökön naprakész operációs rendszer és vírusvédelem alkalmazása kötelező.
d) A vezeték nélküli hálózathoz csatlakozó eszközökön automatikus csatlakozás idegen hálózatokra tilos.
e) A felhasználónak be kell tartania az Egyetem által kiadott információbiztonsági és adatvédelmi szabályokat, valamint haladéktalanul jeleznie kell az IBF felé, ha biztonsági eseményt észlel (pl. gyanús hálózati viselkedés, adatvesztés, illetéktelen hozzáférés gyanúja).

4.5. **Mobil eszközök és külső rendszerek**

A mobil eszközök és külső rendszerek használata elengedhetetlen a korszerű munkavégzéshez, ugyanakkor ezek fokozott információbiztonsági kockázatot is jelentenek. Ennek megfelelően az alábbi szabályokat kell alkalmazni minden olyan esetben, amikor az Egyetem információvagyonához való hozzáférés mobil eszközön vagy külső rendszerből történik.

4.5.1. Mobil eszközök használata

- Hozzáférési szabályok:
  Az Egyetem által biztosított alapvető szolgáltatásokhoz (pl. e-mail, naptár, Teams, e-learning rendszerek) egyetemi és – a 3.3.3. pontban foglaltak szerint – engedélyezett saját tulajdonú mobil eszközről is lehet csatlakozni.
  Az adminisztratív rendszerekhez és nagy mennyiségű, bizalmas adatot kezelő EIR-ekhez mobil eszközről főszabályként csak az Egyetem által biztosított, menedzselt mobil eszközről engedélyezett a hozzáférés. Ettől eltérni csak akkor lehet, ha az adott EIR Rendszerbiztonsági Terve vagy az alkalmazás Alkalmazásbiztonsági adatlapja ezt kifejezetten megengedi.
- Biztonsági követelmények:
  Az Egyetem által a felhasználók számára biztosított mobil eszköz, illetve az engedélyezett saját tulajdonban lévő mobil eszköz csak akkor csatlakozhat az Egyetem hálózatához, ha az eszköz megfelel az alábbi követelményeknek:
  - naprakész operációs rendszer és biztonsági frissítések,
  - aktív vírusvédelem és tűzfal,
  - jelszavas vagy biometrikus zárolás,
  - automatikus képernyőzár rövid inaktivitás után,
  - az adatok titkosítása (ha lehetséges).
- Eseménykezelés:
  Az eszköz elvesztését, ellopását vagy kompromittálódását haladéktalanul írásban jelenteni kell az IBF részére.

4.5.2. Külső rendszerekhez való hozzáférés

Külső rendszernek minősül minden olyan informatikai rendszer, amely nem az Egyetem közvetlen irányítása alatt áll (pl. felhőszolgáltatások, szerződött partnerek által üzemeltetett rendszerek stb.).

A hozzáférés során amennyiben lehet, biztosítani kell a titkosított adatátvitelt (pl. VPN, HTTPS), valamint a hitelesítés legalább kétfaktoros módját.

Az Egyetem információinak külső rendszerbe történő átvitele során vizsgálni kell, hogy az érintett szolgáltató adatfeldolgozóként vagy önálló adatkezelőként jár-e el.

Amennyiben a szolgáltató adatfeldolgozónak minősül, az együttműködés feltétele egy olyan írásbeli szerződés (ideértve az adatfeldolgozói szerződést is), amely egyértelműen rögzíti a titoktartási, adatvédelmi és információbiztonsági kötelezettségeket, valamint az adattovábbítás célját és kereteit.

4.6. Azonosítás/hitelesítés nélküli hozzáférések kezelése

Az elektronikus információs rendszerekhez (EIR-ekhez) való hozzáférés kizárólag megfelelő azonosítást és hitelesítést követően engedélyezett. Kivételt kizárólag azok a felhasználói tevékenységek képezhetnek, amelyek az adott EIR Rendszerbiztonsági tervében előzetesen azonosításra, dokumentálásra és jóváhagyásra kerültek.

4.6.1. Engedélyezett kivételek

Az Egyetem az EIR-ek Rendszerbiztonsági tervében köteles azonosítani és dokumentálni azokat a tevékenységeket, amelyek az adott rendszerben azonosítás vagy hitelesítés nélkül is végrehajthatók. Ilyen tevékenységek kizárólag akkor engedélyezhetők, ha:

- nem járnak személyes, bizalmas vagy védett adatok elérésével,
- nem teszik lehetővé adatmódosítást vagy rendszerkonfiguráció változtatását,
- kizárólag nyilvánosan közzétett, olvasható tartalmakhoz biztosítanak hozzáférést.

4.6.2. **Felelősség és ellenőrzés**

Az azonosítás vagy hitelesítés nélküli hozzáférések engedélyezéséért és dokumentálásáért az adott alkalmazás Adatgazdája, a beállítások technikai érvényesítéséért pedig az Alkalmazásgazda felel.

Az Információbiztonsági Felelős (IBF) köteles kétévente ellenőrizni az ilyen hozzáférések meglétét, indokoltságát és naprakész dokumentáltságát.

4.7. **Hitelesítő eszközök kezelése**

Az Egyetem az információbiztonság megerősítése érdekében a jelszavas hitelesítésen túlmenően különféle hitelesítő eszközöket is alkalmazhat. Ezek használata különösen indokolt privilegizált hozzáférések, távoli elérés, valamint érzékeny vagy különleges adatokhoz való hozzáférés esetén.

4.7.1. **Hitelesítő eszközök típusai**

A hitelesítő eszközök körébe tartoznak többek között:

- Hardveres tokenek (pl. időalapú egyszer használatos jelszót generáló eszközök),
- Intelligens kártyák (pl. chipkártyák, belépőkártyák),
- Biometrikus azonosítók (pl. ujjlenyomat, arcfelismerés),
- Digitális tanúsítványok és kriptográfiai kulcsok.

4.7.2. Kiadás és nyilvántartás

- A hitelesítő eszközök kiadását az Üzemeltetésért felelős egység végzi, az Információbiztonsági Felelős (IBF) jóváhagyásával.

- Minden kiadott eszközt egyedi azonosítóval kell nyilvántartani, és a kiadás tényét dokumentálni kell.
- A felhasználó köteles az eszköz átvételét írásban vagy elektronikusan visszaigazolni.

4.7.3. Használat és biztonság

- A hitelesítő eszközöket kizárólag az arra jogosult személy használhatja.
- Az eszközöket tilos más személynek átadni, megosztani vagy más módon hozzáférhetővé tenni.
- Az eszköz elvesztését, sérülését vagy kompromittálódását a felhasználó köteles haladéktalanul jelenteni az IBF részére.

4.7.4. Visszavétel és selejtezés

- A hitelesítő eszközt a felhasználói jogviszony megszűnésekor, vagy az eszköz használatának megszűnése esetén vissza kell szolgáltatni.
- A visszavett eszközöket az Üzemeltetésért felelős egység köteles deaktiválni, és szükség esetén biztonságosan megsemmisíteni vagy újrahasznosítani.
- A visszavétel tényét dokumentálni kell.

4.7.5. **Ellenőrzés**

Az IBF kétévente köteles ellenőrizni a hitelesítő eszközök nyilvántartását, használatát és a kapcsolódó biztonsági intézkedések betartását.

4.8. Újrahitelesítés és munkaszakasz zárolás

Az Egyetem biztosítja, hogy az Elektronikus Információs Rendszerekhez (EIR-ekhez) való hozzáférés során a felhasználói munkamenetek megfelelően védettek legyenek, és az inaktív állapotban lévő munkamenetek ne jelentsenek biztonsági kockázatot. Amennyiben az adott EIR ezt támogatja vagy technikailag megvalósítható, automatikus zárolási és újrahitelesítési mechanizmusok kerülnek alkalmazásra a jogosulatlan hozzáférés és az információszivárgás kockázatának csökkentése érdekében.

4.8.1. Újrahitelesítési kötelezettség

Az Egyetem EIR-jeiben a felhasználókat bizonyos időközönként, vagy kritikus műveletek elvégzése előtt kötelező újra hitelesíteni. Ez a követelmény hozzájárul ahhoz, hogy még egy esetlegesen kompromittált vagy felügyelet nélkül hagyott munkamenet esetén is minimálisra csökkenjen az információbiztonsági kockázat.

Az újrahitelesítés szükségessége az adott EIR kockázati szintjétől, az általa kezelt adatok érzékenységétől és a végrehajtott művelet jellegétől függően kerül meghatározásra.

Az egyes EIR-ek rendszerbiztonsági terve tartalmazza azokat a konkrét időintervallumokat (pl. 2-4 óra inaktivitás után), vagy azokat a kritikus műveleteket (pl. bizalmas adatok módosítása, privilegizált funkciók használata), amelyek újrahitelesítést vonnak maguk után.

Az újrahitelesítés az eredeti bejelentkezéshez hasonlóan, jelszóval, többfaktoros azonosítással (MFA), vagy más, az EIR-ben engedélyezett hitelesítési módszerrel történhet.

Azon munkaállomásokon, melyek az Egyetem hálózatához csatlakoznak, vagy Egyetemi adatokhoz férnek hozzá, kötelező az automatikus képernyőzárolás beállítása egy előre

meghatározott, konfigurálható inaktivitási idő (javasoltan 15 perc) után. A képernyő feloldásához a felhasználónak újra hitelesítenie kell magát.

Amennyiben az adott EIR támogatja vagy technikailag megvalósítható, az EIR-ek és webes alkalmazások automatikusan kijelentkeztetik (session timeout) a felhasználókat egy meghatározott inaktivitási idő (javasoltan 15-30 perc) elteltével. Ez az időtartam az adott rendszer kockázati szintjéhez igazodik.

A felhasználók kötelesek manuálisan zárolni munkaállomásaikat és kijelentkezni az EIR-ekből, amikor felügyelet nélkül hagyják azokat, még rövid időre is.

Ezen szabályok alól kivételt képezhetnek azok az automatizált folyamatok vagy szolgáltatások, amelyek folyamatos munkamenetet igényelnek, azonban ezek esetében az EIR rendszerbiztonsági tervében részletes kockázatelemzést és indoklást kell dokumentálni, valamint megfelelő kompenzáló vezérlőket (pl. hálózati szegmentálás, szigorúbb naplózás) kell alkalmazni.

5. Fizikai és környezeti biztonság

Az Egyetem célja, hogy a fizikai és környezeti biztonság szabályozásával megvédje az Elektronikus információs rendszerekhez kapcsolódó eszközöket, adathordozókat és infrastruktúrát a jogosulatlan fizikai hozzáféréstől, károsodástól, lopástól, valamint a környezeti hatásokból eredő veszélyektől.

5.1. Fizikai hozzáférés-szabályozás

Az Egyetem épületeibe a foglalkoztatottakon kívül hallgatók, látogatók, vendégek és más külső személyek is beléphetnek.

Ugyanakkor az Egyetem területén találhatóak olyan kiemelten védett helyiségek, amelyekhez való hozzáférés engedélyköteles, és kizárólag jogosult személyek számára biztosított. Ilyen helyiségek például az Egyetem által használt EIR-ek rendszerelemeinek helyt adó szervertermek, aktív hálózati eszközöket tartalmazó hálózati elosztóhelyiségek.

Ezen helyiségek fizikai védelmét beléptető rendszer, zárt ajtók, kulcskezelés, vagy elektronikus azonosítóval történő hozzáférés biztosítja. A hozzáférési jogosultságok kialakítását és kezelését az Informatikai Katasztrófaterv szerint kell végezni.

