CSFK-01663-001/2024

CSILLAGÁSZATI ÉS FÖLDTUDOMÁNYI KUTATÓKÖZPONT

Informatikai Biztonsági Szabályzat (IBSZ)

Összeállította és jóváhagyásra előterjesztette:

Varga Szabolcs
informatikai vezető

Jóváhagyom:

Kiss László
főigazgató

Csillagászati és Földtudományi Kutatóközpont
CSFK
1.

2023.

1 Dokumentum adatai

Dokumentum típusa	Informatikai Biztonsági Szabályzat
Hatályba lépés dátuma	2023.12.20.
Érvényesség vége	Visszavonásig
Következő felülvizsgálat időpontja	Hatályba lépés + 1 év, vagy releváns MKH keretszabályzat, jogszabályi, lényeges kockázat, súlyos incidens bekövetkezése esetén.
Felelős szakterület	Információbiztonsági Felelős (IBF) – SSM Kft.
Kibocsájtó	Csillagászati és Földtudományi Kutatóközpont
Szakmai felelős	Főigazgató
Biztonsági besorolás	Belső használatra

2 Változások jegyzéke

Módosítás dátuma	A módosítás oka /rövid leírása	Verziószám
2023.12.20.	Első kiadott verzió	v1.0

3 Tartalomjegyzék

4 Bevezetés

4.1 A Szabályzat célja

Jelen Szabályzat a Csillagászati és Földtudományi Kutatóközpont (továbbiakban: kutatóközpont vagy CSFK) információs környezetére vonatkozó biztonsági működési elvárások meghatározása, melynek alkalmazásával az információs rendszerek teljes életciklusában megvalósítja és biztosítja az alábbi alapvető információbiztonsági védelmi követelmények teljesülését:

- Az információs rendszerekben kezelt adatok és információk bizalmassága, sértetlensége és rendelkezésre állása.
- információs rendszerek és elemeinek sértetlensége és rendelkezésre állása,
- a fizikailag elkülönített helyszíneik közötti kormányzati célú hálózaton, továbbá a publikus internet felületen zajló, az elektronikus hírközlési törvény szerinti szolgáltató igénybevételével vagy egyéb információs társadalommal összefüggő szolgáltatásaik igénybevétele során zárt, teljes körű, folytonos és kockázatokkal arányos kriptográfiai védelmét.
- Az információs rendszernek kockázatarányos védelme érdekében a CSFK logikai, fizikai és adminisztratív védelmi intézkedéseket valósít meg, amelyek támogatják:
    - a megelőzést és a korai figyelmeztetést,
    - az észlelést,
    - a reagálást,
    - a biztonsági események kezelését
- elvesztés vagy eltulajdonítás elleni védelem;
- célravezető használat biztosítása;
- hitelesség védelme;
- letagadás elleni védelem (letagadhatatlanság);
- az üzleti és a személyes adatok védelme.

4.2 Alanyi(személyi) hatály

A Szabályzat alanyi hatálya kiterjed:

- Munkaviszonyban vagy munkavégzésre irányuló egyéb jogviszonyban álló személyekre, valamint azon személyekre, akik – munkatapasztalat-szerzési, kutatási vagy képzési célból – szakmai gyakorlatukat a kutatóhelynél töltik (pl.: egyetemi vagy PhD hallgatók, vendégkutatók stb.), (a továbbiakban együttesen: foglalkoztatottak);

- Minden személyre, aki a szervezeti hatály informatikai vagy azzal összefüggő rendszerét, szolgáltatásait igénybe veszi, informatikai struktúráját és annak eszközeit üzemelteti vagy használja, függetlenül a kutatóhelyhez kapcsolódó jogviszonyától, a vele kötött szerződésben vagy a részére kiadott engedélyben rögzített mértékben, feltéve, hogy a keretszabályzat tartalmát számukra megismerhetővé tették.

4.3 Tárgyi hatály

A Szabályzat tárgyi hatálya kiterjed:

- Minden, a CSFK által folytatott tevékenységre, működtetett folyamatra, eljárásra, hatályos szabályozásra, utasításra, döntésre, amelyek a CSFK informatikai szempontú biztonságos működését közvetlenül vagy közvetetten érintik, továbbá befolyásolják;

- A CSFK által birtokolt vagy azok érdekében létrehozott, továbbá kezelt információs adatvagyonra, különösen a kutatási eredményekre, a szellemi tulajdonra, az üzleti, a személyes vagy egyéb okokból érzékeny, védendő információkra;

- Az információs adatvagyon elemeit kezelő, tároló, valamint továbbító információs eszközvagyonra, különösen az informatikai és telekommunikációs eszközökre, munkaállomásokra, kiszolgálókra, adattárolókra, mobil eszközökre, valamint a kutatóhely által igénybe vett külső (pl.: felhőalapú) informatikai szolgáltatásokra.

