2-Szab/3-1/2025

HUN-REN Wigner Fizikai Kutatóközpont

1121 Budapest,
Konkoly-Thege Miklós út 29-33.
1525 Budapest, Pf. 49
Tel.: +36 1 392 2512
Fax: +36 1 392 2598
E-mail: wigner@wigner.hun-ren.hu
Web: wigner.hun-ren.hu

Informatikai biztonsági szabályzat

Hatályba lépés napja:

2025-12-15

Jóváhagyom:

Dr. Lévai Péter József, főigazgató

HUN-REN Wigner Fizikai Kutatóközpont
Főigazgató

Tartalomjegyzék

1. Bevezető

1.1. Az IBSZ célja

Az Informatikai Biztonsági Szabályzat (a továbbiakban: IBSZ) elsődleges célja a HUN-REN Wigner Fizikai Kutatóközpont (a továbbiakban: Kutatóközpont) információs kockázati tényezőinek kezelése az alábbi területeken:

- A Kutatóközpont működéséhez fontos információk bizalmasságának, sértetlenségének, rendelkezésre állásának folyamatos biztosítása.
- A Kutatóközpont számára jelentős információs eszközök és szolgáltatások rendeltetésszerű és jogszerű használatának, megfelelő üzemvitelének biztosítása, üzembiztonságának védelme.
- A személyiségi jogok védelme, adatvédelmi, és egyéb jogszabályi megfelelőség biztosítása.

Az IBSZ a fenti célokat úgy kívánja elérni, hogy a Kutatóközpont által működtetett vagy igénybe vett informatikai rendszerekre vonatkozóan a biztonsági intézkedéseket szabályozza, meghatározza a számítástechnikai eszközök beszerzésének és használatának, a szoftverfejlesztés és alkalmazás, az adatkezelés folyamatának biztonsági szabályait, továbbá az informatikai szerepköröket, és előírja az egyes szereplők informatikai biztonságot érintő feladatait.

1.2. Az IBSZ hatálya

Az IBSZ tárgyi hatálya kiterjed:

- mindazon, a Kutatóközpont által folytatott tevékenységre, folyamatra, eljárásra, hatályos szabályozásra, utasításra, döntésre, amelyek a Kutatóközpont informatikai szempontú biztonságos működését közvetlenül vagy közvetetten érintik, illetve befolyásolják,
- a Kutatóközpont által birtokolt vagy érdekében létrehozott, illetve kezelt kutatási eredményekre, a szellemi tulajdonra, az üzleti-, a személyes- vagy az egyéb okból érzékeny, védendő információkra (a továbbiakban: Információs Adatvagyon vagy röviden Adatvagyon),
- az Információs Adatvagyon elemeit kezelő, illetve tároló információs eszközvagyonra, különösen az informatikai és telekommunikációs eszközökre, munkaállomásokra, kiszolgálókra, adattárolókra, mobil eszközökre (a továbbiakban: Információs Eszközök vagy röviden Eszközök),
- az Információs Eszközök által nyújtott információs szolgáltatásokra (a továbbiakban: Információs Szolgáltatások vagy röviden Szolgáltatások).

Az IBSZ tárgyi hatálya alá tartozó Információs Adatvagyont, Eszközöket és Szolgáltatásokat a továbbiakban együttesen a Kutatóközponti Információs Infrastruktúrának vagy röviden Infrastruktúrának nevezzük.

Az IBSZ személyi hatálya kiterjed:

- az IBSZ tárgyi hatálya alá tartozó Eszközöket vagy Szolgáltatásokat igénybe vevő, vagy üzemeltető természetes, illetve jogi személyekre (a továbbiakban együttesen: Felhasználók).

Az IBSZ ismerete és betartása a hatálya alá tartozó minden Felhasználó számára kötelező. Az IBSZ aktuális változata a Kutatóközpont weboldalán, a közérdekű adatok között kerül közzétételre.

Az IBSZ ismeretét, az abban foglaltak elfogadását minden természetes személynek igazolnia kell, ennek hiányában nem jogosult az IBSZ tárgyi hatálya alá tartozó adatokhoz, eszközökhöz vagy szolgáltatásokhoz való hozzáférésre.

A jogi személyek esetében azokkal úgy köthető az IBSZ tárgyi hatálya alá tartozó Kutatóközponti Információs Infrastruktúrához való hozzáférésre, annak üzemeltetésére vonatkozó szerződés, hogy abban a jogi személy elfogadja a hatályos IBSZ szabályait. Amennyiben a jelenleg érvényes szerződés nem tartalmazza ezt a feltételt, a jogi személlyel szerződésmódosítást kell végrehajtani.

Az IBSZ alkalmazása során az elsődleges cél az informatikai biztonsági kockázatok, hibák, problémák feltárása és azok javítása. A Kutatóközpont információs biztonsága közös érdekünk.

Az IBSZ előírásait kirívóan súlyosan sértő, vagy ismétlődő módon szándékos, vagy súlyos gondatlan magatartás esetén az ezért felelős természetes személlyel szemben az főigazgató eljárást indíthat, jogi személlyel a szerződés felbontását kezdeményezheti.

Kapcsolódó szabályzások

Az IBSZ előírásai összhangban vannak:

- az MKH Informatikai Biztonsági Keretszabályzatával,
- a Kutatóközpont Szervezeti és Működési Szabályzatával,
- a Kutatóközpont beszerzésekre vonatkozó szabályzataival,
- az KIFÜ IKT Felhasználói Szabályzatával (korábbi NIIF AUP, https://kifu.gov.hu/wp-content/uploads/2022/07/KIFU_NIIF_Program_Felhasznaloi_Szabalyzat_v2.pdf).

2. A Kutatóközpont Információs Rendszere

2.1. A Kutatóközpont Információs Infrastruktúrája

A Kutatóközpont Információs Infrastruktúráját a következő csoportokba soroljuk.

2.1.1. Központi Információs Infrastruktúra

A Kutatóközpont alaptevékenységének ellátására és az összes Felhasználó munkavégzésének támogatására központi információs infrastruktúrát tart fenn.

A Központi Információs Infrastruktúra elemei különösen:

- A passzív számítógépes hálózati kábelezés, a labor, az irodai és egyéb célú helyiségekben elhelyezett fali csatlakozókkal bezárólag.
- Az aktív hálózati elemek (pl. routerek, switchek, vezeték nélküli elérési pontok).
- A Kutatóközpont felhasználói nyilvántartási rendszere és az arra épülő azonosítási és föderatív szolgáltatások.
- A wigner.hu és wigner.hun-ren.hu, valamint minden jogelőd intézményhez, továbbá projekthez létrehozott domain nevekhez kapcsolódó elektronikus levelezési szolgáltatások, postafiókok, levelezési listák és az ezek elérését szolgáló kiegészítő szolgáltatások.
- A wigner.hu és wigner.hun-ren.hu, valamint minden jogelőd intézményhez, továbbá projekthez létrehozott nyilvános weblapok, valamint az ezekhez kapcsolódó nyilvános és zárt felhasználású társ-weboldalak.
- A Kutatóközpont központi kiszolgáló cluster és szerverparkja.
- A felsorolt elemek működését támogató Információs Eszközök és Szolgáltatások.

A Központi Információs Infrastruktúra üzemeltetését a Számítógép Hálózati központ (SzHK) végzi.

2.1.2. Információs Részinfrastruktúrák

A Központi Információs Infrastruktúra elemeitől elkülönülő részinfrastruktúrák (a továbbiakban: Információs Részinfrastruktúrák) elemei például:

- A Gazdasági Igazgatóság, valamint a titkárságok személyzetének munkaállomásai, nyilvántartásai és az ezeket kizárólagosan kiszolgáló eszközök.
- Az Adatközpont személyzetének munkaállomásai, nyilvántartásai és az ezeket kizárólagosan kiszolgáló eszközök.
- Az egyes osztályok, kutatócsoportok, projektek által saját belső célra üzemeltetett kiszolgálók, zárt hálózatot üzemeltető hálózati eszközök vagy egyéb Információs Szolgáltatások.

Információs részinfrastruktúra csak az Informatikai Biztonsági Felelős tájékoztatása mellett létesíthető.

2.1.3. Információs Személyi Infrastruktúra elemek

A Munkatársak személyi számítógépei és mobil eszközei (munkaálllomásai).

2.2. A Kutatóközpont Informatikai Szervezete

2.2.1. Felhasználói csoportok és szerepkörök

Az IBSZ a Felhasználókat az alábbi elkülönült szervezeti csoportokba osztja.

Egy Felhasználó egy időben csak az alábbi szervezeti csoportok egyikébe tartozhat.

Kutatóközponti Munkatárs

A Kutatóközponttal munkaviszonyban álló Felhasználó.

Partner Munkatárs

Adott projekthez, kutatási feladathoz tartozó, annak végrehajtásában szerepet játszó partner kutató vagy szakértő (ide tartoznak a megbízással, az önkéntesként foglalkoztatottak, valamint a gyakornokok is).

Egyetemista

Adott projekthez, kutatási feladathoz tartozó, abban részt vevő, az anyaintézményénél aktív BsC, MsC vagy Phd jogviszonnyal rendelkező egyetemi hallgató.

Nyugdíjas

A kutatóközpont felhasználói nyilvántartásában szereplő, nyugdíjba vonult volt kutatóközponti munkatárs.

Vendég Felhasználó

Vendég Felhasználóknak tekintendők a fenti szerepkörök egyikébe sem sorolható, a társintézményi, intézményközi, föderatív szolgáltatások Felhasználói.