Az állandó belépésre nem jogosult személyek (pl.: látogatók, munkavégzésre irányuló szerződéses jogviszonyban álló karbantartók stb.) kiemelten védett helyiségekben csak felügyelet mellett tartózkodhatnak, illetve végezhetnek munkát. A felügyelet biztosítása az ideiglenes belépési engedéllyel rendelkező személyt fogadó és/vagy kíséretét ellátó foglalkoztatott, az informatikai erőforrásokat koncentráltan tartalmazó, illetve az EIR-ek központi rendszerelemeinek helyt adó helyiség (pl.: szerver szoba) esetében az Üzemeltetésért felelős feladata. A belépések adatait az őket fogadó és/vagy kíséretüket, felügyeletüket ellátó foglalkoztatott köteles a belépésekről vezetett nyilvántartásban (belépési napló) rögzíteni.

A jogosulatlan belépési kísérleteket, valamint az azonosítás nélküli belépést kísérő eseményeket vizsgálni kell, és szükség esetén informatikai biztonsági eseményként kell kezelni.

Az Egyetem saját rendelkezésében, illetve felügyelete alatt álló, látogatók számára folyamatosan vagy ideiglenesen (pl.: átszervezés, költözés, átépítés miatt) nyitott, felügyelet

nélkül hozzáférhető területein, helyiségeiben gondoskodni kell arról, hogy a hálózathoz való csatlakozásra alkalmas, szabad hálózati végpontokról közvetlenül ne legyen jogosulatlan hozzáférés az Egyetem belső hálózataihoz. Ennek eszköze lehet többek között a végpontok letiltása, fizikai leválasztása vagy hálózati szűrés alkalmazása.

Fizikai hozzáféréssel kapcsolatos biztonsági esemény gyanújának felmerülése, bekövetkezése, illetve észlelése esetén a jelen Szabályzat 10.1 Biztonsági események jelentése pontban foglaltak szerint az azt észlelő haladéktalanul köteles jelezni közvetlen felettese számára.

5.2. Környezeti biztonság

Az Egyetem gondoskodik arról, hogy az Elektronikus információs rendszerek és az azokat kiszolgáló infrastruktúra – különösen a szerverhelyiségek, hálózati elosztók, adattároló eszközök – olyan környezeti feltételek között működjenek, amelyek minimálisra csökkentik a természeti, technológiai vagy emberi eredetű környezeti károkból eredő kockázatokat.

A környezeti biztonságot az alábbi intézkedésekkel kell biztosítani:

- Hőmérséklet- és páratartalom-szabályozás: A szervertermekben és hálózati eszközöket tartalmazó helyiségekben biztosítani kell az eszközök működési hőmérséklet-tartományának megfelelő hűtést és szellőzést. A környezeti paraméterek figyelését automatizált rendszereknek kell végezni.
- Tűzvédelmi intézkedések: Minden informatikai berendezést tartalmazó helyiségben érvényes tűzvédelmi szabályzatnak megfelelően tűzérzékelő rendszert, valamint az informatikai eszközök védelmére alkalmas tűzoltó berendezést (pl. inert gázos oltórendszert, CO_2-oltót) kell alkalmazni. A kézi tűzoltó készülékek meglétéről és időszakos felülvizsgálatáról gondoskodni kell.
- Áramszünet elleni védelem: Kritikus eszközöket – például szervereket, adatmentő eszközöket, hálózati eszközöket – szünetmentes tápegységgel (UPS) kell védeni az áramkimaradás és feszültségingadozás hatásai ellen.
- Víz- és nedvesség elleni védelem: Az informatikai eszközök nem helyezhetők el olyan helyiségben, ahol csőtörés, beázás, magas páratartalom vagy egyéb vízkárok veszélye fennáll. Szükség esetén vízérzékelő rendszer beépítéséről kell gondoskodni.
- Por, szennyeződés, rágcsálók elleni védelem: Az IT-eszközök elhelyezésére szolgáló helyiségeknek tisztának, pormentesnek, jól zárhatónak kell lenniük. Gondoskodni kell arról, hogy rágcsálók vagy más élőlények ne férhessenek hozzá a kábelekhez, hálózati eszközökhöz.
- Fizikai károsodás elleni védelem: Az érzékeny eszközöket megfelelő mechanikai védelemmel kell ellátni (pl. zárt rack szekrény), valamint védeni kell őket a véletlen fizikai behatásoktól (pl. leejtés, ütődés, túlterhelés).

5.3. Adathordozók és hordozható eszközök átfogó védelme

Az Egyetem biztosítja, hogy a kezelésében lévő digitális és papír alapú adathordozók, valamint a beépített adattárolót tartalmazó hordozható eszközök (pl. laptopok, táblagépek, okostelefonok, külső merevlemezek, pendrive-ok, memóriakártyák, optikai lemezek) teljes életciklusuk során védettek legyenek a jogosulatlan hozzáférés, károsodás, lopás és adatszivárgás ellen. Ezen intézkedések célja az információvagyon bizalmasságának, sértetlenségének és rendelkezésre állásának megőrzése.

5.3.1. Általános szabályok és felhasználói felelősség

Az Egyetem által biztosított adathordozókhoz és hordozható eszközökhöz, valamint az azokon tárolt információvagyonhoz kizárólag a munka- és feladatkörük ellátásához szükséges mértékben, az arra feljogosított személyek férhetnek hozzá.

A foglalkoztatottak felelősek a rájuk bízott adathordozók és hordozható eszközök fizikai védelméért, biztonságos tárolásáért és kezeléséért. Ez magában foglalja az eszközök és adathordozók felügyelet nélküli hagyásának elkerülését.

Tilos az adathordozókat és hordozható eszközöket felügyelet nélkül, illetéktelenek számára hozzáférhető helyen hagyni (pl. asztalon, nem zárható fiókban, vagy közterületen parkoló, zárt gépjárműben sem). Használaton kívül azokat zárható fiókban, szekrényben kell tárolni.

A logikai védelemről (pl. titkosítás, jelszavas vagy biometrikus zárolás) a 4.5.1 Mobil eszközök használata pontban foglaltak az irányadóak.

Papír alapú adathordozók (dokumentumok) védelméről és kezeléséről az Egyetem Iratkezelési Szabályzata az irányadó.

5.3.2. Külső és ismeretlen adathordozók csatlakoztatása

Az Egyetem által használt EIR-ekhez és rendszerelemeikhez elsősorban az Egyetem által biztosított vagy ellenőrzött adathordozók csatlakoztatása engedélyezett.

Ettől eltérően, oktatási vagy adminisztratív célból – például hallgatói beadandók, prezentációk, külső partnertől származó dokumentumok átvétele esetén – külső adathordozó is csatlakoztatható az alábbi feltételekkel:

- az adathordozó tulajdonosa és származása ismert és beazonosítható,
- az adathordozót használat előtt vírusellenőrzésnek kell alávetni, vagy kizárólag olvasási jogosultsággal szabad megnyitni,
- amennyiben lehetséges, az adathordozót nem hálózatra csatlakoztatott (izolált) munkaállomáson kell megnyitni,
- az adathordozóról az Egyetem rendszerébe csak ellenőrzött fájlok másolhatók be.

Tilos olyan idegen adathordozót csatlakoztatni, amelynek tulajdonosa, származása vagy tartalma nem ismert, illetve amely fertőzésgyanús.

Engedély nélküli, vagy a fenti feltételeket megszegő adathordozó-használat információbiztonsági eseménynek minősül, amely a 10. Biztonsági események kezelése pontban, illetve a 11.5. Fegyelmi intézkedések pontban meghatározott eljárást vonja maga után.

5.3.3. Eszközök és adathordozók szállítása

Az informatikai eszközök – különösen adattárolókat is tartalmazó berendezések – és adathordozók szállítása során biztosítani kell, hogy azok ne sérüljenek meg, és illetéktelenek ne férhessenek hozzájuk.

Az Egyetem ellenőrzött, felügyelt környezetéből kikerülő, adattovábbítás céljából szállított digitális adathordozón tárolt adatokat, amennyiben azok típusa vagy bizalmasságuk indokolja, a szállítást megelőzően az adathordozó típusának megfelelő (pl. fájl- vagy tárolószintű) titkosítási megoldással kell ellátni. Az adattitkosítás beállításában az Üzemeltetésért felelős köteles közreműködni.

A titkosítás visszafejtéséhez szükséges kulcsot vagy kódot a címzetthez való eljuttatása a szállítástól eltérő, biztonságos kommunikációs csatornán keresztül történhet. Ez az adattovábbítással megbízott, azt kezdeményező foglalkoztatott feladata és felelőssége.

Külső szállítás esetén kizárólag megbízható, az Egyetemmel szerződéses kapcsolatban álló partnerek vagy ellenőrzött futárszolgálatok vehetnek részt a feladatban, megfelelő kíséret és dokumentáció mellett. A szállított eszközöket – lehetőség szerint – zárt, plombált csomagolásban kell mozgatni, és a feladásról, átvételről, valamint a csomag épségéről jegyzőkönyvet vagy igazolást kell készíteni.

Az Egyetem által ellenőrzött, felügyelt területről történő kiszállítását az Információbiztonság Szabályozásáért Felelős Vezető engedélyezheti, s az Üzemeltetésért felelős gondoskodik annak szakmai felügyeletéről, valamint az eszközmozgás indokának megfelelő dokumentálásáról.

Papír alapú vagy egyéb analóg adathordozó szállítására, amennyiben a továbbítandó adattartalom bizalmassága indokolja, kizárólag dokumentált és átvételi visszaigazolást biztosító kézbesítést garantáló postai vagy futárszolgáltatás vehető igénybe.

5.3.4. Ideiglenes tárolás

Az ideiglenesen nem használt, de működőképes és újrahasznosítható eszközöket, adathordozókat zárt, ellenőrzött helyiségben kell tárolni. A tárolás során meg kell akadályozni a jogosulatlan hozzáférést, továbbá védeni kell az eszközöket fizikai sérüléstől, környezeti károsodástól (pl. nedvesség, hő, por, rágcsálók).

5.3.5. Eszközök selejtezése és adatok megsemmisítése

Az életciklusuk végére ért informatikai eszközök (pl. merevlemezek, SSD-k, mobiltelefonok, pendrive-ok) selejtezése előtt az azokon tárolt minden adatot visszavonhatatlanul meg kell semmisíteni.

Kezdeményezés és felelősség: Az érintett Adatgazda vagy az Információbiztonság Szabályozásáért Felelős Vezető, illetve munkavégzéshez kiadott beépített adathordozót tartalmazó mobil eszköz vagy hordozható adattároló esetén a foglalkoztatott közvetlen felettese az eszközön tárolt adatok típusa és kockázatok mérlegelése alapján kezdeményezheti az adathordozó tartalmának törlését. Az Üzemeltetésért felelős feladata az adathordozó típusának megfelelő, helyreállíthatatlanságot biztosító törlési technikát (pl. többszörös felülírás, fizikai roncsolás, degaussing) alkalmazva gondoskodni az adathordozón tárolt adatok törléséről azok leselejtezése, megsemmisítése vagy újrafelhasználásra való kibocsátása előtt.

Amennyiben külső szolgáltatót vonnak be az adattörlésbe vagy eszközselejtezésbe, az Egyetemnek biztosítania kell, hogy a szolgáltató megfelelően tanúsított legyen, és a szerződésben rögzített legyen az adatok biztonságos kezelésére és megsemmisítésére vonatkozó kötelezettsége.