4.4 Területi hatály

A Szabályzat területi hatálya kiterjed:

- A Kutatóközpont irányítása alá tartozó minden telephelyre.

- A beszállítók minden olyan helyszínére, telephelyére, amely a beszállítók irányítása alá tartozik és amelyektől szolgáltatást vesz igénybe.

- az otthoni munkavégzés helyéül szolgáló ingatlanokra.

4.5 Időbeli hatály, felülvizsgálat

A Szabályzat a Dokumentum adatai fejezetben a „Hatályba lépés dátuma" sorban jelzett napon lép hatályba és legkésőbb 12 havonta felül kell vizsgálni, vagy MKH keretszabályzat változás, releváns jogszabályi, lényeges új kockázat azonosítása, súlyos incidens bekövetkezése esetén.

5 Az IBSZ-szel kapcsolatos feladatok

Feladat	(R)Végrehajtó	(A)Döntéshozó	(C)Konzulensek	(I)Tájékoztatandó(k)
IBSZ elkészítése, felülvizsgálata és módosítása	IBF	Főigazgató	Informatikai osztály, beszállítók	-
IBSZ elfogadása és kihirdetése	Főigazgató	Főigazgató	IBF	CSFK munkatársak, beszállítók
IBSZ betartásának ellenőrzése	IBF	IBF	Informatikai osztály, beszállítók	Főigazgató

5.1 A szabályzat elkészítése, felülvizsgálata és módosítása

A szabályzat elkészítése, felülvizsgálata és szükség szerinti módosítása az Információbiztonsági Felelős (továbbiakban: IBF) feladata és felelőssége, együttműködve az Informatikai osztállyal, az adatgazdákkal, az adatvédelmi szakértőkkel és a releváns beszállítókkal. A szabályzat elkészítésében, felülvizsgálatában és módosításában közreműködnek az elektronikus információbiztonsági feladatok ellátásában közreműködő személyek, szervezeti egységek, valamint az elektronikus információs rendszer üzemeltetéséért, fejlesztéséért felelős szervezeti egységek vezetői. A felülvizsgálat eredményéről az Informatikai biztonsági felelős tájékoztatja a Főigazgatót.

5.2 A szabályzat elfogadása és kihirdetése

A szabályzat elfogadása és kihirdetése a Főigazgató feladata. A kihirdetés normatív utasítással történik. A kihirdetés során a Főigazgató gondoskodik arról, hogy annak tartalma ne legyen módosítható, és az abban foglalt adatok csak az arra felhatalmazott személyek által legyen megismerhető.

5.3 A szabályzat betartásának ellenőrzése

A szabályzat betartásának ellenőrzése az IBF feladata, melyben közreműködnek az Informatikai osztály munkatársai, szervezeti egységek, valamint az elektronikus információs rendszer üzemeltetéséért, fejlesztéséért felelős szervezeti egységek vezetői.

6 Az informatikai biztonság szervezete

6.1 Informatikai biztonsági szerepek és felelősségek

6.1.1 Főigazgató

Hatásköre: A CSFK működését és személyi állományát érintő döntések meghozatala és a rá delegált munkáltatói jogok gyakorlása. A szabályzatok és eljárásrendek elfogadása és szervezeti szintű kihirdetése és az Informatikai Biztonsági Felelős (IBF) kinevezése, valamint a Cselekvési terv és az ahhoz kapcsolódó Költségvetési terv elfogadása.

Felelőssége: A szervezet operatív működésének elősegítése és felügyelete, a rendelkezésre álló személyi és tárgyi erőforrások optimális kihasználásának biztosítása, valamint a jogszabályoknak megfelelő működés ellenőrzése. Az informatikai biztonság személyi és tárgyi feltételeinek, valamint a jogszabályoknak megfelelő működéshez szükséges feltételek biztosítása.