2.2.2. Kiemelt szerepkörök

Az IBSZ a tárgyi hatálya alá tartozó eszközök kezelésében játszott szerepük szerint az alábbi kiemelt felhasználói szerepköröket határozza meg. Kiemelt szerepkört alapesetben csak Kutatóközponti Munkatárs tölthet be. Nem Kutatóközponti Munkatárs csak az Informatikai Biztonsági Felelős (IBF) hozzájárulásával tölthet be kiemelt szerepkört.

Rendszergazda

Minden Információs Eszközhöz és Szolgáltatáshoz legalább egy kijelölt és egy kijelölt helyettes Rendszergazda tartozik.

A Rendszergazda feladata és felelőssége az általa felügyelt infrastruktúra-elemek szolgáltatási céljaiknak megfelelő üzemeltetése, valamint információbiztonságuk folyamatos biztosítása: a Rendszergazda felel az adott szolgáltatást biztosító informatikai rendszer üzemeltetéséért, operációs rendszereinek és szoftvereinek naprakészen tartásáért, frissítéséért.

Az Információs Személyi Infrastruktúra elemek esetében általában az eszközt használó Felhasználó tölti be a Rendszergazda szerepet. Információs Személyi Infrastruktúra elemeken alapszabályként Szolgáltatás nem nyújtható. Ez alól kivételt az IBF engedélyezhet.

Alkalmazásgazda

Minden Információs Szolgáltatáshoz legalább egy kijelölt Alkalmazásgazda tartozik.

Az Alkalmazásgazda feladata az általa felügyelt szolgáltatás szakmai funkcióinak, illetve ezek átalakításának, konfigurációjának felügyelete, kiemelten a hozzáférési jogosultságok, illetve az alkalmazás által támogatott folyamatok szabályozása.

Az Alkalmazásgazda felelőssége az általa felügyelt szolgáltatások információbiztonságának adminisztratív eszközökkel történő, folyamatos biztosítása: az Alkalmazásgazda felel az alkalmazást megvalósító szoftver komponensek beállításaiért, konfigurációjáért.

A Rendszergazdát és az Alkalmazásgazdát együttesen Eszközgazdának nevezzük.

Adatgazda

Minden Információs Adatvagyon elemhez legalább egy kijelölt Adatgazda tartozik.

Az Adatgazda feladata az általa felügyelt adatok tekintetében az érvényes adatkezelési szabályok szerinti adatkezelés biztosítása, a hozzáférés adminisztratív szabályozása, illetve az adatokra vonatkozó biztonsági és védelmi elvárások meghatározása.

Az Adatgazda felelőssége az általa felügyelt adatok információbiztonságának, adminisztratív eszközökkel történő, folyamatos biztosítása.

Informatikai Biztonsági Felelős (IBF)

Az Informatikai Biztonsági Felelős alapvető feladatai és felelőssége:

- az IBSZ előírásainak meghatározása, ezek karbantartása, szükség szerinti, de legalább kétévenkénti felülvizsgálata,
- folyamatos kockázatelemzés, továbbá kockázatarányos védekezési stratégia és intézkedési terv megvalósítása az IBSZ hatálya alá tartozó információs elemek és folyamatok védelme tekintetében,
- az IBSZ által meghatározott intézkedések és folyamatok ellenőrzése, hatékonyságának folyamatos javítása,
- az IBSZ előírásaitól való szükségszerű ideiglenes eltérések vagy tartós kivételek dokumentált engedélyezése,
- annak ellenőrzése és a szükséges intézkedések meghozatala, hogy a Központi Információs Infrastruktúra az IBSZ előírásainak folyamatosan megfeleljen,
- az informatikai katasztrófa elhárítási terv és üzemfolytonossági terv bevezetése, karbantartása,

- a Kutatóközpontot érintő Biztonsági Incidensek kezelése, a tájékoztatási kötelezettségek betartása,
- a felelősségi körében a főigazgató számára közvetlenül adhat jelentést, tájékoztatást.

Informatikai Felelős

A Központi Informatikai Infrastruktúrához, valamint minden Informatikai Részinfrastruktúrához legalább egy kijelölt és egy helyettes Informatikai Felelős tartozik.

Az Informatikai Felelős feladata az adott Informatikai Infrastruktúrához rendelt Felhasználók, Rendszergazdák és Adatgazdák támogatása, koordinációja, oktatása és képviselete az IBF felé.

Az Informatikai Felelős felelőssége:

- annak biztosítása, hogy a Felhasználók, Rendszergazdák és Adatgazdák ismerjék az IBSZ előírásait,
- annak biztosítása, hogy az egységhez tartozó Információs Részinfrastruktúrák az IBSZ előírásainak folyamatosan megfeleljenek,
- az egységhez tartozó Információs Részinfrastruktúrákkal összefüggő Biztonsági Incidensek kezelése, az IBF bevonásával,
- az IBF munkájának elősegítése, a kért intézkedések megtétele, és a kért tájékoztatások haladéktalan megadása.

Munkaügyi Felelős

A Munkaügyi Felelős feladata a Kutatóközponti Munkatársak státuszának és annak változásainak rögzítése, amelyre a munkatársak azonosító rekordjainak aktiválási és passziválási munkafolyamatai épülnek.

A Munkaügyi Felelős felelőssége, hogy Kutatóközponti Munkatárs státusszal csak a Kutatóközponttal munkaviszonyban álló természetes személyek rendelkezzenek.

Egységvezető

Az Egységvezetők az IBSZ értelmezésében az SZMSZ szerinti szervezeti egységek vezetői.

Az Egységvezetők feladata az egységükhöz tartozó Informatikai Felelősök, Adatgazdák és Rendszergazdák kijelölése.

Az Egységvezető elsődleges felelősséggel tartozik a szervezeti egységéhez tartozó Információs Adatvagyon, Eszközök és Szolgáltatások IBSZ szerinti megfelelőségéért.

Főigazgató

A főigazgató általános felelősséggel tartozik a Kutatóközponthoz tartozó Információs Adatvagyon, Eszközök és Szolgáltatások IBSZ és jogszabály szerinti megfelelőségéért. Az főigazgató feladata az IBF kijelölése.

2.2.3. Külső szereplők

Információbiztonsági Auditor

A Kutatóközponttól független, releváns szakértői minősítéssel (pl.: ISO 27000, CISA) rendelkező szakember. Feladata az IBSZ előírásainak és ezek megvalósulásának időszakos, független felülvizsgálata, az IBSZ tárgyi hatálya alá tartozó eszközök, szolgáltatások és folyamatok információs kockázatainak elemzése, audit jelentés készítése. Az audit előkészítésébe, az audit jelentés értékelésébe és elfogadásába, valamint az esetleges intézkedési terv elfogadásába a Kutatóközpont belső ellenőrzési vezetőjét be kell vonni.

2.3. Informatikai kockázatkezelés

2.3.1. Informatikai biztonsági osztályok, besorolás

Az egyes információs rendszerekre vonatkozó informatikai kockázat értékelése során fontos tényező ezek biztonsági besorolása. Az IBSZ a kockázatkezelési folyamat támogatására az alábbi biztonsági osztályokat határozza meg.

Adatvédelem szempontjából:

Kritikus rendszerek

A Kutatóközpont működése szempontjából kritikus, az intézmény egészére kiterjedő rendszerek, amelyek érzékeny, illetve személyes adatokat tartalmaznak. Információbiztonsági és adatvédelmi szempontból egyaránt kiemelt védelmet igényelnek.

- Központosított illetményszámfejtési rendszer (KIRA, üzemeltető: Magyar Államkincstár)
- Államháztartási Számviteli Adatszolgáltatások (KGR-K11, üzemeltető: Magyar Államkincstár)
- Integrált Pénzügyi, Számviteli, Eszköz- és Készletgazdálkodási Rendszer (CT-EcoSTAT - üzemeltető: CompuTREND Zrt.)
- Központi Projektnyilvántartó Rendszer (KöPeNY - CT-EcoSTAT, üzemeltető: CompuTREND Zrt. és HUN-REN MKH)
- Fejezeti és Intézményi Adatok Tára (FIAT - CT-EcoSTAT - üzemeltető: CompuTREND Zrt. és HUN-REN MKH)
- Központi levelező kiszolgálók (Kutatóközponti e-mail)
- Intézményi központi azonosítási és jogosultságkezelési rendszer (PITS) és az arra épülő további azonosítási rendszerek
- A Wigner Ügyintéző Rendszer (WÜR, üzemeltető: Wigner FK)
- Wigner Iratkezelő Rendszer (DMS One Ultimate, üzemeltető: DMSOne Zrt. és Wigner FK)

- A felsorolt rendszereket közvetlenül kiszolgáló központi hardveres, virtualizációs és operációs komponensek, valamint az ezek működését lehetővé tevő hálózati elemek és szolgáltatások

Kiemelt rendszerek

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

- Telekommunikációs hálózat
- Technológiai (environment, middleware) rendszerek
- Kommunikációs rendszerek
- Központi tárhely-kiszolgálók (mycloud, mydrive)
- Központi forráskód repozitórium (gitlab)
- Központi konferenciakezelő rendszer (indico)
- Az Internet felé elérhető szolgáltatást nyújtó rendszerek

Normál rendszerek

Az előző kategóriákba nem sorolt, a teljes kutatóközpont napi működése szempontjából nem kritikus, illetőleg csak egyes részeire kiterjedő rendszerek.

- Labor berendezések
- Kutatói rendszerek
- Az egyes egységek kiszolgáló szerverei
- Általános célú munkaállomások
- Könyvtári rendszerek

Üzemfolytonosság szempontjából:

Kritikus rendszerek

A Kutatóközpont működése szempontjából kritikus, az intézmény egészére kiterjedő rendszerek, amelyek érzékeny, illetve személyes adatokat tartalmaznak. Információbiztonsági és adatvédelmi szempontból egyaránt kiemelt védelmet igényelnek.