Az adattörlés és az eszközselejtezés minden lépését részletesen dokumentálni kell, beleértve az eszköz azonosítóját, az elvégzett adattörlési módszert, a dátumot és a jelenlévő személyeket. Ez biztosítja az elszámoltathatóságot és a megfelelőséget.

6. Kockázatkezelési eljárásrend

A kockázatkezelési eljárásrend célja a biztonsági fenyegetések és sérülékenységek felderítése, azok Egyetemre gyakorolt hatásának felmérése, valamint a kockázatok elfogadható szintre csökkentő, arányos védelmi intézkedések bevezetése. Ez a folyamat biztosítja az erőforrások hatékony felhasználását a legkritikusabb területeken.

Az Egyetem az alaptevékenysége végzéséhez használt EIR-ekkel, az azokban kezelt adatokkal és az EIR-ek által nyújtott vagy azokon keresztül elérhető szolgáltatásokkal összefüggő kiberbiztonsági kockázatok kezelésével kapcsolatban az alábbiakat határozza meg:

- Az Információbiztonság Szabályozásáért Felelős Vezető feladata és felelőssége gondoskodni a kockázatkezelés megszervezéséről és végrehajtásáról, valamint az ahhoz szükséges erőforrások rendelkezésre állásának biztosításáról.
- A biztonsági szerepköröket betöltő személyek kötelesek a kockázatkezelés teljes folyamatában — munka- és feladatkörüknek megfelelően — egymással együttműködni, a Kockázatkezelésért felelős vezető irányításával, valamint az Információbiztonsági Felelős (IBF) szakmai támogatásával az alábbi feladatok ellátásában:
    - Az Egyetem által használt EIR-ek beazonosítása, az EIR-ekben kezelt adatok és az adott EIR-nek az Egyetem működésében betöltött szerepe és funkciója alapján, a hatályos jogszabályi előírások szerinti hatáselemzési szempontok mentén végzett biztonsági osztályba sorolása, és ennek dokumentált rögzítése az EIR-ek nyilvántartásában.
    - Az EIR-eket érintő fenyegetettségek alapján a releváns kockázatok azonosítása, felmérése és értékelése, továbbá a felmerült, illetve feltárt kockázatok kezelésére vonatkozó, a kockázatokkal arányos védelmi intézkedési javaslatok kidolgozása és döntésre előterjesztése.
    - A jóváhagyott kockázatkezelési intézkedések dokumentált végrehajtása.
    - A végrehajtott kockázatkezelési intézkedések hatásosságának és eredményességének vizsgálata, az érintett EIR-ek biztonságára gyakorolt hatások és teljesítmények mérése, elemzése és értékelése, valamint a kockázatkezelési tevékenységek rendszeres felülvizsgálata. Az ezekkel kapcsolatos jelentések elkészítése és a vezetői döntések előkészítésében való közreműködés szintén e körbe tartozik.
- Az Információbiztonság Szabályozásáért Felelős Vezető dönt a javasolt kockázatkezelési válaszlépések végrehajtásának elrendeléséről, a végrehajtásukért felelős(ök) és határidő kijelölésével.
- A jóváhagyott kockázatkezelési intézkedések dokumentált végrehajtása az arra kijelölt felelős(ök) kötelessége, végrehajtásukat az IBF jogosult feladatellátása keretében ellenőrizni.
- A Szabályzat személyi hatálya alá tartozók munka- illetve feladatkörüknek megfelelő mértékben kötelesek a Szabályzat tartalmát, a benne foglalt előírásokat, különösen a számukra meghatározott feladatokat és felelősségeket megismerni, a kockázatkezelés teljes folyamatában egymással együttműködni.

6.1. Kockázatelemzés

A kockázatok azonosítása az információbiztonsági kockázatmenedzsment folyamatának első és alapvető lépése. Célja az Egyetem információvagyonát érintő potenciális fenyegetések, sérülékenységek és azok lehetséges hatásainak módszeres feltárása, különös tekintettel az elektronikus információs rendszerek (EIR-ek) működésére, szerepére és az általuk kezelt adatok biztonságára.

6.1.1. Azonosítási kör és alapelvek

A kockázat azonosításának ki kell terjednie az Egyetem valamennyi releváns információvagyonára (adatok, szoftverek, hardverek, hálózatok, szolgáltatások, személyzet, folyamatok, fizikai környezet), valamint az azokhoz kapcsolódó üzleti folyamatokra, kritikus funkciókra, és az intézmény alaptevékenységének folyamatosságát biztosító rendszerekre.

Fenyegetésnek minősül minden olyan potenciális esemény, veszély, gyenge pont, sérülékenység vagy védelmi intézkedést érintő hiányosság (pl. természeti katasztrófa, technikai meghibásodás, emberi hiba vagy szándékos támadás), amely károsíthatja az információvagyon bizalmasságát, sértetlenségét vagy rendelkezésre állását. Az azonosítást függetlenül attól el kell végezni, hogy az Egyetemnek az adott fenyegetettségre van-e érdemi befolyása vagy kockázatmérséklő hatása. Sérülékenységnek minősül az a gyengeség vagy hiányosság, amely egy fenyegetés bekövetkezését lehetővé teszi vagy annak következményeit súlyosbítja.

A kockázatok azonosítása során figyelembe kell venni, hogy az egyes EIR-ek által kezelt, tárolt adatok típusa és mennyisége jelentősen befolyásolja a fenyegetettség kihasználásának lehetséges következményeit. Emiatt az azonosítás során meg kell határozni, hogy a fenyegetettség bekövetkezése esetén az milyen adatokat érinthet és milyen mennyiségben.

Az Egyetem az általa használt EIR-ekkel kapcsolatban értelmezhető fenyegetéseket a jelen Szabályzat 1. számú melléklet Fenyegetések katalógusában felsorolt szempontrendszer alapján határozza meg. Amennyiben a működés körülményei, az EIR-ek jellemzői, a korábbi kockázatelemzések tapasztalatai vagy az új fenyegetések megjelenése miatt indokolt, az IBF, illetve az IBSZ-ben rögzített biztonsági szerepköröket betöltő további személyek jogosultak javaslatot tenni a fenyegetés katalógus kibővítésére vagy módosítására, amelyről az Információbiztonság Szabályozásáért Felelős Vezető dönt, s gondoskodik arról, hogy a jóváhagyott módosítások a Szabályzat felülvizsgálata alkalmával érvényesítésre kerüljenek.

6.1.2. Azonosítási módszerek és gyakoriság

A kockázatok azonosítása folyamatos feladat, amelyet évente legalább egyszer, valamint minden olyan esetben el kell végezni, amikor:

- új informatikai rendszer vagy szolgáltatás kerül bevezetésre;
- meglévő rendszerben jelentős technikai, szervezeti vagy funkcionális változás történik;
- új fenyegetés vagy sérülékenység válik ismertté;
- biztonsági esemény következik be.

Az azonosítás módszerei:

- szakértői interjúk és kérdőívek;
- workshopok és brainstormingok a felelősökkel;
- meglévő nemzeti vagy nemzetközi kockázati listák alkalmazása;

- a korábbi biztonsági események és incidensek naplóinak elemzése;
- automatizált sérülékenységvizsgálatok és auditjelentések értékelése;
- EIR-kataszter és hatáselemzések alapján végzett értékelés.

6.1.3. **Felelősségek**

Az Információbiztonsági Felelős (IBF) koordinálja a kockázatok azonosítási folyamatát.

Az egyes EIR-ekért felelős vezetők, adatgazdák és felhasználók aktívan közreműködnek a területüket érintő kockázatok azonosításában.

Minden foglalkoztatott köteles jelenteni az általa észlelt potenciális biztonsági kockázatokat vagy hiányosságokat közvetlen felettesének és az IBF-nek.

6.1.4. Dokumentálás:

Az azonosított kockázatokat (beleértve a fenyegetéseket, sérülékenységeket és az érintett eszközöket) a Kockázati Nyilvántartásban kell rögzíteni. A nyilvántartásban meg kell jelölni:

- a kockázat egyedi azonosítóját;
- a leírást (mi a kockázat, milyen körülmények között jelentkezhet);
- a fenyegetés és sérülékenység típusát;
- az érintett rendszert vagy területet;
- az észlelés dátumát;
- a felelős személy(eke)t;
- az esetleges előzményeket, megelőző intézkedéseket.

A nyilvántartás alapján az Egyetem értékelni tudja az információbiztonsági kockázatok alakulását, trendjeit, és megalapozott döntést hozhat a szükséges védelmi intézkedésekről.

6.2. Kockázatértékelési módszerek

A kockázatértékelés célja, hogy az azonosított információbiztonsági kockázatokat rendszerezett módon elemezze, azok hatását és bekövetkezési valószínűségét meghatározza, valamint ezek alapján kockázati szintet rendeljen hozzájuk. A kockázatértékelés alapján határozható meg, hogy mely kockázatok elfogadhatók, és melyek esetén szükséges védelmi intézkedések meghozatala.

6.2.1. Hatáselemzés

A fenyegetettség kihasználásának hatásait, az azonosított kockázatok bekövetkezése esetén a lehetséges következményeket és a várható kár mértékét az Egyetem az alábbi, háromszintű szempontrendszer szerint értékeli:

- 1 – Alacsony: csekély káresemény, melynek során,
  - a jogszabály által nem védett adat vagy legfeljebb kis mennyiségű személyes adat sérülhet;
  - az üzletmenetre gyakorolt hatása csekély;
  - a társadalmi/reputációs hatás belső szinten kezelhető;
  - a közvetlen és közvetett anyagi kár nem haladja meg az Egyetem éves költségvetésének 1%-át.
- 2 – Közepes: káresemény, melynek során,
  - nagy mennyiségű személyes, esetenként különleges adat sérülhet;

- személyi sérülések esélye megnőhet;
- érzékeny folyamatokat kezelő rendszer, információt képező adat sérülhet;
- az Egyetemmel szembeni bizalomvesztés kockázata fennáll, a jogszabályok betartása, vagy végrehajtása elmaradhat;
- a közvetlen és közvetett anyagi kár az Egyetem éves költségvetésének 1–10% közötti.

- 3 – Magas:
  - különleges személyes adat nagy mennyiségben sérülhet;
  - emberi életek kerülnek közvetlen veszélybe, személyi sérülések nagy számban következhetnek be;
  - nemzeti adatvagyon helyreállíthatatlanul megsérülhet;
  - kritikus folyamat/infrastruktúra kiesés;
  - súlyos társadalmi/reputációs hatás;
  - a közvetlen és közvetett anyagi kár meghaladja meg az Egyetem éves költségvetésének 10%-át.

6.2.2. **Bekövetkezési valószínűség megállapítása**

Az azonosított kockázatok bekövetkezési valószínűsége az iparági tapasztalatok, nyílt forrású statisztikák/trendek, korábbi incidensek és a feltárt sérülékenységek alapján, a támadási potenciált (szükséges eszköz/idő/szakértelem, védelem erőssége) figyelembe véve kerülnek becslésre.

A támadási potenciál a sikeres támadás esélyét fejezi ki és függ a támadási cél értékétől, a támadáshoz szükséges szakértelemtől, eszközöktől és időtől, valamint a védelem erősségétől is.