Feladatai: Mint a Kutatóközpont első számú vezetője, köteles gondoskodni a jogszabályi megfelelésnek a következők szerint:

- biztosítja az elektronikus információs rendszerre irányadó biztonsági osztály tekintetében a jogszabályban meghatározott követelmények teljesülését,
- biztosítja a szervezetre irányadó biztonsági szint tekintetében a jogszabályban meghatározott követelmények teljesülését,
- az elektronikus információs rendszer biztonságáért felelős személyt nevez ki vagy bíz meg,
- meghatározza a szervezet elektronikus információs rendszerei védelmének felelőseire, feladataira és az ehhez szükséges hatáskörökre, felhasználókra vonatkozó szabályokat, illetve kiadja az IBSZ-t,
- jóváhagyja az Informatikai Biztonsági Stratégiát (IBS) és a hiányosságok megszüntetésének céljából készített Cselekvési tervet, valamint biztosítja az ezekben foglaltak végrehajtásához szükséges személyi és tárgyi feltételeket,
- gondoskodik az elektronikus információs rendszerek védelmi feladatainak és felelősségi köreinek oktatásáról, saját maga és a szervezet munkatársai elektronikus információbiztonsági ismereteinek szinten tartásáról,
- rendszeresen végrehajtott biztonsági kockázatelemzések, ellenőrzések, auditok lefolytatása révén biztosítja, hogy a szervezet elektronikus információs rendszereinek biztonsága megfeleljen a jogszabályoknak és a kockázatoknak.
- gondoskodik az elektronikus információs rendszer eseményeinek nyomon követhetőségéről,
- biztonsági esemény bekövetkezésekor minden szükséges és rendelkezésére álló erőforrás felhasználásával gondoskodik a biztonsági eseményre történő gyors és hatékony reagálásról, és ezt követően a biztonsági események kezeléséről,
- ha az elektronikus információs rendszer létrehozásában, üzemeltetésében, auditálásában, karbantartásában vagy javításában közreműködőt vesz igénybe, gondoskodik a szerződéses kötelmek teljesüléséről,

- felelős az érintetteknek a biztonsági eseményekről és a lehetséges fenyegetésekről történő haladéktalan tájékoztatásáért.

6.1.2 Információbiztonsági Felelős (IBF)

A Szervezet elektronikus információs rendszer biztonságáért felelős személy (Információbiztonsági Felelős).

Hatásköre: Az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy, közreműködik az elektronikus információbiztonsággal kapcsolatos vezetői döntések előkészítésében, kivizsgálja az informatikai rendkívüli eseményeket, elvégzi a rendszeres biztonsági ellenőrzéseket, és javaslatokat tesz a hibák kijavítására. Ezen tevékenysége során szorosan együttműködik a biztonság megvalósításában résztvevő informatikai és egyéb szakemberekkel. Jogosult bármely elektronikus információs rendszer tervezésében, fejlesztésében, létrehozásában, üzemeltetésében, auditálásában, vizsgálatában, kockázatelemzésében és kockázatkezelésében, karbantartásában vagy javításában közreműködőtől a biztonsági követelményekről tájékoztatást kérni. Ennek keretében a követelményeknek való megfelelőség alátámasztásához jogosult bekérni a közreműködői tevékenységgel kapcsolatos adatot, illetve az elektronikus információs rendszerek biztonsága tárgyában keletkezett valamennyi dokumentumot. Jogosult ezen bekért információk és dokumentumok véleményezésére, továbbá véleményezési joga van valamennyi elektronikus információbiztonságot érintő szabályzat tekintetében, továbbá minden olyan beszerzés esetében, amelynek közvetlen vagy közvetett hatása lehet az elektronikus információbiztonságra. Elektronikus információbiztonsági szakmai kérdésekben döntéshozó. Feladatai ellátása során a Főigazgatónak közvetlenül adhat tájékoztatást, jelentést.

Felelőssége: Gondoskodik az elektronikus információbiztonsági ellenőrzések módszereinek és rendszerének kialakításáról és működtetéséről, valamint részt vesz a katasztrófa-elhárítási terv összeállításában és a működésfolytonosság biztosításában. A szervezet elektronikus információbiztonságának fenntartása és folyamatos fejlesztése, az Informatikai Biztonsági Szabályzat (a továbbiakban: IBIR) eseti és rendszeres karbantartása, illetve a folyamatos szakmai kapcsolat fenntartása az érdekeltekkel.