- Központosított illetményszámfejtési rendszer (KIRA, üzemeltető: Magyar Államkincstár)
- Államháztartási Számviteli Adatszolgáltatások (KGR-K11, üzemeltető: Magyar Államkincstár)
- Integrált Pénzügyi, Számviteli, Eszköz- és Készletgazdálkodási Rendszer (CT-EcoSTAT - üzemeltető: CompuTREND Zrt.)
- Központi Projektnyilvántartó Rendszer (KöPeNY - CT-EcoSTAT, üzemeltető: CompuTREND Zrt. és HUN-REN MKH)

- Fejezeti és Intézményi Adatok Tára (FIAT - CT-EcoSTAT - üzemeltető: CompuTREND Zrt. és HUN-REN MKH)
- Központi levelező kiszolgálók (Kutatóközponti e-mail)
- Intézményi központi azonosítási és jogosultságkezelési rendszer (PITS) és az arra épülő további azonosítási rendszerek
- A Wigner Ügyintéző Rendszer (WÜR, üzemeltető: Wigner FK)
- Wigner Iratkezelő Rendszer (DMS One Ultimate, üzemeltető: DMSOne Zrt. és Wigner FK)
- A felsorolt rendszereket közvetlenül kiszolgáló központi hardveres, virtualizációs és operációs komponensek, valamint az ezek működését lehetővé tevő hálózati elemek és szolgáltatások

Kiemelt rendszerek

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

- Telekommunikációs hálózat
- Technológiai (environment, middleware) rendszerek
- Kommunikációs rendszerek
- Központi tárhely-kiszolgálók (mycloud, mydrive)
- Központi forráskód repozitórium (gitlab)
- Központi konferenciakezelő rendszer (indico)
- Az Internet felé elérhető szolgáltatást nyújtó rendszerek

Normál rendszerek

Az előző kategóriákba nem sorolt, a teljes kutatóközpont napi működése szempontjából nem kritikus, illetőleg csak egyes részeire kiterjedő rendszerek.

- Labor berendezések
- Kutatói rendszerek
- Az egyes ek kiszolgáló szerverei
- Általános célú munkaállomások
- Könyvtári rendszerek

2.3.2. A kockázatkezelés módszere

A Kutatóközpont a működése során jelentkező informatikai kockázatok arányos kezelésére törekszik. Ennek érdekében az IBF rendszeresen kockázatértékelést végez, melynek során meghatározza az adatvédelem és az üzemfolytonosság szempontjából az egyes rendszereket érintő fenyegetettségek által okozott potenciális kár névleges mértékét, valamint a lehetséges káresemények bekövetkezési valószínűségét.

Az így előállt, az egyes rendszerekre értelmezett kockázati besorolását az IBSZ alábbi táblázat szerint határozza meg:

	kis valószínűség (évente <1 esemény)	közepes valószínűség (évente <5 esemény)	nagy valószínűség (évente >5 esemény)
kis kár (<500e Ft)	alacsony kockázat	közepes kockázat	kiemelt kockázat
közepes kár (<5M Ft)	közepes kockázat	kiemelt kockázat	kritikus kockázat
jelentős kár (>5M Ft)	kiemelt kockázat	kritikus kockázat	kritikus kockázat

Az IBF az előállt kockázati besorolások alapján az egyes rendszerekhez azok biztonsági besorolása alapján a működésükben érintett döntéshozók bevonásával intézkedési tervet készít. A tervnek a feltárt kockázatokat a Kutatóközpont számára elfogadható mértékben csökkentő intézkedéseket kell tartalmaznia legalább az alábbiak szerint:

- Kritikus rendszerek esetén: közepes és afölötti kockázati szintű eseményekre
- Kiemelt rendszerek esetén: kiemelt és afölötti kockázati szintű eseményekre
- Normál rendszerek esetén: kritikus kockázati szintű eseményekre

2.3.3. Biztonsági Események és Incidensek kezelése, Üzemfolytonosság (BCP), Katasztrófahelyzetek kezelése (DRP)

A Kutatóközponti Információs Infrastruktúra elemeinek működésében, környezetében, folyamataiban vagy működtető személyzetének cselekedeteiben bekövetkező, a normál, vagy elvárható viselkedéstől eltérő, megfigyelhető változásokat, amennyiben ezek információbiztonsági vetülete is azonosítható, Biztonsági Eseménynek nevezzük.

A személyes adatot érintő Biztonsági Eseményről (Adatvédelmi Incidens) az Adatvédelmi Tisztviselőt (DPO) haladéktalanul értesíteni kell.[1]

A Biztonsági Események alapvető típusai (súlyossági besorolásai):

- Normál Biztonsági Esemény - az alábbi feltételek **mindegyike** teljesül:
  - nem érint Kiemelt vagy Kritikus rendszert;
  - nem érint személyes adatot;
  - nem igényel olyan beavatkozást, melynek konfigurációkezelési vonzata van;
  - nem igényel eljárásbeli vagy szabályzati módosítást;
- Kiemelt Biztonsági Esemény – az alábbi feltételek **bármelyike** teljesül

[1] Az adatvédelmi incidens a GDPR 4. cikk 12. pontja értelmében a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését (rendelkezésre állás sérülése), megváltoztatását (integritás sérülése), jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést (bizalmas jelleg sérülése) eredményezi.

    - Kiemelt vagy Kritikus rendszert érint;
    - személyes adatot érint;
    - konfigurációkezelési vonzattal járó beavatkozást igényel;
    - eljárásbeli vagy szabályzati módosítást igényel.
- Kritikus Biztonsági Esemény – az alábbi feltételek **bármelyike** teljesül:
    - személyek biztonságát vagy egészségét befolyásolhatja;
    - kritikus rendszerek működését akadályozhatja;
    - bizonyos rendszerek teljesítményét oly mértékben befolyásolhatja, hogy azok biztonsági funkciói kárt szenvedhetnek;
    - egyéb, az üzemvitelt érintő okból kritikusnak minősül.

Biztonsági Incidens minden Kiemelt, vagy Kritikus súlyosságú Biztonsági Esemény.

Minden Felhasználó köteles a Biztonsági Incidensek jelzésére az IBF felé. Az IBF a továbbított Biztonsági Incidenseket, illetve kezelésük folyamatát rögzíti, azokról nyilvántartást vezet.

Az IBF jogosult a Biztonsági Incidensek esetén a tevékenység azonnali megakadályozására, az ilyen tevékenységgel érintett erőforrások felhasználásának részleges vagy teljes korlátozására vagy ezen intézkedések elrendelésére.

A Kritikus Biztonsági Események megelőzésére, illetve az ezek bekövetkezése során bekövetkező károk minimalizálására, a normál üzemmenet helyreállítására az IBF az Informatikai Felelősök és Rendszergazdák közreműködésével az érintett infrastruktúra elemek tekintetében üzemmenet folytonossági tervet (BCP) és katasztrófa helyreállítási tervet (DRP) készíttet. Az IBF gondoskodik az elkészült tervek folyamatos karbantartásáról, oktatásáról, teszteléséről, illetve szükség esetén végrehajtásáról.

3. Szabályozási elemek

3.1. Általános szabályok

A Kutatóközpont Információs Infrastruktúrájának elsődleges célja, rendeltetése és feladata a Kutatóközpontban folyó magas színvonalú kutató- és fejlesztő munka támogatása.

Az Infrastruktúra rendeltetésszerű működését akadályozni, biztonságát veszélyeztetni tilos.

Az Infrastruktúra magáncélra történő felhasználása (például: magáncélú e-mail használat) – jogszerű célokra és a Kutatóközpont belső szabályzataiban foglaltak, így különösen a jelen szabályzatban foglalt biztonsági előírások betartása mellett - megengedett. A magáncélú használat szabályai különösen a következőek:

- A magáncélú használat nem jog, hanem egy lehetőség, amelyet a Felhasználó Adatgazdája, Egységvezetője, az IBF, a Főigazgató megtilthatnak.
- A magáncélú használat mértéke nem mehet az elsődleges célok rovására. A magáncélú használat nem veszélyeztetheti az infrastruktúra rendeltetését, a Kutatóközpont feladatainak ellátását.
- A Felhasználó felelőssége, hogy ha él a lehetőséggel, akkor a magán célú adatait a kutatóközponti eszközökön egyértelműen elkülöníti az elsődleges célok adataitól.
- A Felhasználók tudomásul veszik, hogy az üzemfolytonosság biztosítása vagy az incidenskezelés során, illetve az Infrastruktúra Felhasználók általi használatának egyéb ellenőrzése érdekében a Rendszergazdák, az Informatikai Felelősök, illetve az IBF két tanú jelenlétében, az Adatvédelmi Tisztviselő értesítése mellett a Felhasználó által a Kutatóközponttal fennálló jogviszony teljesítéséhez használt számítástechnikai eszközökön tárolt, a jogviszonnyal összefüggő adatokba betekinthet. Ezen ellenőrzési jogosultság szempontjából munkaviszonnyal összefüggő adatnak minősül bármely és minden olyan adat, ami ahhoz szükséges, hogy az eljáró személyek meg tudják állapítani azt, hogy a vizsgált adatok a munkaviszonnyal összefüggenek-e. Amennyiben megállapítást nyer, hogy az adat magánjellegű, az abba történő betekintést az eljáró személy nem folytathatja. A fentiek irányadók arra az esetre is, ha a felek megállapodása alapján a Felhasználó a Kutatóközponttal fennálló jogviszonya teljesítése érdekében saját számítástechnikai eszközt használ.
- A Felhasználók tudomásul veszik, hogy amennyiben megszűnik Kutatóközponttal fennálló jogviszonyuk vagy az Infrastruktúra használatára való jogosultságuk, Felhasználó által a Kutatóközponttal fennálló jogviszony teljesítéséhez használt számítástechnikai eszközökön tárolt, a jogviszonnyal összefüggő adatokba keletkezett adatokat a Kutatóközpont az üzemfolytonosság biztosítása érdekében megőrzi. Ezért a Felhasználók felelőssége, hogy az Infrastruktúra használatára való jogosultságuk megszűnése előtt a magánjellegű adataikat a kutatóközponti eszközökről eltávolítják.