A bekövetkezési valószínűség lehetséges besorolási értékei ezek alapján az alábbiak lehetnek:

- 1 - Alacsony: bekövetkezhet, de nem valószínű.
- 2 - Közepes: előfordulhat a jövőben, érdemben számolni kell a bekövetkezéssel.
- 3 - Magas: várhatóan bekövetkezik a közeljövőben (széles körben ismert, könnyen kihasználható sérülékenység).

6.2.3. Kockázatértékelési mátrix

Az azonosított információbiztonsági kockázatok értékelése a lehetséges hatás és a bekövetkezés valószínűségének szorzataként meghatározott kockázati érték alapján történik. E módszer célja az információbiztonsági kockázatok objektív összehasonlíthatósága, valamint a kezelési prioritások meghatározása.

		Bekövetkezési valószínűség		
		1	2	3
Hatás	1	1	2	3
	2	2	4	6
	3	3	6	9

A kapott kockázati érték alapján a kockázatok négy kategóriába sorolhatók:

Kockázati érték	Kockázati kategória
1 – 2	alacsony szintű kockázat
3 – 5	közepes szintű kockázat
6 – 8	magas szintű kockázat
9	kritikus szintű kockázat

A kockázatértékelés eredményét az Egyetemi kockázatértékelési nyilvántartásban kell rögzíteni, a szükséges intézkedési javaslatokkal és felelősökkel együtt. A nyilvántartás kezelése az Információbiztonsági Felelős feladata.

6.3. Kockázatkezelés

A kockázatelemzés alapján a feltárt kockázatok kezelésének módját, a kockázat megszüntetésére vagy elfogadható szintre való csökkentésére irányuló válaszlépéseket a kockázat értéke, illetve az intézkedések alkalmazhatósága, megvalósításuk költsége és várható hatásai alapján kell meghatározni.

A Szervezetnél alkalmazott, lehetséges kockázatkezelési válaszlépések:

- kockázat elkerülése (pl. tevékenység megszüntetése),
- kockázat csökkentése (védelmi intézkedések),
- kockázat áthárítása, megosztása (biztosítás, kiszervezés),
- kockázat felvállalása (dokumentált döntés alapján).

6.3.1. Kockázat elkerülése

A kockázat elkerülésére irányuló válaszlépés célja a kockázat teljes megszüntetése a kockázatot kiváltó ok vagy tevékenység megszüntetésével (pl.: egy adott folyamat vagy tevékenység átszervezésével, helyettesítésével vagy megszüntetésével), amennyiben az hatékonyan, az Egyetem alaptevékenységének ellátását nem veszélyeztető módon kivitelezhető.

A kockázat elkerülése bármely szintű kockázati kategória besorolás esetén alkalmazható kockázatkezelési válaszlépés az Egyetemnél.

A kockázat elkerüléséről a kockázatkezelési javaslat alapján az Információbiztonság Szabályozásáért Felelős Vezető dönt.

6.3.2. A kockázat csökkentése

A kockázatcsökkentés célja, olyan védelmi intézkedések bevezetése, amelyekkel a kockázat megszüntethető, megelőzhető, vagy amelyek a kockázat bekövetkezésének valószínűségét, illetve annak hatását az elfogadható szintre mérséklik.

A javasolt kockázatcsökkentő védelmi intézkedés lehet már meglévő intézkedés módosítása vagy új kontroll, illetve intézkedés bevezetése (pl.: technikai kontrollok, szervezeti intézkedések, oktatási- képzési programok, redundancia, mentési és helyreállítási megoldások bevezetése)

A kockázat csökkentése során figyelembe kell venni az intézkedések költséghatékonyságát és megvalósíthatóságát.

A kockázat csökkentése bármely szintű kockázati kategória besorolás esetén alkalmazható és preferált kockázatkezelési válaszlépés az Egyetemnél.

A kockázat csökkentéséről a kockázatkezelési javaslat alapján az Információbiztonság Szabályozásáért Felelős Vezető dönt.

6.3.3. A kockázat áthárítása, megosztása

A kockázat áthárításának, megosztásának célja, hogy a lehetséges kár vagy felelősség egy részét vagy egészét egy külső fél viselje. Ez nem szünteti meg a kockázatot, de csökkenti az Egyetemre háruló következményeket (pl.: biztosítási szerződés, kötbér, SLA-k bevezetése, vagy szolgáltatói biztonsági feltételekkel).

Áthárítás akkor lehet indokolt, ha a kockázat technikailag nehezen csökkenthető vagy elkerülhető, illetve ezek költsége aránytalanul magas lenne. Ilyen esetekben a kockázat jogi és pénzügyi eszközökkel – például szerződéses felelősségvállalással, biztosítással vagy kötbérkikötéssel – részben vagy egészben külső félre hárítható, így az Egyetem közvetlen kitettsége mérsékelhető.

A kockázat áthárítása elvileg bármely kockázati kategória esetén alkalmazható, azonban nem megengedett olyan magas vagy kritikus kockázat esetében, amely az Egyetem alaptevékenységéhez nélkülözhetetlen EIR-t, kritikus infrastruktúrát vagy kulcsfontosságú erőforrást érint, és amelynek működése harmadik fél szolgáltatásaitól (pl. beszállítóktól, külső üzemeltetőktől) függ. Ilyen esetekben az Egyetem a kockázat áthárításának alkalmazását kizárja, s helyette a kockázat tényleges megszüntetését vagy mérséklését célzó válaszlépésként a kockázat csökkentését vagy elkerülését fogadja kizárólag el.

A kockázat elkerüléséről a kockázatkezelési javaslat alapján az Információbiztonság Szabályozásáért Felelős Vezető dönt.

6.3.4. Kockázat felvállalása

A Szervezet a kockázat tudatos elfogadását, felvállalását kizárólag abban az esetben alkalmazhatja, amennyiben a kockázat megfelel az alábbi elfogadási kritériumokban foglaltaknak:

- a megállapított kockázati kategória besorolás: alacsony vagy közepes;
- nem történik külső vagy belső normatíva (jogszabály, szabályzat) megsértése;
- a lehetséges károk mértéke az Egyetem számára elfogadható;
- a társadalmi-politikai hatás a Szervezeten belül kezelhető, nem sérül az egyetem jó hírneve, reputációja;
- a kockázat elkerülése vagy csökkentése nagyobb költséggel vagy erőforrás igénnyel jár, mint amekkora kár a bekövetkezésekor keletkezik vagy a helyreállításhoz szükséges;
- közvetve vagy közvetlenül testi épséget vagy emberi életet nem veszélyeztet.

Az alacsony szintű kockázati kategória besorolású kockázat indoklás nélkül felvállalható.

A közepes szintű kockázati besorolású kockázat elfogadása, felvállalása kizárólag részletes indoklással, az Információbiztonság Szabályozásáért Felelős Vezető dokumentált jóváhagyásával történhet meg.

Kritikus vagy magas kockázati kategória besorolású kockázat semmi esetben sem vállalható fel!

Fenti kritériumok alapján az Egyetem jelen Szabályzat tárgyában – az általa használt EIR-ek kockázataival kapcsolatban – megállapított kockázati tűréshatára a közepes kockázati szint besorolásnál került kijelölésre.

6.3.5. Kockázatkezelési javaslat és végrehajtás

A kockázatelemzés eredménye alapján a kockázatkezelési javaslat elkészítését az IBF a kockázatok kezelésére kijelölt biztonsági szerepköröket betöltő személyek közreműködésével végzi el. A javaslatnak tartalmaznia kell a kezelendő kockázatok leírását, a javasolt válaszintézkedéseket, azok indokoltságát, feladatokat, végrehajtásért felelősöket, határidőt, valamint a végrehajtás nyomon követésének módját. A kockázatkezelési javaslatot az Információbiztonság Szabályozásáért Felelős Vezető hagyja jóvá, aki rendelkezik a megfelelő erőforrásokról és jogosultságokról a javasolt intézkedések végrehajtásához.

Az intézkedések végrehajtásában köteles minden, a jelen Szabályzat személyi hatálya alá tartozó személy munka-, illetve feladatkörének megfelelő mértékben közreműködni.

A kockázatkezelési folyamat során biztosítani kell a megfelelő belső kommunikációt a szervezeten belül. A kommunikációnak ki kell terjednie az intézkedések céljára, a felelősökre, az elvárt eredményekre, valamint az érintett munkatársak tájékoztatására és képzésére is, különösen olyan esetekben, amikor új eljárásokat vagy technikai intézkedéseket vezetnek be.

Fentiek biztosítása céljából a kockázatkezelési jelentés megőrzéséről, valamint tartalmának a kockázatkezelésben érintettekkel történő megismertetéséről az Információbiztonság Szabályozásáért Felelős Vezető köteles gondoskodni.

6.3.6. Kockázatok nyomon követése és felülvizsgálat

A kockázatok kezelését követően szükséges azok rendszeres nyomon követése, értékelése és szükség esetén módosítása. A végrehajtott intézkedések hatékonyságát az IBF – indokolt esetben a további biztonsági szerepkört betöltő személy(ek) bevonásával – ellenőrzi, és szükség esetén további intézkedéseket javasolnak. A kockázatok felülvizsgálatát legalább évente egyszer, illetve minden olyan esetben el kell végezni, amikor jelentős változás történik az EIR-ekben, új fenyegetés válik ismertté, biztonsági esemény következik be, vagy új jogszabályi előírás lép hatályba. A felülvizsgálat eredményeiről szóló jelentést az Információbiztonsági Felelős készíti el, és azt továbbítja az Információbiztonság Szabályozásáért Felelős Vezető, felé.

Ezek az eljárások biztosítják, hogy az Egyetem képes reagálni a változó kockázati környezetre, és fenntartsa információbiztonsági szintjét az alaptevékenység zavartalan ellátása érdekében.

6.4. Rendszerbiztonsági terv

Az Egyetem a rendelkezésében lévő elektronikus információs rendszerek (EIR) esetében Rendszerbiztonsági Tervet (RBT) készít és tart karban. Az RBT célja az EIR teljes életciklusán keresztül történő biztonságos működtetésének biztosítása, a kockázatokkal arányos védelem megvalósítása érdekében.

A Rendszerbiztonsági tervnek meghatároznia és dokumentálnia kell az alábbiakat:

- az EIR alapfunkcióit és működési környezetét;
- az EIR biztonsági osztályba sorolását;
- a rendszer által kezelt adatok körét és bizalmassági szintjét;
- az EIR kapcsolatait más rendszerekkel, alkalmazásokkal;
- a konfigurációs és üzemeltetési beállításokat;

- az alkalmazandó biztonsági követelményeket és védelmi intézkedéseket;
- a felelős személyek és szervezeti egységek, különösen az adott EIR-hez rendelt Adatgazda és Alkalmazásgazda megnevezését.

Az RBT elkészítése és frissítése az EIR-hez rendelt Adatgazda és Alkalmazásgazda feladata, az IBF szakmai támogatásával.

Nem EIR-nek minősülő, de az Alkalmazásnyilvántartásban megjelölt alkalmazások esetében az Alkalmazásgazda és az Adatgazda rövid, alkalmazásbiztonsági adatlapot készít. Az adatlapnak legalább az alkalmazás célját, a kezelt adatköröket, a felhasználói szerepköröket és jogosultsági szinteket, a főbb biztonsági jellemzőket (pl. jelszókezelés, naplózás, autentikációs módok), valamint az IBSZ-től való esetleges eltéréseket és azok kompenzáló intézkedéseit kell tartalmaznia.