Feladatai: Az elektronikus információs rendszer biztonságáért felelős személynek elsősorban, de nem kizárólagosan az alábbi feladatokat kell ellátnia:

- gondoskodik a szervezet elektronikus információs rendszereinek biztonságával összefüggő tevékenységek jogszabályokkal való összhangjának megteremtéséről és fenntartásáról,
- elvégzi az előző pont szerinti tevékenységek tervezését, szervezését, koordinálását és ellenőrzését,
- előkészíti a szervezet elektronikus információs rendszereire vonatkozó informatikai biztonsági szabályzatot,
- előkészíti a szervezet elektronikus információs rendszereinek biztonsági osztályba sorolását és a szervezet biztonsági szintbe történő besorolását,

- véleményezi az elektronikus információs rendszerek biztonsága szempontjából a szervezet e tárgykört érintő szabályzatait és szerződéseit,
- kapcsolatot tart a hatósággal és a kormányzati eseménykezelő központtal.
- felügyeli a beruházásokat, a fejlesztéseket és az ügyvitelt elektronikus információbiztonsági szempontból,
- munkája során felügyeli és ellenőrzi az elektronikus információbiztonsági követelmények megvalósulását, a szabályzatokban és eljárásrendekben foglaltak szabályszerű végrehajtását,
- a Szervezeti és Működési Szabályzat (a továbbiakban: SZMSZ), az ügyrend és a beosztási okirat alapján az informatikai rendszer szereplőinek jogosultságai ellenőrzésében közreműködik,
- az informatikai rendkívüli eseményeket, az esetleges rossz szándékú hozzáférési kísérletet, illetéktelen adatfelhasználást, visszaélést kivizsgálja, javaslatot tesz a Főigazgatónak a további intézkedésekre, a felelősségre vonásra,
- összehangolja a biztonságot meghatározó, befolyásoló területek tevékenységét az informatikai biztonság érdekében,
- végrehajtja és/vagy támogatja a külső és belső auditok eredményes elvégzését.

6.1.3 Szervezeti egység vezetők / Adatgazdák

Hatáskörük: A szervezeti egységükhöz tartozó rendszerekhez és adatokhoz a hozzáférési – igénylés, módosítás, visszavonás – jogosultságok elbírálása, továbbá a szervezeti egységek dolgozói felé utasítási jogkörrel rendelkeznek.

Felelősségük: A közvetlen munkatársaik körében, illetve hatáskörébe tartozó elektronikus információs rendszerekben kezelt adatok informatikai biztonsági követelményeinek betartatása és az elektronikus információbiztonsági kontrollok működtetése, a Felhasználói Felelősségvállalási Nyilatkozatok adminisztrálása. Felelősségük továbbá a területükhöz tartozó személyes adatoknak a személyes adatok kezelésére vonatkozó jogszabályok szerinti, illetve a hivatali adatoknak a vonatkozó jogszabályoknak és elvárásoknak megfelelő kezelése, valamint az ezekhez kapcsolódó hozzáférési jogosultságok szabályozása valamint felülvizsgálata.

Feladataik: Az IBSZ szabályozó dokumentumokban rögzítettek szerint.

6.1.4 Informatikai feladatok ellátásáért felelős vezető (továbbiakban: IT vezető)

Hatásköre: Utasítási joggal rendelkezik az informatikai feladatokat ellátó szervezeti egységek munkatársai felé, valamint véleményezési, tájékoztatási joga van az informatikai üzemeltetést és fejlesztést érintő stratégiai és koncepcionális kérdésekben. Jogosult továbbá az elektronikus információbiztonság megszervezésére és ellenőrzésére.

Felelőssége: Irányítási jogkörének megfelelően az informatikai feladatokat ellátó szervezeti egységek és az elektronikus információs rendszerek szabályzatoknak és előírásoknak megfelelő működtetése.

Feladatai: Az IBSZ szabályozó dokumentumokban rögzítettek szerint.

6.1.5 Rendszerüzemeltetést végző munkatársak (továbbiakban: IT üzemeltetés)

Hatáskörük: A közvetlen szakmai vezetőjük, az Informatikai feladatok ellátásáért felelős vezetőn keresztül szakmai véleményt és javaslatokat fogalmazhatnak meg a szabályozásokkal és eljárásrendekkel, valamint az alkalmazott technológiákkal kapcsolatban.