A Kutatóközpontban kizárólag jogtiszta szoftverek használhatók.

Az IBSZ tárgyi hatálya alá eső tevékenységek esetén - úgy mint informatikai fejlesztések, beszerzések, érintett szabályozások, folyamatok változtatása, adatkezelés stb. - az Informatikai Biztonsági Felelőst, vagy az általa delegált személyt véleményezési jogkörrel felruházva már a tevékenység elejétől kezdve be kell vonni.

3.2. Fizikai eszközökre vonatkozó szabályok

3.2.1. Irodai eszközök üzemeltetése

A felügyelet nélkül hagyott, kiemelt vagy kritikus biztonsági besorolású munkaállomásokat elhagyásuk esetén manuálisan, illetve 10 perces határidővel

automatikusan is zárolni kell. A zárolás feloldásához az IBSZ előírásainak megfelelő, erős jelszót vagy biometriai azonosítást kell alkalmazni.

3.2.2. Géptermek használati szabályai

Folyamatosan üzemelő szerver számítógépek - beleértve a virtuális szerver szolgáltatásokat is - csak az erre a célra kijelölt Kutatóközponti géptermekben vagy laborokban (a továbbiakban gépterem) üzemeltethetők.

A géptermekbe csak az arra jogosultak léphetnek be. Belépési jogosultságot a gépterem üzemeltetők és a főigazgató adhatnak.

A gépterembe belépni csak a gépterem üzemeltetőknél, aláírás ellenében átvett kulccsal, és/vagy belépésre jogosító belépőkártyával lehet. A kiosztott kulcsokról, belépőkártyákról a géptermet üzemeltetőknek nyilvántartást kell vezetniük.

A gépteremben tilos enni, inni, tüzet okozó tevékenységet folytatni, vagy kiemelten tűzveszélyes anyagokat (pl.: papír csomagolás) tárolni.

3.2.3. Fizikai adattárolók külső használatára vonatkozó szabályok

A Kutatóközpont Információs Adatvagyonának részét képező fontos adatokat tároló eszközök (adattárolók) a Kutatóközpont őrzött telephelyein kívüli szállítása vagy egyéb célú használata során különös gondossággal kell eljárni annak érdekében, hogy az ezeken tárolt adatok bizalmassága ne sérülhessen.

Ennek érdekében az ilyen adatok, illetve adattárolók vonatkozásában az alábbi védelmi intézkedéseket kell alkalmazni:

- Az adatokat és adattárolókat az IBSZ előírásainak megfelelő, erős jelszóval, illetve erős (legalább: SHA-1, AES256 vagy ezekkel egyenértékű) titkosítással kell védeni.
- Adattárolót szállítás vagy használat során nem szabad őrizetlenül hagyni.
- A fontos adatokat csak a szükséges legrövidebb ideig szabad a Kutatóközpont telephelyein kívül eső adattárolón tárolni.
- Az adattárolók jelszaváról a főigazgatói titkárságon biztonsági másolatot kell leadni a Felhasználónak, amelyet ott zárt, biztonságos helyen kell tárolni:
  - Az adattároló jelszavát zárt borítékban kell elhelyezni. A borítékon fel kell tüntetni a Felhasználó nevét, a lezárás időpontját, a Felhasználó aláírását. A borítékot felbontani csak jegyzőkönyvvel szabad. A felbontás tényéről a Felhasználót haladéktalanul tájékoztatni kell. A felbontást követően a felbontónak a borítékot újra le kell zárnia. A borítékon a fentieken kívül rögzíteni kell a felbontó nevét, a felbontás időpontját és a felbontó aláírását.
  - A boríték külsején fel kell tüntetni az adattároló egyértelmű azonosítóját.

3.2.4. Fizikai adattárolók használatára vonatkozó egyéb szabályok

A Kutatóközpont Információs Adatvagyonának részét képező, fontos adatokat tároló eszközök esetén:

- Selejtezés vagy egyéb célú újrahasznosítás esetén az adatokat az adattárolóról visszaállíthatatlan módon törölni kell, vagy amennyiben ez nem lehetséges, akkor az adattárolót fizikailag meg kell semmisíteni.
- A fontos adatokról rendszeres időközönként biztonsági másolatot kell készíteni. A biztonsági másolatot jogosulatlan fizikai hozzáféréstől és káros környezeti hatásoktól védett helyen kell tárolni.

3.2.5. Eszközbeszerzés, -karbantartás és -szállítás

A Kutatóközponti infrastruktúra bővítése során csak az IBSZ előírásainak megfelelni képes hardver és szoftver eszközöket szabad beszerezni.

Az információs eszközöket folyamatos rendelkezésre állásuk és sértetlenségük biztosítása érdekében előírásszerűen karban kell tartani.

A Kutatóközponti Hálózatra csatlakozó aktív vagy passzív hálózati eszközök beszerzéséhez a Központi Információs Infrastruktúra üzemeltetők engedélye szükséges. Kivételt képeznek ez alól a WiFi hálózatra csatlakozó mobil eszközök, valamint a standard Ethernet hálózati csatlakozóval kapcsolódó szerver számítógépek és személyes munkaállomások (PC-k).

3.3. Jogosultságkezelési szabályok

3.3.1. A jogosultságkezelés általános szabályai

Az Információs Szolgáltatásokat igénybe vevő Felhasználókat, a nyilvános szolgáltatások kivételével, minden esetben azonosítani kell.

A Kutatóközponti Infrastruktúra csak a szükséges legkisebb mértékben, illetve (a nyilvános szolgáltatások kivételével) csak az indokoltan szükséges legkisebb felhasználói kör számára nyújthat szolgáltatásokat.

A Kutatóközpontban kezelt, az Információs Infrastruktúra elemeihez hozzáférést lehetővé tevő felhasználói adatok tekintetében minden esetben Adatgazdát kell kijelölni. Az így kijelölt Adatgazda (vagy megbízottjának) felelőssége:

- A felhasználói adatok célhoz kötött rögzítése és aktiválása az engedélyezett hozzáférési időszak kezdetével
- Az adatkezelésre vonatkozó eljárásrend és műszaki környezet megfelelőségének biztosítása
- A felhasználói adatok törlése vagy inaktiválása az engedélyezett hozzáférési időszak lejártával.

Az azonosított Felhasználók egy adott Információs Infrastruktúra elemre vonatkozó hozzáférésének mértékét (azaz jogosultságainak körét) az adott elemhez, illetve Felhasználóhoz rendelt Informatikai Felelősök és Adatgazdák együttesen határozzák meg.

A rendszerek és folyamatok kialakítása során törekedni kell arra, hogy a jogosultságok igénylése és jóváhagyása követhető legyen. A felhasználói jogosultságokat javasolt rendszeres időközönként felülvizsgálni, és a már nem aktuális jogosultságokat lezárni.

3.3.2. Jelszókezelés

A Felhasználók azonosítása során erős jelszavak használata kötelező. Az IBSZ szerint erős jelszó jellemzői:

- alapesetben legalább 12 karakter, kiemelt jogosultsági szint esetén legalább 16 karakter hosszúságú,
- nem tartalmaz felhasználói azonosítót, számsorozatot, és egyéb, könnyen kikövetkeztethető személyes adatot.

A jelszavak kezelésére vonatkozó szabályok:

- A Felhasználók azonosítóinak, jelszavainak átruházása, illetéktelen felhasználása tilos.
- Felhasználói jelszavakat jogosulatlan személy számára hozzáférhető módon tárolni tilos.
- A kezdetben generált jelszót az első bejelentkezés alkalmával kötelezően meg kell változtatni.
- A Felhasznló felelőssége, hogy az azonosításhoz erős jelszót állítson be.
- A mindenkori Kutatóközponti jelszó más, Kutatóközponton kívüli rendszerek esetén nem használható.
- A jelszónak minden felhasználó számára bármikor, saját maga által megváltoztathatónak kell lennie.

3.3.3. Kutatóközponti Munkatársak azonosítása

A Kutatóközpont számára nyújtott, felhasználói azonosítást igénylő webes szolgáltatások esetén lehetőség szerint a Kutatóközponti felhasználói nyilvántartásra épülő központi azonosítási (Wigner IdP) szolgáltatást kell felhasználni. Egyéb esetekben, lehetőség szerint a Kutatóközpont számára nyújtott, felhasználói azonosítást igénylő szolgáltatások esetén közvetlenül a Kutatóközponti felhasználói rendszer (PITS) azonosítási szolgáltatását kell használni.

Kutatóközponti Munkatársak hozzáférése az Információs Infrastruktúra elemeihez csak a Kutatóközpont és az adott személy között fennálló munkaviszony időtartamában engedélyezett.

A felsorolt központi azonosítási módok esetén a felhasználói adatok vonatkozásában a Munkaügyi Felelős gyakorolja az Adatgazda szerepkört. Amennyiben a fent felsorolt központi azonosítási módok nem alkalmazhatók, akkor a felhasználói adatok vonatkozásában az adott szolgáltatás vagy eszköz üzemeltetéséért felelős Egységvezető gyakorolja az Adatgazda szerepkört.

3.3.4. Partner Munkatársak azonosítása

Partner Munkatársak azonosítása elsődlegesen a Kutatóközponti Munkatársak azonosításával azonos műszaki megoldások szerint történhet.