7. Üzemeltetési biztonsági intézkedések

Az Egyetem informatikai rendszereinek üzemeltetése során olyan eljárásokat kell alkalmazni, amelyek biztosítják a rendszerek megbízható, biztonságos és ellenőrizhető működését. Az üzemeltetési biztonsági intézkedések célja a hibák, sérülékenységek és jogosulatlan beavatkozások megelőzése, valamint a rendszerintegritás és rendelkezésre állás fenntartása.

7.1. Konfiguráció- és változáskezelés

Az Egyetem az általa használt elektronikus információs rendszerek (EIR) és rendszerelemeik konfigurációjának kezelésére vonatkozó szabályokat jelen Szabályzat keretei között rögzíti. A konfigurációk kezelésének célja a rendszerek biztonságos, megbízható és ellenőrizhető működésének fenntartása, valamint a jogosulatlan vagy nem dokumentált változtatások megakadályozása.

A konfiguráció kezelése általánosan az üzemeltetésért felelős feladata és felelőssége. Ettől eltérő esetben a feljogosított szerepkört és felelősségi szinteket az adott EIR rendszerbiztonsági tervében kell meghatározni.

Minden konfigurációs változtatást kötelező dokumentálni a vonatkozó rendszer-dokumentációban és nyilvántartásban. Az információbiztonsági felelős (IBF) évente legalább egy alkalommal köteles ellenőrizni a konfigurációkezelési szabályok betartását a biztonsági helyzetértékelés keretében, és annak eredményéről beszámolni az Információbiztonság Szabályozásáért Felelős Vezető részére.

7.1.1. Alapkonfiguráció

Az Egyetem az EIR-ek alapkonfigurációját és annak változásait a rendszerbiztonsági tervben dokumentálja és tartja karban. A rendszerbiztonsági terv tartalmazza a rendszer működéséhez szükséges minimális hardver- és szoftverkövetelményeket, a kompatibilitási elvárásokat, és a biztonsági beállításokat (pl. kikapcsolt nem használt szolgáltatások, portok, protokollok). Az alapkonfiguráció felülvizsgálata a rendszerbiztonsági tervben előírtak szerint történik. Központi üzemeltetésű vagy külső szolgáltatótól igénybe vett EIR-ek esetében a rendszer tulajdonosa határozza meg és dokumentálja a használathoz szükséges alapkonfigurációt, valamint a minimális hardver- és szoftverkövetelményeket.

7.1.2. Konfigurációs beállítások

Az Egyetem az EIR-ek rendszerelemeire vonatkozó egységes biztonsági konfigurációs beállításokat a legszűkebb funkcionalitás elve alapján határozza meg. A beállítások célja, hogy csak a működéshez szükséges funkciók, portok, protokollok és szolgáltatások legyenek engedélyezve, minden más – biztonsági szempontból kockázatos – funkciót le kell tiltani. A meghatározott konfigurációs beállítások végrehajtása az üzemeltetésért felelős feladata, az előírásoktól való eltérést dokumentálni kell.

7.1.3. Változáskezelés

Minden hardver-, szoftver- vagy hálózati konfigurációs módosítást előzetes hatásvizsgálatot követően, jóváhagyott változáskezelési folyamat részeként kell végrehajtani. A változtatásokat naplózni kell, szükség esetén visszaállítási tervet is készítve. A változáskezelési eljárás biztosítja, hogy a rendszer működését, biztonságát és rendelkezésre állását érintő változások nyomon követhetők és visszafordíthatók legyenek.

7.2. Naplózás és monitorozás

Az Egyetem számára kulcsfontosságú, hogy az általa használt elektronikus információs rendszerek (EIR) működésével és használatával összefüggő eseményekről, valamint az azokhoz való hozzáférésekről és az azokban történt változtatásokról olyan hiteles és ellenőrizhető információk álljanak rendelkezésre, amelyek lehetővé teszik az események utólagos visszakövetését, kivizsgálását, valamint szükség esetén a felelősség egyértelmű megállapítását.

A naplózással kapcsolatos követelmények célja a rendszerek átlátható és elszámoltatható működésének biztosítása, a biztonsági események időben történő felismerése, valamint a bizonyítékok megőrzése a vizsgálatok és auditok számára.

7.2.1. Naplózási követelmények

Az EIR-eknek és rendszerelemeiknek olyan naplózási képességekkel kell rendelkezniük, amelyek az alábbi eseménycsoportok rögzítését lehetővé teszik:

Rendszeresemények:

- indítás,
- leállás,
- hibák,
- szoftver telepítése/eltávolítása,
- konfiguráció módosítása.

Felhasználói hozzáférés:

- sikeres és sikertelen bejelentkezés,
- kijelentkezés,
- jelszóváltoztatás.

Felhasználói fiókműveletek:

- létrehozás,
- engedélyezés,
- módosítás,
- letiltás,
- törlés.

Hálózati forgalommal kapcsolatos események:

- megvalósult kapcsolat
- blokkolt kapcsolat.

Naplókezelés:

- naplózás elindítása/leállítása,
- naplóbeállítások módosítása,
- napló kiürítése, törlése,
- naplóvesztés lehetősége (pl. tárhelykapacitás kimerülése).

Új EIR vagy rendszerelem beszerzése, illetve bevezetése előtt kötelező annak naplózási képességeit előzetesen megvizsgálni. A vizsgálatot az Üzemeltetésért felelős végzi az érintett szerepkörökkel és az IBF bevonásával, az eredményeket pedig a Beszerzésekért felelős számára kell továbbítani, aki azokat a beszerzési dokumentációban követelményként rögzíti.

A már működő rendszerek esetében a naplózási képességek értékelése a rendszeres kockázatelemzés részeként történik. Az azonosított hiányosságokat az adott EIR rendszerbiztonsági tervében kell kockázatként rögzíteni és kezelni.

7.2.2. Naplóbejegyzések tartalma

Az események utólagos vizsgálatának és a felelősség egyértelmű megállapítása érdekében a naplóbejegyzéseknek minden esetben olyan részletességű információt kell tartalmazniuk, amely biztosítja a történések hiteles és pontos visszakövethetőségét. A naplóbejegyzések minimálisan elvárt tartalma:

- minden esemény esetében az esemény időpontja, típusa, keletkezésének helye (mely rendszerelem generálta), a kimenetel (sikeres vagy sikertelen), valamint – ha lehetséges – a műveletet kezdeményező vagy végrehajtó felhasználói vagy szolgáltatásfiók azonosítója;
- hibaeseményeknél a hibát kiváltó komponens vagy művelet megnevezése, valamint a hiba következményei;
- hálózati eseményeknél a forrás és cél azonosításához szükséges adatok (pl. IP-cím, port, protokoll);

A naplóbejegyzéseknek tartalmazniuk kell továbbá időbélyeget megbízható és egységes központi időforrás alapján, valamint biztosítani kell azok változtathatatlanságát és integritását, hogy utólagos módosításuk vagy törlésük kizárható legyen.

7.2.3. Naplóinformációk védelme és megőrzése

Az Egyetem az általa használt EIR-ek és rendszerelemek esetében – azok adattartalmát, funkcióját és kockázati szintjét figyelembe véve – határozza meg a naplóbejegyzések megőrzési időtartamát oly módon, hogy az biztosítsa a biztonsági események utólagos kivizsgálhatóságát és a felelősség egyértelmű megállapíthatóságát.

A naplóinformációk védelmének alapelvei:

- Hozzáférés-korlátozás: a naplóállományokhoz és naplózási beállításokhoz kizárólag az erre feljogosított, kiemelt jogosultsággal rendelkező személyek férhetnek hozzá, a legkisebb jogosultság elvének alkalmazásával.

- Integritásvédelem: a naplóbejegyzéseket védeni kell jogosulatlan módosítással, törléssel és manipulációval szemben. Ennek érdekében indokolt esetben kriptográfiai védelmet (pl. digitális aláírás, hash) kell alkalmazni.
- Biztonsági mentés: a naplóállományok mentéséről és az incidensek kivizsgálásához szükséges biztonságos visszaállíthatóságukról gondoskodni kell.
- Megőrzési idők: A naplók megőrzési idejét úgy kell meghatározni, hogy az biztosítsa a biztonsági események utólagos kivizsgálhatóságát. Az adott EIR-hez vagy alkalmazáshoz tartozó naplók megőrzési idejét az érintett EIR Rendszerbiztonsági Tervében, illetve az alkalmazásbiztonsági adatlapon kell meghatározni.
- Tárolási biztonság: a naplókat olyan tárolórendszeren kell elhelyezni, amely védett a fizikai és logikai hozzáférési kockázatokkal szemben (pl. központi naplószerver, redundáns tárolás).
- Időszinkronizáció: minden naplózott esemény időbélyegének hitelessége érdekében a rendszerek központi időforráshoz való szinkronizációja kötelező.

Az Egyetem az egyes EIR-ekhez kapcsolódó részletes naplózási követelményeket a Rendszerbiztonsági tervben, illetve központi szolgáltatások esetében az Rendszer üzemeltetési dokumentációban rögzíti.

7.2.4. Naplózás beállítása és üzemeltetése

Az Üzemeltetésért felelős, illetve a kijelölt Alkalmazásgazda feladata és felelőssége a naplózás beállításainak kialakítása, azok folyamatos felügyelete és a működés biztosítása a jelen Szabályzatban meghatározott általános követelmények, az érintett EIR Rendszerbiztonsági Tervében rögzített előírások, valamint olyan nem EIR-nek minősülő alkalmazások esetében, amelyekre alkalmazásbiztonsági adatlap készült, az abban foglaltak szerint. Egyéb nem EIR-nek minősülő alkalmazások esetében a naplózást az alkalmazásspecifikus üzemeltetési leírásokban vagy az Adatgazda által meghatározott követelmények szerint kell kialakítani.

Ide tartozik a naplózandó események körének meghatározása, a naplóbejegyzések tartalmának és megőrzési idejének biztosítása, továbbá a tárolókapacitás és a hozzáférési jogosultságok kezelése a legkisebb jogosultság elvének megfelelően.

A hiteles és időben visszakövethető naplózás érdekében minden rendszerórával rendelkező komponens esetében kötelező központi, megbízható időforrás konfigurálása. Az Üzemeltetésért felelős gondoskodik a naplózás infrastruktúra-szintű beállításainak és az időszinkronizálásnak a rendszeres ellenőrzéséről, a kapcsolódó hibák elhárításáról, valamint a naplózási folyamatok biztonságos és megszakítás nélküli működéséről.

Az egyes alkalmazásokon belüli naplózási funkciók megfelelő működésének, a naplózott eseménykör megfelelőségének és az esetleges alkalmazásspecifikus naplózási hibák jelzésének biztosítása az érintett alkalmazás Alkalmazásgazdájának feladata.

7.2.5. Monitorozás és elemzés

Az Üzemeltetésért felelős köteles az Egyetem központi informatikai infrastruktúrájához kapcsolódó naplóbejegyzések rendszeres vizsgálatát és elemzését elvégezni annak érdekében, hogy azonosíthatók legyenek a nem megfelelő vagy szokatlan működésre utaló jelek.

Az Alkalmazásgazda köteles az általa felügyelt EIR / alkalmazás naplóbejegyzéseinek rendszeres vizsgálatára és elemzésére, különös tekintettel a jogosulatlan hozzáférésre, szokatlan felhasználói aktivitásra, hibás vagy rendellenes működésre utaló eseményekre.

Amennyiben a naplóelemzés során biztonsági esemény gyanúja merül fel, az észlelő (Üzemeltetésért felelős vagy Alkalmazásgazda) köteles haladéktalanul értesíteni az Adatgazdát és az Információbiztonsági Felelőst. Ha a vizsgálat alapján megállapítható, hogy az esemény veszélyezteti vagy veszélyeztetheti az Egyetem által használt EIR-ekben vagy alkalmazásokban tárolt, továbbított vagy kezelt adatok, illetve szolgáltatások rendelkezésre állását, sértetlenségét vagy bizalmasságát, akkor a 1/2024. (11.01) rektori-kancellári közös utasítás – Informatikai Katasztrófaterv (Informatikai biztonsági incidensek kezelése) előírásai szerint kell eljárni.

7.2.6. Naplózás felülvizsgálat

Az Információbiztonsági Felelős (IBF) köteles a naplózással kapcsolatos beállítások rendszeres felülvizsgálatára. Ennek keretében ellenőrzi a naplózható és ténylegesen naplózott események körét, a naplóbejegyzések tartalmát, megőrzésük és védelmük szabályait, valamint a naplózás konfigurációját.

A felülvizsgálatok célja annak biztosítása, hogy a naplózási rendszer megfeleljen a jogszabályi, biztonsági és intézményi követelményeknek, valamint támogassa a biztonsági események utólagos vizsgálatát.

Szükség esetén az IBF javaslatot tehet további események naplózására, a naplózási szabályok, beállítások vagy a naplókezelési folyamatok módosítására, illetve megerősítésére.

7.3. Szoftverfrissítések, patch management

A szoftverekben és operációs rendszerekben felfedezett biztonsági rések (sebezhetőségek) a legsúlyosabb fenyegetések közé tartoznak. Az Egyetem kötelessége gondoskodni arról, hogy az általa használt rendszerek naprakész állapotban legyenek, és a gyártók által kiadott biztonsági frissítések és hibajavítások időben telepítésre kerüljenek.

7.3.1. A frissítések kezelésének alapelvei

- Rendszeres frissítés: Az összes használt operációs rendszert, szoftvert és firmware-t naprakészen kell tartani a gyártók által kiadott frissítések és hibajavítások (patchek) telepítésével.
- Fejlesztői támogatás: Kizárólag olyan szoftverek és rendszerelemek használata engedélyezett, amelyekhez a gyártó vagy fejlesztő biztosít biztonsági frissítéseket.
- Automatizálás: Ahol lehetséges, a frissítési folyamatokat automatizálni kell a gyors és hibamentes végrehajtás érdekében, minimalizálva az emberi mulasztás lehetőségét.
- Központi felügyelet: A frissítési folyamatok központi felügyeletét biztosítani kell, amely lehetővé teszi a patchelési státusz nyomon követését és az esetleges hibák gyors azonosítását.

7.3.2. Patch management eljárásrend

A szoftverfrissítési eljárás végrehajtásáért az Üzemeltetésért felelős a felelős. Az eljárás a következő lépéseket foglalja magában:

- Felmérés és kockázatértékelés: Az újonnan felfedezett sebezhetőségeket és az azokhoz kiadott frissítéseket folyamatosan monitorozni és értékelni kell. Különös figyelmet kell fordítani a kritikus vagy széles körben kihasználható sebezhetőségekre.
- Tesztelés: A kritikus frissítések telepítése előtt amennyiben lehetséges, azokat tesztkörnyezetben kell validálni, hogy a telepítésük ne okozzon működési zavarokat az éles rendszerekben.
- Végrehajtás: A frissítéseket az érintett rendszerek üzemeltetési sajátosságaihoz igazodva, ütemezett módon kell telepíteni. A gyártók által kiadott biztonsági frissítéseket a lehető legrövidebb időn belül, kiemelt prioritással kell alkalmazni.
- Naplózás és ellenőrzés: A frissítések telepítéséről naplót kell vezetni, aminek tartalmaznia kell a frissített alkalmazás nevét, a frissítés verziószámát, a telepítés időpontját és a frissítést végző személy nevét.
- Kivételek kezelése: Amennyiben egy frissítés telepítése nem lehetséges (pl. technikai inkompatibilitás miatt), az Üzemeltetésért felelős köteles a telepítés elmaradását írásban indokolni. Ebben az esetben a kockázatokat az Információbiztonság Szabályozásáért Felelős Vezetővel egyeztetve kell kezelni, aki dönt a kockázat felvállalásáról vagy az alternatív védelmi intézkedések bevezetéséről.

7.4. Karbantartás

Az Egyetem rendszereinek karbantartását csak előre ütemezett, dokumentált és ellenőrzött módon lehet elvégezni.

A karbantartási tevékenységekre az alábbi szabályok vonatkoznak:

- minden karbantartást dokumentálni kell, feltüntetve annak tárgyát, időpontját, végrehajtóját és eredményét;
- szolgáltatás-kieséssel járó karbantartást előzetesen ütemezni kell és az illetékes vezetővel és az Információbiztonság Szabályozásáért Felelős Vezetővel jóvá kell hagyatni;
- kritikus rendszerek karbantartását csak megfelelő biztonsági intézkedések mellett szabad végrehajtani;
- külső szolgáltató vagy karbantartó igénybevétele esetén biztosítani kell a hozzáférések korlátozását, a tevékenységek felügyeletét és titoktartási kötelezettség előírását;
- karbantartás után kötelező a rendszer működésének ellenőrzése, valamint szükség esetén a biztonsági mentésből történő helyreállítás tesztelése.

7.5. Vírusvédelem és végponti biztonság

A rosszindulatú szoftverek (pl. vírusok, zsarolóvírusok, kémprogramok) jelentik az Egyetem informatikai rendszereire és adataira nézve az egyik leggyakoribb és legsúlyosabb fenyegetést. A hatékony vírusvédelem és végponti biztonság alapvető követelmény a rendszerek integritásának, rendelkezésre állásának és bizalmasságának fenntartásához.

7.5.1. Alapelvek

- Kötelező védelem: Az Egyetem minden informatikai eszközén és végpontján (pl. munkaállomások, szerverek, laptopok, tabletek, telefonok) kötelező központilag telepített és felügyelt vírusvédelmi és végpontbiztonsági szoftvert működtetni. Ez a szoftver a beépített biztonsági beállításoknak megfelelően konfigurálva és folyamatosan aktívan kell, hogy fusson.

- Automatikus frissítés és ellenőrzés: A védelmi szoftvernek képesnek kell lennie a vírusdefiníciós adatbázisok és a programmotorok automatikus frissítésére, valamint rendszeres, időzített ellenőrzések végrehajtására.
- Valós idejű védelem: A végpontvédelmi megoldásnak valós időben kell ellenőriznie a külső forrásokból származó fájlokat (pl. letöltött, megnyitott, vagy e-mail mellékletként érkező állományokat), valamint a hálózati forgalmat a fenyegetések azonnali észlelése és blokkolása érdekében.
- Hordozható adathordozók ellenőrzése: Külső adathordozók (pl. USB-meghajtók, külső merevlemezek) csatlakoztatásakor a rendszernek automatikus vizsgálatot kell indítania.
- Felhasználói kötelezettség: A felhasználók nem tilthatják le vagy kerülhetik meg a végponti védelmet. A vírusvédelmi szoftver által megjelenített riasztást haladéktalanul jelenteniük kell az Üzemeltetésért felelősnek. Minden, a szabályzatba ütköző cselekedet fegyelmi felelősségre vonást vonhat maga után.

7.5.2. Eljárásrend és felelősségi körök

A vírusvédelem és a végponti biztonság működéséért és felügyeletéért az Üzemeltetésért felelős felel. Az eljárásrend a következőket foglalja magában:

- Védelmi szoftver kiválasztása: A megfelelő védelmi szoftver kiválasztása, konfigurálása és a szükséges licencek beszerzésének biztosítása az Üzemeltetésért felelős feladata. Az Információbiztonsági Felelős (IBF) jogosult felülvizsgálatot végezni és javaslatot tenni a megoldás lecserélésére, ha az nem biztosítja a megfelelő védelmet.
- Riasztások kezelése: A védelmi szoftver által generált riasztásokról a felhasználó köteles haladéktalanul értesíteni az Üzemeltetésért felelőst. Az Üzemeltetésért felelős feladata a riasztások kivizsgálása és a szükséges intézkedések megtétele és szükség esetén a 1/2024. (11.01) rektori-kancellári közös utasítás – Informatikai Katasztrófaterv előírásai szerint eljárni.
- Fertőzés kezelése és helyreállítás: Igazolt vírusfertőzés esetén az érintett eszközt azonnal le kell választani a hálózatról. Az Üzemeltetésért felelős köteles gondoskodni a fertőzés megszüntetéséről, a veszélyeztetett rendszerek ellenőrzéséről, valamint – szükség esetén – az adatok és konfigurációk biztonsági mentésből történő helyreállításáról.

7.6. Biztonsági mentések és helyreállítási követelmények

Az Egyetem az általa az alaptevékenysége végzéséhez használt, rendelkezésében lévő EIR-ek rendszeres biztonsági mentésével kapcsolatban az alábbi intézkedéseket határozza meg:

- A rendszeres biztonsági mentésekre vonatkozó információkat (mentendő adatok köre, mentési gyakoriság, megőrzési idő, tárolási helyszín, stb.) az adott EIR rendszerbiztonsági tervében rögzíti.
- A biztonsági mentéseknek ki kell terjednie az EIR felhasználói és rendszerszintű információira, valamint minden olyan adatra, amely a helyreállítási, illetve újraindítási feladatok maradéktalan teljesítéséhez szükséges.
- A biztonsági mentések konfigurálása és rendszeres végrehajtása a fentiek szerint dokumentált mentési rend alapján az Üzemeltetésért felelős feladata és felelőssége.
- Az eseti biztonsági mentések, valamint a helyreállítási, illetve tesztelési célú visszatöltések végrehajtásáról az Üzemeltetésért felelős köteles nyilvántartást vezetni.

- Amennyiben az Egyetem által használt EIR-eket, rendszerelemeiket érintő hiba vagy biztonsági esemény kezelése biztonsági mentésből történő helyreállítási tevékenységet igényel, annak végrehajtása az Üzemeltetésért felelős feladata és felelőssége.

A fentiekben rögzített intézkedések megfelelőségét és végrehajtását az IBF jogosult és köteles feladatellátása, illetve rendszeres biztonsági helyzetértékelése keretében ellenőrizni, s annak eredményéről az Információbiztonság Szabályozásáért Felelős Vezetőt indokolt esetben, illetve beszámolójában tájékoztatni.

7.7. Rendszer- és szolgáltatásbeszerzés

Az Egyetem által lefolytatott beszerzésekre vonatkozó általános szabályokat az Egyetem Beszerzési Szabályzata tartalmazza. Az Egyetem az általa használt, rendelkezésében lévő, illetve felügyelete alatt álló elektronikus információs rendszerek (EIR), alkalmazások és az ezeket kiszolgáló informatikai infrastruktúra-elemek beszerzése, fejlesztése és módosítása során a jelen Szabályzatban meghatározott speciális információbiztonsági előírásokat alkalmazza.

Az Egyetem köteles gondoskodni arról, hogy az alaptevékenysége végzéséhez használt EIR-ek és alkalmazások folyamatos és biztonságos működéséhez szükséges erőforrások rendelkezésre álljanak. Az informatikai rendszert, alkalmazást vagy szolgáltatást érintő beszerzési javaslatok előkészítése az érintett Adatgazda, az Alkalmazásgazda és az Üzemeltetésért felelős közös feladata, az Információbiztonsági Felelős (IBF) szakmai támogatásával.