Partner Munkatársak hozzáférése az Információs Infrastruktúra elemeihez csak legfeljebb egy évre adható meg, ami a jogosultság felülvizsgálata után újabb legfeljebb egy évvel meghosszabbítható.

A felhasználói adatok vonatkozásában az Adatgazda szerepkört az a Egységvezető gyakorolja, akinek az egységében a Partner Munkatárs az együttműködésben részt vesz. Amennyiben a Partner Munkatárs csak egy adott labor IT erőforrásaihoz férhet hozzá, akkor az Adatgazda szerepkört a labor felelős Adatgazdája látja el.

3.3.5. Egyetemisták azonosítása

Egyetemisták azonosítása elsődlegesen a Kutatóközponti Munkatársak azonosításával azonos műszaki megoldások szerint történhet.

Egyetemisták hozzáférése az Információs Infrastruktúra elemeihez csak legfeljebb egy évre adható meg, ami a jogosultság felülvizsgálata után újabb legfeljebb egy évvel meghosszabbítható.

A felhasználói adatok vonatkozásában az Adatgazda szerepkört az a Egységvezető gyakorolja, akinek az egységében az Egyetemista a kutatásban részt vesz.

3.3.6. Nyugdíjas Munkatársak azonosítása

A Nyugdíjas Munkatársak azonosítása elsődlegesen a Kutatóközponti Munkatársak azonosításával azonos műszaki megoldások szerint történhet.

Nyugdíjas Munkatársak hozzáférése az Információs Infrastruktúra elemeihez legfeljebb egy évre adható meg, ami a jogosultság felülvizsgálata után újabb legfeljebb egy évvel meghosszabbítható.

A felhasználói adatok vonatkozásában az Adatgazda szerepkört az a Egységvezető gyakorolja, akinek az egységéből a Nyugdíjas Munkatárs nyugdíjba vonult.

3.3.7. Vendég Felhasználók azonosítása

Fizikai jelenlét esetén

A Kutatóközpontot meglátogató Vendég Felhasználók számára korlátozott Internet hozzáférés biztosítása kizárólag a Kutatóközpontban tartózkodásuk idejére, ideiglenesen lehetséges. Az ideiglenes hozzáférés érvényességi ideje legfeljebb 30 naptári nap lehet.

A Vendég Felhasználók azonosító adatainak tekintetében az őket vendégül látó Kutatóközponti Munkatárs gyakorolja az Adatgazda szerepkört.

Föderatív szolgáltatások esetén

A Kutatóközpont által az EduID és EduGAIN föderációk keretében nyújtott szolgáltatásokat igénybe vevő Vendég Felhasználók esetében a föderációs megállapodás alapján a gazdaintézmény gyakorolja az Adatgazda szerepkört.

Egyéb esetekben

A nyilvános szolgáltatások kivételével, fizikai jelenlét vagy föderatív azonosítás hiányában Vendég Felhasználó nem férhet hozzá az Információs Infrastruktúrához.

3.4. Hálózathasználati szabályok

3.4.1. Általános hálózathasználati szabályok

A Központi Információs Infrastruktúra számítógépes hálózati elemeire (a továbbiakban: Kutatóközponti Hálózat) csak az üzemeltetéséért felelős szervezeti egység (a továbbiakban: Hálózat Üzemeltetés) engedélyével, az általuk meghatározott módon csatlakoztathatók eszközök.

A Hálózat Üzemeltetés feladatát a Számítógép Hálózati Központ (SzHK) végzi.

A Kutatóközponti Hálózatra csatlakozó eszközt az eszközgazdának regisztrálni kell. A regisztráció során megadásra kerülő adatok legalább az alábbiak:

- az eszközhöz rendelt Rendszergazda és Informatikai Felelős azonosító adatai,
- az eszköz hálózati csatlakozóinak fizikai azonosító (MAC) címei.

Az eszközök hálózati csatlakozóinak fizikai azonosító (MAC) címeit megváltoztatni tilos.

A regisztráció során megadott adatok változásáról a Hálózat Üzemeltetést haladéktalanul értesíteni kell. Ennek hiányában a Hálózat Üzemeltetés jogosult az adott eszköz csatlakozásának azonnali megszüntetésére.

A Kutatóközponti Hálózatra csatlakozó eszközök esetében a hardver és szoftver nyilvántartás naprakészen tartása érdekében az eszköz Rendszergazdájának a Hálózat Üzemeltetés által megadott nyilvántartó szoftvercsomagot az eszközre telepíteni kell. Amennyiben az eszköz operációs rendszere nem támogatja a nyilvántartó

szoftvercsomagot, az eszköz Rendszergazdája köteles a hardverről, az operációs rendszerről és a szoftvercsomagokról naprakész nyilvántartást vezetni és azt Hálózat Üzemeltetés kérésére azok számára egy munkanapon belül átadni.

A Kutatóközponti Hálózatra csatlakozó eszközök esetében:

- csak a Hálózat Üzemeltetés által meghatározott IP címek felhasználása engedélyezett,
- az IP címen bármilyen, a Kutatóközponttól független szolgáltatás biztosítása, az IP címre domain név bejegyzése, illetve bármilyen, az IP címmel összefüggésbe hozható, a Kutatóközponti munkatárs tevékenységétől független felhasználás csak az IBF engedélyével lehetséges,
- a hálózati forgalom és a felhasználás IBSZ szerinti megfelelőségéért az adott eszköz felhasználói, illetve az eszközhöz rendelt Rendszergazda egyaránt felelős.

A Kutatóközponti Hálózat üzemeltetése során a diagnosztikai és konfigurációs pontokhoz való fizikai és logikai hozzáférést a Hálózat Üzemeltetésnek folyamatosan ellenőrizni kell.

Magántulajdonú eszközök csak a Kutatóközponti Hálózat vendégek számára fenntartott részeire csatlakoztathatók, amely hálózatok a következők:

- eduroam
- Wigner guest

A Kutatóközponti Hálózat vendégek számára fenntartott részeire csatlakoztatott eszközökről sem nyilvántartást nem kell vezetni, sem azokra nyilvántartó programot nem kell telepíteni.

3.4.2. Vezetékes hálózatok használata

A Kutatóközpontban csak a Hálózat Üzemeltetés üzemeltethet vezetékes hálózatot. Ez azt is jelenti, hogy épület, helyiség felújítás megkezdése előtt a Hálózat üzemeltetőivel konzultálni kell. A Hálózat Üzemeltetés tudta és hozzájárulása nélkül a vezetékes hálózatot tilos

- megbontani, átalakítani,
- a hálózaton aktív hálózati eszközt (router, switch) elhelyezni, üzembe helyezeni, üzemeltetni.

3.4.3. Vezeték nélküli hálózatok használata

A Kutatóközpontban csak a Központi Információs Infrastruktúra vezeték nélküli hálózati (WiFi) szolgáltatása üzemeltethető, egyéb vezeték nélküli elérési pont vagy szolgáltatás működtetése csak a Kutatóközponti Hálózat üzemeltetés engedélyével történhet.

A Kutatóközpont területén elérhető eduroam valamint Wigner guest vezeték nélküli hálózati szolgáltatások felhasználási feltételeit az eduroam szolgáltatás egyedileg szabályozza.

3.4.4. Zárt alhálózatok szabályai

A zárt alhálózat egy fizikai eszközön túl terjedő, tűzfallal védett, jellemzően NAT, VPN, SOCKS, illetve egyéb proxy, routing, tunneling vagy port forwarding technológia alkalmazásával létrehozott, jellemzően privát IP címeket alkalmazó számítógépes hálózat.

Az IBSZ előírásai szempontjából nem minősül zárt alhálózatnak:

- a kizárólag egy fizikai eszközön belül üzemelő, jellemzően virtualizációs technológiából eredő alhálózat,
- a kizárólag kliensként igénybe vett VPN hálózati szolgáltatás.

A Kutatóközponti Hálózatra csatlakozó eszközök esetén csak a Kutatóközponti Hálózat üzemeltetés engedélyével alakítható ki zárt alhálózat.

A Kutatóközponti Hálózatra csatlakozó, elkülönített zárt alhálózathoz tartozó eszközök esetében, a elkülönített alhálózatot üzemeltető Rendszergazdának gondoskodnia kell arról (pl.: netflow és megfelelő azonosítási naplózás segítségével), hogy az érintett eszközökről származó hálózati forgalomért felelős Felhasználók visszamenőleg is azonosíthatók legyenek.

Az elkülönített alhálózatot üzemeltető Rendszergazdának az alhálózatukat használó eszközökről az Általános hálózathasználati szabályoknak megfelelő nyilvántartást kell vezetni.

3.4.5. Az Internet felé elérhető szolgáltatást nyújtó rendszerek

Az Internet felé elérhető szolgáltatást nyújtó rendszerek célhoz kötötten regisztrálni kell. A regisztrációt legalább évente, de a regisztrációs adatok változása esetén minden esetben meg kell újítani. A nem megújított regisztrációhoz köthető szolgáltatási portok, illetve IP címek visszavonásra / tiltásra kerülnek.

A szolgáltatás regisztráció során megadásra kerülő adatok legalább az alábbiak:

- a szolgáltatáshoz rendelt Rendszergazda és Informatikai Felelős azonosító adatai;
- a szolgáltatás rövid leírása, célja;
- a szolgáltatást nyújtó TCP/UDP portok és ezek leírásai.