A beszerzési igény és az ajánlatkérés során meg kell határozni a beszerzés tárgyára vonatkozó funkcionális, biztonsági és dokumentációs követelményeket, külső szolgáltatás (pl. felhőalapú vagy hosztolt megoldás) esetén a rendelkezésre állási és szolgáltatási szintmutatókat (SLA), valamint a támogatás és incidenskezelés feltételeit. Ezeket szerződéses kötelezettségként kell rögzíteni.

Az Információbiztonsági Felelős jogosult és köteles a biztonsági követelmények véleményezésére, javaslattételre és az információbiztonsági szempontú döntés előkészítésére. Az információbiztonsági szempontú jóváhagyásról az Információbiztonság Szabályozásáért Felelős Vezető dönt, míg a beszerzés lefolytatása és pénzügyi jóváhagyása az Egyetem Beszerzési Szabályzatában meghatározott hatáskörök szerint történik.

7.7.1. Fejlesztésre vonatkozó szabályok

Az új alkalmazások fejlesztése, valamint a meglévők továbbfejlesztése során alkalmazni kell az iparági bevált gyakorlatokat és a biztonságos kódolási irányelveket. A fejlesztési életciklus minden szakaszában (tervezés, kódolás, tesztelés, bevezetés) kötelező a biztonsági szempontok figyelembevétele és ellenőrzése.

A fejlesztési környezetet el kell különíteni az éles rendszerektől. Újonnan beszerzett rendszerelemeknek aktív gyártói támogatással kell rendelkezniük legalább két évig a bevezetést követően; támogatás nélküli vagy kivezetés előtt álló komponens nem szerezhető be.

Az IBF a fejlesztési folyamat során részt vesz a biztonsági követelmények meghatározásában és felülvizsgálatában, valamint ellenőrzi azok teljesítését a mérföldkövek során. Az Információbiztonság Szabályozásáért Felelős Vezető dönt a fejlesztés elfogadásáról, bevezetéséről, illetve szükség esetén javításáról.

8. Kommunikáció és hálózatbiztonság

Az Egyetem kiemelt feladata, hogy megvédje az elektronikus információs rendszereit (EIR) és a bennük kezelt adatokat a külső és belső fenyegetésektől. A kommunikáció- és hálózatbiztonsági szabályok és eljárások biztosítják a hálózati forgalom bizalmasságát, sértetlenségét és rendelkezésre állását.

Az Egyetem hálózatbiztonsági rendszerei és eljárásai a fenyegetések arányos, dokumentált és ellenőrizhető kezelésére épülnek, figyelembe véve az Egyetem információvagyonának értékét és a kockázati szinteket.

A hálózati biztonsági intézkedések kiterjednek többek között a tűzfalak, behatolás-megelőző rendszerek (IDS/IPS), hálózati szegmentáció, titkosított kommunikációs csatornák (VPN, TLS), valamint a naplózási és felügyeleti mechanizmusok alkalmazására.

Ennek megvalósításáért az Üzemeltetésért Felelős a felelős, a szabályok betartásának felügyeletét és felülvizsgálatát pedig az IBF végzi, aki évente köteles biztonsági helyzetértékelése keretében beszámolni az Információbiztonság Szabályozásáért Felelős Vezetőnek.

8.1. Szolgáltatásmegtagadással járó támadások (DDoS) elleni védelem

A szolgáltatásmegtagadással járó (DoS, DDoS) támadások megbéníthatják az informatikai rendszerek működését. Az Egyetem a kockázatkezelési tevékenységei során rendszeresen felméri az ilyen típusú támadások elleni védekezés megfelelőségét. Ennek keretében:

- a felhasználói tevékenységek korlátozásával, a kártékony kódok elleni védelmi intézkedésekkel és a szoftverhasználat szabályozásával biztosítani kell, hogy az Egyetem belső hálózatából ne lehessen külső rendszerek ellen szolgáltatásmegtagadásos támadásokat indítani;
- túlterheléses támadás gyanúja esetén az Üzemeltetésért felelős köteles a jelen szabályzat 10. Biztonsági események kezelése és az Informatikai Katasztrófaterv**ről** szóló, 1/2024 Rektori-Kancellári közös utasítás előírásai szerint eljárni.

8.2. Hálózati határvédelem

A belső hálózatok és a külső hálózatok (internet) közötti határ védelme elengedhetetlen a jogosulatlan hozzáférések és a fenyegetések elleni védelemhez.

- Tűzfal alkalmazása: Az Egyetem határvédelmi megoldásként tűzfalat alkalmaz a belső hálózati forgalom felügyeletére és irányítására. A tűzfalnak naplóznia kell a sikeres, engedélyezett, valamint a blokkolt forgalom adatait (forrás/cél cím, port, protokoll stb.), a 7.2 Naplózás és monitorozás pontban megfogalmazott elveknek megfelelően.
- Adminisztráció és hozzáférés: A határvédelmi eszközök adminisztrációja kizárólag a belső hálózatból, vagy biztonságos, titkosított kapcsolaton keresztül engedélyezett.
- Hálózati szegmentálás: A nyilvánosan hozzáférhető rendszereket (pl. webszerverek) el kell különíteni a belső hálózattól egy demilitarizált zónában (DMZ). A szegmentálás az Üzemeltetésért felelős feladata.

9. Üzletmenet-folytonosság

Az Egyetem az alaptevékenysége végzéséhez használt Elektronikus Információs Rendszerek (EIR-ek) rendelkezésre állásának, valamint az EIR-ekben tárolt, illetve kezelt adatok sértetlenségének és rendelkezésre állásának megőrzése érdekében az alábbi intézkedéseket teszi:

- Gondoskodik a működéséhez szükséges adatok, információk megfelelő és rendszeres biztonsági mentéséről, valamint a mentési adathordozók biztonságos tárolásáról.
- Biztosítja az informatikai eszközök rendszeres karbantartását, szükség szerinti javítását és a kieső informatikai erőforrások pótlását.
- Külső szolgáltató igénybevétele esetén a szolgáltatási szerződésben rögzíti a folytonossági és helyreállítási követelményeket.
- Gondoskodik az EIR-eket használó foglalkoztatottak szerepkörüknek megfelelő üzletmenet-folytonossági és vészhelyzeti felkészítéséről.

9.1. Informatikai Katasztrófa Vészhelyzeti Terv

Az üzletmenet-folytonossággal kapcsolatos eljárásrendet, ideértve a vészhelyzet elhárítására, a helyreállításra és a normál működéshez való visszatérésre vonatkozó részletes lépéseket, az Egyetem az Informatikai Katasztrófatervről szóló, 1/2024 Rektori-Kancellári közös utasításban rögzíti.

A Katasztrófaterv elkészítésének koordinálása, módszertani támogatása és szakmai tartalmának ellenőrzése az IBF feladata. A terv végrehajtásában érintett személyeket és felelősségi köröket a Katasztrófaterv határozza meg.

A Katasztrófatervben rögzített eljárások megismertetése és a Tervhez való hozzáférés biztosítása az Információbiztonság Szabályozásáért Felelős Vezető feladata.

10. Biztonsági események kezelése

Az Egyetem alapvető érdeke, hogy az alaptevékenysége végzéséhez használt EIR-eket, alkalmazásokat és az ezeket kiszolgáló informatikai infrastruktúrát érintő minden információbiztonsági eseményt a legrövidebb időn belül észleljen és felismerjen, s azokra a kockázat minimalizálása érdekében hatékony és gyors válaszintézkedésekkel tudjon reagálni.

10.1. Biztonsági események jelentése

Az Egyetem az általa használt EIR-eket, alkalmazásokat és informatikai infrastruktúra-elemeket érintő biztonsági események kivizsgálására, értékelésére és kezelésére vonatkozó részletes eljárásrendet az Informatikai Katasztrófat**ervről szóló, Rektori**-Kancellári közös utasításban rögzíti.

A jelen Szabályzat személyi hatálya alá tartozó foglalkoztatottak kötelesek az általuk használt EIR-ek, alkalmazások vagy informatikai szolgáltatások bármely rendellenes, zavart vagy hibás működését, hibajelzését, illetve bármely rendellenes eseményt annak észlelését követően közvetlen munkahelyi felettesük és az Üzemeltetésért felelős számára haladéktalanul jelezni. A jelzés az eseményt észlelő személy kötelessége.

Az Üzemeltetésért felelős a jelzés formájától függetlenül köteles gondoskodni a bejelentés adatainak dokumentált rögzítéséről.

Biztonsági esemény gyanújának felmerülése esetén az Üzemeltetésért felelős köteles értesíteni az érintett Alkalmazásgazdát, az érintett adatkör Adatgazdáját, az Információbiztonság Szabályozásáért Felelős Vezetőt és az Információbiztonsági Felelőst (IBF). Ha a vizsgálat alapján megállapítható, hogy az esemény veszélyezteti vagy veszélyeztetheti az Egyetem által használt EIR-ekben vagy alkalmazásokban tárolt, továbbított vagy kezelt adatok, illetve szolgáltatások rendelkezésre állását, sértetlenségét vagy bizalmasságát, akkor a 1/2024. (11.01.) rektori–kancellári közös utasítás – Informatikai Katasztrófaterv (Informatikai biztonsági incidensek kezelése) előírásai szerint kell eljárni.

10.2. Biztonsági események kivizsgálása, értékelése és kezelése

Az informatikai incidensek biztonsági eseménnyé minősítésére vonatkozó javaslatot az IBF terjeszti elő az Információbiztonság Szabályozásáért Felelős Vezető részére az eset összes körülményéről rendelkezésre álló információk kiértékelése alapján.

Kivizsgálás és együttműködés: A biztonsági esemény értékeléséhez, kivizsgálásához és bejelentéséhez szükséges információk (pl. naplóbejegyzések) begyűjtésében az Üzemeltetésért felelős köteles közreműködni.

Intézkedések: Az IBF a kivizsgálást követően javaslatot tesz az Információbiztonság Szabályozásáért Felelős Vezető számára az esemény kezelési módjára, a szükséges intézkedések végrehajtásában pedig minden érintett köteles együttműködni.

Az informatikai erőforrások kiesésével járó, az üzletmenet-folytonosságot veszélyeztető esemény bekövetkezése esetén az **Informatikai Katasztrófatervről szó**ló, 1/2024 Rektori-Kancellári közös utasításban meghatározott eljárásrend az irányadó.

Az IBF a bejelentési kötelezettség körébe tartozó biztonsági eseményt jelenti a vonatkozó, hatályos jogszabályi előírásokban meghatározott eseménykezelő szerv, illetve felügyeleti hatóság felé.

A biztonsági esemény kezelésének lezárását követően az IBF jogosult a hasonló események jövőbeni előfordulási kockázatának csökkentése érdekében indokolt új védelmi intézkedések bevezetésére javaslatot tenni.

11. Személyi biztonság

Az Egyetem elemi érdeke, hogy az általa használt elektronikus információs rendszerekhez (EIR), az azokban kezelt adatokhoz, az EIR-ek rendszerelemeihez és szolgáltatásaihoz hozzáférő foglalkoztatottak, valamint az Egyetemmel munkavégzésre irányuló jogviszonyban álló személyek feladataikat biztonságosan, szakszerűen és felelősséggel, a vonatkozó szabályoknak és kötelezettségeiknek tudatában végezzék. Az Egyetem célja, hogy a személyi biztonsággal összefüggő követelmények jogi és szervezeti garanciái biztosítottak legyenek.