Az Internet felé elérhető szolgáltatást nyújtó rendszereken minden lehetséges eszközzel meg kell akadályozni, hogy az Infrastruktúra erőforrásai az Internet irányából jogosulatlan fél számára elérhetővé váljanak. A felsorolt szabályok alól az IBF adhat felmentést. A hozzáférés védelme érdekében az állomások üzemeltetésével szemben támasztott minimális elvárások:

- Az állomások nem csatlakozhatnak zárt alhálózatokhoz.
- Privilegizált távoli hozzáférési célra a Kutatóközponti VPN szolgáltatás használata kötelező. Az Internet irányából tilos a jelszó alapú SSH, távoli asztal, vagy más, rendszerszintű adminisztratív hozzáférés engedélyezése.
- Tilos a jelszó (passphrase) nélküli ssh kulcs használata.
- Tilos a NAT, VPN, SOCKS, TOR, illetve egyéb proxy, routing, tunneling vagy port forwarding technológia általános, de különösen adminisztratív elérési célra történő alkalmazása. Kivételt képeznek az ilyen szolgáltatásokat dedikáltan nyújtó állomások.
- Az Internet irányába nem nyújthatók elavult, megfelelő azonosítási és biztonsági funkciókat nem tartalmazó szolgáltatások.

3.4.6. Biztonsági vizsgálatok

Az Információs Infrastruktúra megfelelő működésének folyamatos biztosítása érdekében a Hálózat Üzemeltetés fenntartja a jogot, hogy:

- a Kutatóközponti Hálózat megfelelő működésének biztosításához szükséges mértékben betekintsenek annak hálózati forgalmába, arról forgalmi adatokat (pl.: netflow) rögzítsenek;
- a Kutatóközponti Hálózatra közvetett vagy közvetlen módon csatlakozó eszközök és szolgáltatások IBSZ szerinti megfelelőségét rendszeresen vagy esetileg vizsgálják, automatizált vagy manuális biztonsági ellenőrzéseket futtassanak;
- az érintettek lehetőség szerinti értesítése mellett, szükség szerint korlátozzák a biztonsági kockázatot jelentő állomásokat;
- a biztonsági vizsgálatoknak a zárt hálózatokra is ki kell terjedni.

A Felhasználók, Rendszergazdák és Informatikai Felelősök kötelesek a felsorolt vizsgálati tevékenységekben aktívan közreműködni, és a kért tájékoztatást haladéktalanul megadni.

3.4.7. Hálózati távmunka

A Kutatóközponti Munkatársak a Kutatóközpont telephelyein kívülről végzett távmunka során a Kutatóközponti VPN szolgáltatást kötelesek használni.

A Kutatóközponti VPN szolgáltatásra csatlakozó Felhasználó kiemelt felelőssége a csatlakozó eszköz IBSZ szerinti megfelelőségének biztosítása, különös tekintettel:

- a Kutatóközponti Infrastruktúra hozzáférésének jogszerűségére, az illetéktelen hozzáférés megakadályozására;
- a csatlakozó hálózati állomás információbiztonsági megfelelőségére, a kártékony szoftverek, valamint a véletlen, illetve szándékos emberi károkozás megakadályozására.

3.4.8. Az Internet használata

A Kutatóközponti Információs Infrastruktúra és az Információs Adatvagyon védelme érdekében, az Internet felhasználása során különös gondossággal kell eljárni:

- kerülni kell a nem megbízható forrásból származó weblapok és fájlok letöltését, megnyitását,
- törekedni kell a korszerű, titkosított és hitelesített hálózati protokollok (például: TLSv1.2+, SSHv2) és védett azonosítási módok felhasználására,
- tilos a Kutatóközponttól független internetes szolgáltatás esetén a Kutatóközponti felhasználói azonosítás során használt azonosító és jelszó megadása,
- tilos a Kutatóközponti e-mail cím megadása bármilyen Kutatóközponttól független internetes szolgáltatás igénybevételéhez, ez alól kivételt képeznek az főigazgatói engedéllyel rendelkező nyugdíjas munkatársak,
- tilos az Információs Adatvagyon bármely elemét a Kutatóközponttal szerződésben nem álló fél által üzemeltetett internetes szolgáltatáson elhelyezni, vagy jogosulatlan fél számára bármely más módon elérhetővé tenni,
- az Internet használata során a KIFÜ IKT Felhasználói Szabályzat (korábbi NIIF AUP) előírásait be kell tartani.

3.5. Információs Rendszerek és Szolgáltatások üzemvédelmi szabályai

3.5.1. Általános szolgáltatás üzemvédelmi kritériumok

Az Információs Rendszerek és Szolgáltatások üzemeltetése során a normál üzemállapothoz tartozó üzemeltetési kritériumokat kell teljesíteni:

- Elsődleges üzemeltetési kritériumok:
  - Bizalmasság: a szolgáltatás, illetve az általa kezelt adatok csak az erre jogosult aktív felhasználók számára elérhetők. A bizalmassági kritérium az adatok tárolása és továbbítása során egyaránt fontos.
  - Sértetlenség: a szolgáltatás által kezelt adatok nem módosulnak és nem sérülnek meg.
  - Rendelkezésre állás: a szolgáltatás, illetve az általa kezelt adatok az elvárt időben és minőségben elérhetők az aktív felhasználók számára.
  - Hatékonyság: a szolgáltatás, illetve annak felhasználása és üzemeltetése célszerűen és arányosan használja fel a rendelkezésre álló anyagi, gépi és emberi erőforrásokat.
  - Alkalmasság: az adatok tárolásának és kezelésének módja, illetve a szolgáltatás funkciói megfelelőek a szolgáltatás kitűzött vagy elvárt céljainak betöltésére.
- Kiegészítő üzemeltetési kritériumok:

- Környezeti megfelelőség: a szolgáltatás, illetve az általa kezelt adatok megfelelnek a hatályos jogi és üzemeltetési szabályzásnak, valamint a felhasználók igényeinek.
- Célhoz kötöttség: a Felhasználók és Rendszergazdák csak célhoz kötötten, a szükséges legkisebb mértékben férnek hozzá a szolgáltatás által kezelt adatokhoz, illetve a szolgáltatási funkciókhoz.
- Minimalitás: a szolgáltatás csak elsődleges céljainak megvalósításához szükséges mértékben tartalmaz funkciókat, illetve kezel adatokat.

3.5.2. Rendszerek és szolgáltatások tartalékolása

Kiemelt vagy kritikus rendszereket kiszolgáló hardver eszközök információbiztonsága érdekében, amennyiben erre lehetőség van, az alábbi előírásokat kell alkalmazni:

- a kiszolgáló hardver eszközöket előírás szerinti fizikai körülmények között, megfelelő légkondicionálással, zavarszűrt, villámcsapás és túláram ellen védett szünetmentes betáplálással kell üzemeltetni,
- a hálózati csatolókat redundáns módon, több fizikai hálózati eszközhöz (switch-hez) kell csatlakoztatni,
- az adattárolókat tükrözéssel vagy egyéb redundancia megoldással (pl. RAID5, RAID6) kell védeni,
- a szolgáltatás folytonosság szempontjából kritikus adatok biztonsági másolatát elkülönült helyszínen kell tárolni,
- a hardver eszközöket aktív biztonsági üzemtartalék céljából többszörözni kell, a tartalék rendszerek közötti automatikus, fél-automatikus vagy manuális átállási folyamatokat definiálni kell.

3.5.3. Biztonsági mentések

A biztonsági mentések kialakítása során kitűzött alapvető célok:

- A mentések teljes körűek legyenek, szükség esetén a mentésből az eredeti működő szolgáltatás, legalább RPO érték szerint meghatározott, ennek hiányában teljes adattartalommal, elfogadható mennyiségű munkával visszaállítható legyen egy teljesen üres, új rendszerre is.
- A mentések konzisztensek, lehetőleg pillanatkép jellegűek, de legalább tranzakcionálisan biztonságosak legyenek, vagyis az adatokat, állományokat ne átmeneti állapotban, nehezen visszaállítható módon tartalmazzák.
- A mentések elkészítése lehetőleg ne korlátozza jelentősen a szolgáltatások teljesítményét, a mentés a lehető legkisebb (célszerűen: zéró) leállással, zárolással járjon.
- A mentésekhez való hozzáférést a mentett rendszerhez való hozzáféréssel azonos biztonsági szinten kell kezelni.

A kritikus vagy kiemelt rendszerek teljes lényegi adattartalmáról legalább heti rendszerességgel biztonsági mentést kell készíteni. Teljes mentésnek minősül az inkrementális vagy differenciális mentés is, amennyiben abból a teljes adattartalom a mentési időpontra visszaállítható.

Minden kritikus vagy kiemelt rendszerhez meg kell határozni az időben mért elfogadható legnagyobb adatvesztés (Recovery Point Objective - RPO), illetve az elfogadható leghosszabb visszaállítási idő (Recovery Time Objective - RTO) értékét. Az RPO és RTO értékek meghatározása az adat- és alkalmazásgazdák feladata. A biztonsági mentési stratégiát, illetve a mentések megőrzési idejét ennek megfelelően, a mentett adattartalom becsült méretét figyelembe véve kell meghatározni.

A biztonsági mentést végző állomásokhoz tartozó tárhelyeket lehetőség szerint el kell különíteni egymástól. Az elkülönítés kötelező, amennyiben az egyes állomásokhoz eltérő felhasználói kör rendelkezik adminisztrációs jogkörrel.

3.5.4. Rendszerek és szolgáltatások dokumentációja

Minden kritikus vagy kiemelt rendszert, valamint az általuk nyújtott szolgáltatásokat dokumentálni kell. A rendszerek vagy szolgáltatások módosítása során gondoskodni kell a dokumentáció aktualizálásáról is. A rendszerek dokumentációs előírásainak biztosítása a Rendszergazda, a szolgáltatások dokumentációs előírásainak biztosítása az Alkalmazásgazda felelősségi körébe tartozik.

A rendszerek és szolgáltatások dokumentációjának főbb céljai:

- A ritkán elvégzett tevékenységek, esetileg felhasznált adatok emlékeztető jellegű rögzítése.
- Az új belépők tájékoztatásának, betanulásának elősegítése.
- A helyettesítések megkönnyítése.
- A kilépők feladat-átadásának megkönnyítése.
- A rendszer átalakítások tervezésének elősegítése.

3.5.5. Rendszerek és szolgáltatások felügyelete

Kritikus vagy kiemelt rendszerekben csak aktív állapot megfigyelés alatt álló fizikai eszközök használhatók. Az ilyen rendszerek által nyújtott szolgáltatások lényegi (felhasználási célra jellemző) működési paramétereit szintén felügyelet alá kell vonni.

A felügyeleti tevékenység alapvető céljai:

- Az üzembiztonság fenntartása az üzemeltetett rendszerekben.
- A krízishelyzetek megelőzése, vagy megfelelő idejű felismerése.
- Az üzemviteli problémák elemzésének támogatása.
- Biztonsági, vagy üzemmenetet érintő incidensek utólagos elemzésének lehetővé tétele.

A megfigyelés során a riasztási határértékek beállításakor az alábbiakra kell törekedni:

- Az üzemeltetők minden fontos, beavatkozást vagy figyelmet igénylő változásról, krízishelyzetről időben értesítést kapjanak.
- Az üzemeltetők ne kapjanak feleslegesen értesítést az üzemszerűen beálló, üzembiztonságot nem veszélyeztető és közvetlen beavatkozást nem igénylő eseményekről.

3.5.6. Üzemi naplózás

Az Információs Adatvagyont kezelő eszközök és szolgáltatások üzemnaplóit folyamatosan, az esetleges biztonsági események észlelését és felderítését, illetve a felelősségek megállapítását lehetővé tevő részletességgel, megbízható módon rögzíteni kell.

A kritikus vagy kiemelt rendszerek üzemnaplóit:

- legalább 6 hónapra visszamenőleg meg kell őrizni,
- a helyi megőrzés mellett egy központi elhelyezésű naplógyűjtő szerverre is továbbítani kell.

Üzemnaplókban felhasználói vagy egyéb jelszavak, érzékeny információk kódolatlan tárolása, naplózása tilos.

Az üzemnaplókra vonatkozó szabályoktól csak az IBF engedélyével szabad eltérni.

3.5.7. Változáskezelés

Az Információs Adatvagyont kezelő eszközök és szolgáltatások szoftveres vagy hardveres konfigurációs változásait folyamatosan, az esetleges biztonsági események észlelését és felderítését lehetővé tevő részletességgel, megbízható módon rögzíteni kell.

A konfigurációs változások végrehajtási és jóváhagyási folyamatát minden kritikus vagy kiemelt szolgáltatásra meg kell határozni. Ennek keretében az új vagy módosított rendszer szolgáltatásokat használatba vétel előtt tesztelni kell, a szolgáltatások helyes működését tesztadatokkal kell ellenőrizni.

3.6. Az elektronikus levelezés szabályai

3.6.1. Központi levelezési szolgáltatások

A Kutatóközponti Munkatársak számára a Központi Információs Infrastruktúra központi levelezési szolgáltatást biztosít. A szolgáltatás fő komponensei:

- @wigner.hu és @wigner.hun-ren.hu végződésű nyilvános e-mail címek, valamint minden megőrzött, régi domainhez tartozó e-mail cím,

- IMAP/TLS, IMAPs protokollon, valamint webmail felületen elérhető levelezési postafiókok,
- SPAM- és vírusszűrés,
- SMTP/TLS levélfeladási és levéltovábbítási szolgáltatás,
- levelezési lista szolgáltatások.

A központi levelezési szolgáltatás célja a Kutatóközponti Munkatársak elsődleges kutatási és fejlesztési tevékenységének standard, felhasználói célú támogatása, a Kutatóközpont üzemszerű működésének elősegítése.

3.6.2. Általános felhasználási szabályok

A központi levelezési szolgáltatások igénybevételi lehetőségei a Felhasználói jogosultság megszűnése esetén az alábbiak:

- A felhasználói jogosultság megszűnését követő napon automatikusan megszűnik a Kutatóközponti postafiók aktív elérési lehetőségének bármely formája
- A felhasználó Kutatóközponti e-mail címváltozatai lekerülnek a Kutatóközponti levelezőlistákról
- Legfeljebb féléves időtartamra kérhető a Kutatóközponti e-mail cím átirányítása a felhasználó személyes e-mail címére
- Az átirányítási határidő leteltével megszűnnek a felhasználó Kutatóközponti e-mail címváltozatai, postafiókjának tartalma pedig végérvényesen törlődik

A Kutatóközpont elektronikus levélben történő megszemélyesítésére, képviseletére, nevében történő eljárásra a @wigner.hun-ren.hu végződésű, hivatalos e-mail címek szolgálnak.

Az elektronikus levelezés során tilos a Kutatóközpont jó hírét, üzleti érdekeit sértő tevékenység, különösen:

- a címzett hozzájárulása nélküli, kéretlen levelek küldése, továbbítása,
- kártékony szoftverek vagy egyéb biztonsági veszélyt jelentő tartalom küldése, továbbítása,
- jogsértő, a Kutatóközpont etikai elveinek nem megfelelő tartalom küldése, fogadása, különösen: privát levelek, lánclevelek engedély nélküli továbbítása,
- a Kutatóközpont nevében politikai, erkölcsi, vagy egyéb, nem szakmai jellegű vélemény kinyilvánítása,
- titkosítatlan levélben többször felhasználható jelszavak, érzékeny pénzügyi adatok, üzleti titkok továbbítása.

A levelezés, illetve a Kutatóközponti munkaállomások védelme érdekében csak megfelelő körültekintéssel és előzetes vizsgálatot követően szabad:

- ismeretlen féltől származó e-mail üzenetet, mellékletet, futtatható fájlt megnyitni,

- nem megbízható forrásból származó felszólításra adatokat közölni.

A levelezési szolgáltatások felhasználása során, azok üzembiztonságának fenntartása érdekében tilos a rendszer alapvető céljaitól eltérő, aránytalanul nagy mennyiségű vagy küldése, vagy továbbítása.

Az elektronikus levelezés során figyelembe kell venni a KIFÜ IKT felhasználási szabályait (korábbi NIIF AUP).

3.6.3. Levél átvételi folyamat, biztonsági szűrések

A levelezési szolgáltatások védelme érdekében a levél átvételi folyamat során a következő védelmi intézkedéseket kell fenntartani:

- a feladó állomások és e-mail címek helyi és nyilvános tiltólista (például: DNSBL) alapú szűrése,
- a feladó állomások és e-mail címek hihetőség vizsgálata (például: SPF, DKIM, DMARC),
- kártékony szoftverek központi és felhasználói munkaállomáson történő szűrése (vírusellenőrzés),
- kéretlen levelek szűrése (SPAM- és tartalomszűrés),
- felhasználói kézbesítési szabályok alkalmazása (ún.: sieve szabályok),
- postafiók méretkorlátok (ún.: quota) betartatása.

3.6.4. A levelezés naplózása

A levelezési szolgáltatások naplóit legalább 1 évre visszamenőleg meg kell őrizni. A naplók minimális adattartalma, az eseményekhez kapcsolt időbélyegeken felül:

- Levél átvételi és továbbítási (transport) naplók, a feladó és címzett állomások, valamint e-mail címek lehetőség szerinti azonosításával.
- A levél tárgya
- Levél kézbesítési (delivery) naplók, a címzett postafiók és postafiók mappa lehetőség szerinti azonosításával.

3.6.5. Levelezési postafiókokhoz történő hozzáférés

A Kutatóközpont hivatalos e-mail címeihez tartozó levelezési postafiókokhoz csak az arra jogosult Felhasználók férhetnek hozzá:

- Személyes felhasználású, illetve egy adott felhasználóhoz köthető postafiókokhoz csak a hozzá rendelt személy férhet hozzá. Személyes postafiókok esetén ez a személy gyakorolja az Adatgazda szerepkört.
- Csoportcélú postafiókokhoz, levelezési listákhoz csak az erre jogosult személyek férhetnek hozzá. A hozzáférési jogosultságok meghatározása a postafiók kezelésére kijelölt Adatgazda feladata. Központi levelezési listák esetén az

Adatgazda a levelezési lista adminisztrátora, csoportos postafiókok esetén az Adatgazda a csoport munkájáért felelős Egységvezető.
- A postafiókokat kezelő Rendszergazdák a postafiókokban tárolt üzenetekbe az üzemvitel biztosításának céljából a szükséges legrövidebb ideig és mértékben betekinthetnek.

A felsorolt eseteken felül, a levelezési postafiókokhoz, illetve az ezekben tárolt üzenetekhez hozzáférési jogot csak a Kutatóközpont főigazgatója adhat.

3.6.6. Külső levelezési szolgáltatók

Hivatalos Kutatóközponti levelezés, a Kutatóközpont képviselete külső, nyilvános levelezési szolgáltatáson (például: Gmail, Freemail, Indamail, Citromail) nem folytatható.

Zárt felhasználású külső kiszolgálón (például: egyetem, más akadémiai Kutatóközpont, szerződéses partner) üzemeltetett postafiók Kutatóközponti célú felhasználása esetén a Felhasználót személyes felelősség terheli azért, hogy a külső kiszolgáló megfeleljen az IBSZ előírásainak.

3.7. Egyéb szabályok

3.7.1. A web- és egyéb tartalomszolgáltatások szabályai

Az Információs Infrastruktúra által nyújtott tartalomszolgáltatásnak minősül minden olyan információs szolgáltatás, mely szöveges információk, adatfájlok vagy multimédiás anyagok elérését több Felhasználó számára biztosítja. Tartalomszolgáltatások különösen: a WEB, FTP, Streaming, SMB és P2P fájlmegosztó szolgáltatások. Nem tartalomszolgáltatások az üzenettovábbító szolgáltatások (például: elektronikus levelezés, Skype, XMPP, IRC, Matrix).