E cél érdekében az Egyetem a személyi biztonsággal kapcsolatos szabályokat jelen Szabályzat keretei között az alábbiak szerint határozza meg.

11.1. Személybiztonsági feltételek

A munkaköri alkalmasságra vonatkozó jogszabályi előírásoknak megfelelően biztosítani kell, hogy az adott munkakör betöltéséhez szükséges iskolai végzettség, szakképzettség, gyakorlat, valamint – indokolt esetben – az egészségi és pszichikai alkalmasság ellenőrzésre kerüljön.

Az EIR-ekhez hozzáféréssel rendelkező személyek kötelesek:

- a munkaköri alkalmassági követelményeknek megfelelni,
- a biztonsági előírásokat és eljárásrendeket megismerni és betartani,
- titoktartási nyilatkozatot aláírni.

Külső partnerek és szerződéses jogviszonyban álló személyek esetében a garanciális feltételeket a vonatkozó szerződéseknek kell rögzíteni. Az IBF jogosult a szerződések információbiztonsági szempontból történő véleményezésére, szükség esetén további biztonsági feltételek javaslatára.

11.2. Kiemelt kockázatú munkakörök

Az engedélyezési és döntési folyamatokban, valamint az EIR-ekhez és az azokban kezelt adatokhoz magasabb hozzáféréssel rendelkező személyek (pl. rendszergazdák, adatgazdák, alkalmazásgazdák) munkakörei információbiztonsági szempontból kiemelt kockázatúak.

Az Egyetem ezen munkakörökhöz kapcsolódó kockázatokat rendszeresen értékeli a kockázatkezelési eljárásrend keretében. A Humánerőforrás menedzsmentért felelős köteles gondoskodni arról, hogy ezen személyek tartós távolléte vagy akadályoztatása esetén megfelelő helyettesítés biztosított legyen.

11.3. **Eljárás a jogviszony megszűnésekor**

Az EIR-ekhez hozzáférő munkavállalók jogviszonyának megszűnésekor munkahelyi felettesük köteles:

- kezdeményezni minden kiadott fizikai és logikai jogosultság azonnali visszavonását,
- gondoskodni az Egyetem tulajdonát képező eszközök (kulcsok, belépőkártyák, hitelesítési eszközök, informatikai eszközök stb.) dokumentált visszavételéről,
- kezdeményezni a kilépő felhasználói fiókjainak letiltását, erőforrásaihoz való hozzáférések megszüntetését, adatállományainak szükség szerinti archiválását vagy törlését,
- a kilépés során átadás-átvételi eljárást lefolytatni a feladatok és felelősségek folyamatos ellátásának biztosítása érdekében,
- a kilépő munkatársat tájékoztatni a jogviszony megszűnése után is fennálló kötelezettségeiről (pl. titoktartás).

11.4. Áthelyezések, átirányítások és kirendelések kezelése

Amennyiben a munkavállaló munkaköre vagy feladatai megváltoznak, a korábbi hozzáféréseit és jogosultságait felül kell vizsgálni, a szükségtelen jogosultságokat meg kell szüntetni, és az új munkakör által igényelt jogosultságokat be kell állítani.

Biztosítani kell, hogy:

- a munkavégzéshez szükséges eszközök rendelkezésre álljanak,
- a megfelelő hozzáférések beállításra kerüljenek,
- a szükséges ismeretek a munkavállaló számára átadásra kerüljenek.

11.5. Fegyelmi intézkedések

A biztonsági szabályok megsértése – a jogsértés súlyosságától függően – írásbeli figyelmeztetéstől a fegyelmi eljárásig terjedő intézkedést vonhat maga után. Szándékos, súlyos vagy ismétlődő szabálysértés esetén az Egyetem fegyelmi eljárást indíthat, súlyos esetben büntetőfeljelentést tehet.

Külső partnerek és szerződéses jogviszonyban álló személyek szabálysértése esetén a vonatkozó szerződésekben rögzített jogkövetkezményeket kell alkalmazni.

Az IBF köteles támogatást nyújtani az esetek dokumentálásához, az Üzemeltetésért felelős pedig közreműködik az evidenciák rögzítésében. A fegyelmi intézkedések során figyelembe kell venni a 10. Biztonsági események kezelése pont előírásait.

11.6. Tudatosság és képzés

Az Egyetem kiemelt fontosságúnak tartja az információbiztonsági tudatosság folyamatos erősítését, mivel a biztonságos működés egyik alapvető előfeltétele a felhasználók megfelelő felkészültsége. A folyamatosan változó kibervédelemmel kapcsolatos ismeretek, a biztonságtudatos gondolkodás és munkavégzés kialakítása, valamint fenntartása érdekében a szervezet gondoskodik a foglalkoztatottak rendszeres képzéséről és tájékoztatásáról.

11.6.1. Tudatosság és képzési eljárásrend

- Belépéskor: Az Egyetem a belépési folyamat részeként gondoskodik arról, hogy az új munkavállalók, hallgatók és – amennyiben releváns – külső partnerek számára a jelen Szabályzat elérhető legyen, és felhívja a figyelmet annak megismerésére. E körben a Szabályzat 1.4 pontjában rögzített általános megismerési kötelezettség, valamint – ahol ezt a munkakör vagy feladat indokolja – a külön nyilatkozat megtételének rendje irányadó.
- Rendszeres képzés: Az Egyetem a foglalkoztatottak számára rendszeres időközönként, lehetőség szerint legalább évente információbiztonsági tudatosságnövelő oktatást vagy e-learning képzést biztosít. A képzések gyakoriságát és formáját az egyes szervezeti egységek és felhasználói csoportok sajátosságaihoz igazodva kell meghatározni. Hallgatók esetében az Egyetem elsősorban tájékoztató anyagokkal, alkalmi kampányokkal (pl. tanulmányi rendszerben vagy e-learning felületen megjelenő üzenetekkel) támogatja az információbiztonsági tudatosságot.
- Célzott képzés: Az Egyetem törekszik arra, hogy a kiemelt jogosultsággal rendelkező felhasználók (pl. rendszergazdák) feladataikhoz igazodó, speciális információbiztonsági képzésben részesüljenek.
- Tájékoztatás: Az aktuális fenyegetésekről, kockázatokról és jelentősebb biztonsági eseményekről az Információbiztonsági Felelős – szükség szerint és lehetőség szerint rendszeres jelleggel – tájékoztatja a felhasználókat (pl. hírlevél, belső portál, tájékoztató kampányok útján).
- Felhasználói felelősség: A felhasználóktól elvárt, hogy az előírt információbiztonsági képzéseken részt vegyenek, és az ott megszerzett ismereteket a napi munkavégzés

során alkalmazzák. A felhasználók kötelesek a tudomásukra jutó rendellenes működést, külső vagy belső fenyegetés gyanúját, illetve a biztonsági eseményeket mielőbb jelezni a vonatkozó eljárásrend szerint.

- Nyilvántartás: A képzéseken és tájékoztatókon való részvételről az Egyetem nyilvántartást vezet (pl. jelenléti ív, e-learning rendszer jelentése). A nyilvántartás elsősorban a felülvizsgálatok és auditok támogatását szolgálja.

A tudatosság és képzés eljárásrend célja, hogy a felhasználók felismerjék az információbiztonsági fenyegetéseket, képesek legyenek megfelelően reagálni a biztonsági eseményekre, és ezáltal hozzájáruljanak az Egyetem informatikai rendszereinek védelméhez.

12. Záró rendelkezések

Jelen Szabályzatot a Tokaj- Hegyalja Egyetem Szenátusa a 26/2025-2026. (12. 10.) sz. határozatával fogadta el.

Rendelkezéseit 2026. év január hó 1. napjától kell alkalmazni.

A Szabályzat az Egyetem honlapján megtalálható.

Sárospatak, 2025. december 10.

Prof. Dr. Kéri Szabolcs
rektor

Tokaj-Hegyalja Egyetem 1. Sárospatak

Vincze Csaba
kancellár

1. számú melléklet – Fenyegetések katalógusa

A 7/2024. (VI. 24.) MK rendelet 3. számú melléklete alapján.

	A	B
1.	Fenyegetés	Érintett információbiztonsági alapelvek
2.	Tűz	R
3.	Kedvezőtlen környezeti feltételek	S, R
4.	Víz	S, R
5.	Szennyeződés, por, korrózió	S, R
6.	Természeti katasztrófák	R
7.	Katasztrófák a környezetben	R
8.	Jelentős környezeti események	B, S, R
9.	Áramellátás megszakadása, vagy hibája	S, R
10.	Kommunikációs hálózatok megszakadása, vagy zavara	S, R
11.	Beszállítói láncok megszakadása, vagy zavara	R
12.	Külső szolgáltatók hibája, vagy működési zavara	B, S, R
13.	Elektromágneses interferencia	S, R
14.	Kompromittáló elektromágneses kisugárzás	B
15.	Kémkedés	B
16.	Lehallgatás	B
17.	Eszközök, adathordozók, dokumentumok eltulajdonítása	B, R
18.	Eszközök, adathordozók, dokumentumok elvesztése	B, R
19.	Rossz tervezés vagy az alkalmazkodás hiánya	B, S, R
20.	Védett információ nyilvánosságra kerülése	B
21.	Nem megbízható forrásból származó információk	B, S, R
22.	Hardver vagy szoftver hamisítása (manipulációja)	B, S, R
23.	Információmanipuláció	S
24.	Elektronikus információs rendszerbe történő illetéktelen belépés	B, S
25.	Eszközök vagy adathordozók megsemmisülése	R
26.	Eszközök vagy az elektronikus információs rendszer működésének megszakadása	R
27.	Eszközök vagy az elektronikus információs rendszer hibás működése	B, S, R

28.	Erőforrások hiánya	R
29.	Szoftverek sérülékenységei vagy hibái	B, S, R
30.	Jogszabályok vagy szerződések megszegése	B, S, R
31.	Eszközök vagy az elektronikus információs rendszer engedély nélküli kezelése vagy használata	B, S, R
32.	Eszközök vagy az elektronikus információs rendszer hibás kezelése vagy használata	B, S, R
33.	Engedélyekkel való visszaélés	B, S, R
34.	Személyi állomány elvesztése	R
35.	Támadás	B, S, R
36.	Kényszerítés, zsarolás vagy korrupció	B, S, R
37.	Eltulajdonított személyazonossággal történő visszaélés	B, S, R
38.	Cselekmények letagadása	B, S
39.	Személyes adatokkal történő visszaélés	B
40.	Rosszindulatú szoftverek (malware)	B, S, R
41.	Szolgáltatásmegtagadással járó támadás (DOS)	R
42.	Szabotázs	R
43.	Pszichológiai manipuláció (social engineering)	B, S
44.	Manipulált hálózati adatforgalom	B, S
45.	Helyiségekbe történő engedély nélküli behatolás	B, S, R
46.	Adatvesztés	R
47.	Védendő információk sértetlenségének elvesztése	S
48.	Kártékony mellékhatások	B, S, R

Alkalmazási útmutató

A táblázat „A” oszlopa a fenyegetések megnevezését tartalmazza.

A táblázat „B” oszlopa az adott fenyegetések által potenciálisan érintett információbiztonsági alapelvek betűjeleit tartalmazza, az alábbiak szerint:

- Bizalmasság: B
- Sértetlenség: S
- Rendelkezésre állás: R