A tartalomszolgáltatások működése során az Adatgazda felelőssége az elérhetővé tett tartalom jogi megfelelőségének folyamatos biztosítása, illetve a tartalomra vonatkozó hozzáférési jogosultságok meghatározása. Az Adatgazda meghatározása a következők szerint történik:

- Weblapok esetén az Adatgazda a weblap tartalmi felelőse.
- Kutatóközponti, vagy valamelyik egységhez köthető fájlmegosztó szolgáltatások esetén az adatgazda a fájlok feltöltője, illetve – amennyiben a tulajdonos nem meghatározható – a szolgáltatást üzemeltető egység vezetője.
- Személyi munkaállomásokon elérhetővé tett, vagy azonosítható felhasználók által közös megosztási helyre feltöltött tartalom esetén az Adatgazda a tartalomhoz köthető Felhasználó.
- Amennyiben a tartalomszolgáltatás a fenti esetek egyikébe sem sorolható, az Adatgazda a szolgáltatást üzemeltető egység vezetője.

3.7.2. Azonnali üzenettovábbító szolgáltatások felhasználása

Azonnali üzenettovábbító szolgáltatások a személyes jelenlétet helyettesítő, az egyedi vagy csoportos információcserét lehetővé tevő szöveges, hang, vagy képtovábbítási kommunikációs szolgáltatások. Azonnali üzenettovábbító szolgáltatások például: a Skype, az XMPP vagy VoIP alapú, illetve az egyéb instant messaging és videokonferencia szolgáltatások.

Azonnal üzenettovábbító szolgáltatások felhasználása során tilos a Kutatóközpont jó hírét, üzleti érdekeit sértő tevékenység, különösen:

- kártékony szoftverek vagy egyéb biztonsági veszélyt jelentő tartalom küldése, továbbítása,
- jogsértő, a Kutatóközpont etikai elveinek nem megfelelő tartalom küldése, fogadása, különösen: privát üzenetek engedély nélküli továbbítása,
- a Kutatóközpont nevében politikai, erkölcsi, vagy egyéb, nem szakmai jellegű vélemény nyilvánítása,
- többször felhasználható jelszavak, érzékeny pénzügyi adatok, üzleti titkok továbbítása.

A Kutatóközponti munkaállomások védelme érdekében csak megfelelő körültekintéssel és előzetes vizsgálatot követően szabad:

- ismeretlen féltől származó mellékletet, futtatható fájlt megnyitni,
- nem megbízható forrásból származó felszólításra adatokat közölni.

3.7.3. Az információs károkozás elleni védelmi intézkedések

A rosszindulatú szoftverek által okozott károk, illetve a szándékos emberi károkozás megelőzése érdekében a Kutatóközponti Információs Infrastruktúrába csatlakozó állomásokon csak korszerű számítógépes biztonsági megoldásokkal védett eszközök és szolgáltatások üzemeltethetők.

Az állomásokkal szemben támasztott minimális elvárások:

- Aktív biztonsági támogatással rendelkező operációs rendszer és kiszolgáló szoftverek használata; a biztonsági frissítések rendszeres és tervezett telepítése.
- Alapértelmezett, gyártói hozzáférések letiltása, vagy megváltoztatása.
- Elérhető szolgáltatások minimalizálása, felesleges szoftverek eltávolítása.
- Lehetőség szerint titkosított és hitelesített hálózati protokollok alkalmazása.
- Nyilvános hálózat irányából elérhető szolgáltatást nyújtó eszközök esetén: rendszerszintű és szolgáltatási események naplózása, a naplók megőrzése legalább 6 hónapig.
- Lehetőség szerint host tűzfal használata, alapértelmezett elutasító üzemmódban.
- Egyéb proaktív védelmi intézkedések lehetőség szerinti alkalmazása.

- Lehetőség szerint korszerű és naprakész adatbázissal rendelkező vírusvédelmi szoftver folyamatos futtatása.

A Kutatóközpontban nem használható információt szivárogtató, ún. spyware, adware és egyéb, a Kutatóközpont érdekeit sértő, külső fél nem kívánt üzleti tevékenységét támogató szoftver.

A Kutatóközpontban fejlesztett, harmadik fél számára elérhető szoftverek, szolgáltatások, valamint műszaki jellegű publikációk létrehozása során kiemelt figyelmet kell arra fordítani, hogy ezek ne nyújtsanak, illetve ne tartalmazzanak:

- az Információs Infrastruktúra elemeihez kiemelt vagy jogosulatlan hozzáférést biztosító beépített azonosítókat, jelszavakat,
- az Információs Infrastruktúra megismerését a szükségesnél jobban lehetővé tevő információkat,
- a Kutatóközpont üzleti érdekeit sértő vagy jó hírét veszélyeztető egyéb információkat.

A Kutatóközpontban törekedni kell a „tiszta asztal” és „tiszta képernyő” irányelvek betartására: az érzékeny információk könnyen hozzáférhető helyen történő tárolását kerülni kell.

4. Hivatkozások

- MKH Titkárság Informatikai Biztonsági Keretszabályzat
- 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról
- A KIFÜ IKT Felhasználói Szabályzata (korábbi NIIF program AUP)

5. Mellékletek

5.1. Információs részinfrastruktúra regisztrációs űrlap

– Általános adatok

Megnevezés	**Leírás**
Név	Az Információs részinfrastruktúra neve
Pontos helyszín	Az összes épület/helyiség, amelyben található
Szervezeti egység neve	A szervezeti egység neve
Informatikai felelős neve, email címe, telefonszáma	
Helyettes informatikai felelős neve, email címe, telefonszáma	

– Hálózati adatok

Belső IP címtartomány (privát IP címek esetén)	
DHCP szerver(ek) IP címei	
A kutatóközponti hálózatra való csatlakozás módja (pl. NAT-olós tűzfal, router)	
A kutatóközponti hálózatra való csatlakozást biztosító eszköz(ök) kutatóközponti hálózati IP címe(i)	
VLAN azonosító (amennyiben VLAN köti össze a helyiségeket és szeparálja a hálózatot)	

– Kiszolgálói adatok (minden kiszolgálóhoz külön-külön)

A kiszolgáló neve	
A kiszolgáló IP címe(i)	
Hol található fizikailag	Épület/helyiség
Rendszergazda neve, email címe, telefonszáma	
Helyettes rendszergazda neve, email címe, telefonszáma	

– Szolgáltatás adatok (minden szolgáltatáshoz külön-külön)

A kiszolgáló neve, amely nyújtja a részinfrastruktúra számára	
A szolgáltatás megnevezése	
A szolgáltatás leírása	
Alkalmazásgazda neve, email címe, telefonszáma (amennyiben eltér a rendszergazdától vagy a helyettesétől)	

5.2. Internet felé elérhető szolgáltatás regisztrációs űrlap

– Általános adatok

Megnevezés	**Leírás**
Név	A szolgáltatás megnevezése
Leírás	A szolgáltatás leírása
Pontos helyszín	Az összes épület/helyiség, amelyben található
Szervezeti egység neve	A szervezeti egység neve
Informatikai felelős neve, email címe, telefonszáma	
Helyettes informatikai felelős neve, email címe, telefonszáma	

– Kiszolgálói adatok

A kiszolgáló neve a DNS-ben, amely a szolgáltatást nyújtja	
A kiszolgáló IP címe(i)	
Hol található fizikailag	Épület/helyiség
Rendszergazda neve, email címe, telefonszáma	
Helyettes rendszergazda neve, email címe, telefonszáma	

– Szolgáltatás adatok

Alkalmazásgazda neve, email címe, telefonszáma (amennyiben eltér a rendszergazdától vagy a helyettesétől)	
Amennyiben a szolgáltatás IP cím alapján korlátozott kör számára elérhető, annak megadása	

6. Fogalomtár

- Aktív felhasználó: egy adott szolgáltatás tekintetében értelmezhető. Az aktív felhasználó olyan természetes személy, aki folyamatosan, vagy időszakosan igényt tart a szolgáltatásra. A szolgáltatás létesítésének elsődleges célja az aktív felhasználók közvetett vagy közvetlen kiszolgálása.
- Belső szolgáltatás: kizárólag azonosított Munkatársak számára nyújtott szolgáltatás
- Fontos adat: az Információs Adatvagyon részét képező, bizalmas, pótolhatatlan, vagy nehezen pótolható adat, amely a szolgáltatás elsődleges, vagy járulékos funkciójának betöltéséhez szükséges. A szolgáltatás működéséhez szükséges konfigurációs adatok jellemzően fontos adatok.
- Kiszolgáló (szerver): telekommunikációs hálózaton keresztül igénybe vehető szolgáltatásokat nyújtó, önálló operációs környezettel rendelkező, fizikai vagy virtuális eszköz.
- Munkaállomás (host): a Kutatóközpont fizikai vagy logikai számítógépes hálózatára csatlakozó bármely eszköz.
- Nyilvános szolgáltatás: elsődleges célját tekintve azonosítás nélkül, vagy nyilvános regisztrációt követő azonosítással igénybe vehető szolgáltatás.
- Szerződéses szolgáltatás: Szerződéses Partner számára nyújtott, vagy föderatív alapú azonosítást alkalmazó szolgáltatás
- Szolgáltatás: kiszolgáló vagy telekommunikációs hálózat által nyújtott funkció(halmaz), melyet felhasználók, vagy az általuk, vagy érdekükben üzemelő rendszerek, illetve egyéb szolgáltatások vehetnek igénybe.
- Zárt hálózat: az Internet irányából közvetlenül nem elérhető, jellemzően privát IP címtartományokat alkalmazó számítógépes hálózat.