Felelősségük: Minden információs eszköz vagy eszközcsoport, információs rendszer, informatikai szolgáltatás működtetésére informatikai feladatkört ellátó munkatársat vagy alkalmazásgazdát (adminisztrátort) kell kijelölni, aki felelős a szabályzatokban és eljárásrendekben megfogalmazott követelmények szerinti üzembe helyezésért, üzemeltetésért, vagy kivonásért.

Feladataik: A szervezeti előírásoknak és a gyártói ajánlásoknak megfelelően a folyamatos működéshez szükséges beállítások elvégzése, munkafolyamatok és ellenőrzések végrehajtása, a dokumentációk naprakészen tartása, a rendszerek felhasználóinak támogatása, valamint ezen tevékenységeik előírásszerű adminisztrálása.

6.1.6 Szervezeten belüli vagy kívüli felhasználók

Hatáskörük: Jogosultak a munkavégzésükhöz szükséges és elégséges mértékű hozzáférést kapni az információs rendszerekhez, eszközökhöz, szolgáltatásokhoz.

Felelősségük: Valamennyi felhasználó felelős az átvett informatikai eszközök előírásszerű használatáért, megőrzéséért, valamint a rájuk vonatkozó előírások és biztonsági követelmények betartásáért azon adatok és információs rendszerek tekintetében, amelyeket használnak, vagy amelyekkel bármilyen módon kapcsolatba kerülnek.

Feladataik: Minden rendellenességet a szabályzatokban meghatározottak szerint haladéktalanul jelenteniük kell.

7 Biztonsági szintbe és osztályba sorolás, informatikai biztonsági kockázatelemzés

Feladat	(R)Végrehajtó	(A)Döntéshozó	(C)Konzulensek	(I)Tájékoztatandó(k)
Biztonsági szintbe és osztályba sorolás	IBF	Főigazgató	Informatikai osztály, adatgazdák	-
Kockázatelemzés	IBF	Főigazgató	Informatikai osztály, adatgazdák	-
Cselekvési terv készítése	IBF	Főigazgató	Informatikai osztály, beszállítók	-

A biztonsági szintbe és osztályba sorolást, valamint az informatikai biztonsági kockázatelemzést az IBF koordinálja az:

- Szervezeti egység vezetők / Adatgazdák,
- Informatikai biztonsági felelős,
- Informatikai feladatok ellátásáért felelős vezető,

(illetve az általuk kijelölt munkatársak) bevonásával.

A CSFK-ban az informatikai biztonság szinten tartása, valamint az elektronikus információs rendszerek biztonsági osztályba sorolása elvégzésének megalapozása érdekében az informatikai biztonsági kockázatelemzésre vonatkozó részletes eljárásokat és szabályokat a Módszertani leírás_CSFK_Kockázatkezelés_v01_20230821.docx tartalmazza.

7.1 Biztonsági szintbe és osztályba sorolás

A CSFK szervezetét, valamint a jogszabályban meghatározott szervezeti egységeit az elektronikus információs rendszerek védelmére való felkészültségük alapján biztonsági szintekbe kell sorolni a jogszabályban meghatározott szempontok szerint. A biztonsági szintbe és osztályba sorolást a szervezet vagy az elektronikus információs rendszer – illetve az abban kezelt adatok – jelentős megváltozása esetén, de legalább 3 évente felülvizsgáltatja a főigazgató, amelyet az IBF hajt végre, dokumentált módon.
A szervezet, szervezeti egységek elvárt biztonsági szintbe, valamint az elektronikus információs rendszerek elvárt biztonsági osztályba sorolását a
„CSFK_BIA_Adatvagyon_nyilvántartás_v01_20230922" nevű dokumentum tartalmazza.

A CSFK biztonsági szintje 2. - 41/2015. (VII. 15.) BM rendelet 2. melléklet 2. pontja alapján.

7.2 Cselekvési terv készítése

Amennyiben a vizsgálat – vagy felülvizsgálat – alapján meghatározott biztonsági szint alacsonyabb, mint az adott szervezetre vagy szervezeti egységre jogszabályban meghatározott biztonsági szint, vagy ha a szervezet az adott elektronikus információs rendszerére vonatkozó biztonsági osztály meghatározásánál hiányosságot állapít meg, akkor a vizsgálatot követő 90 napon belül cselekvési tervet készít az IBF az elvárt biztonsági szint elérésére vagy hiányosságok megszüntetésére.
A cselekvési terv elkészítése és folyamatos nyomon követése az IBF feladata, együttműködve az elektronikus információbiztonsági feladatok ellátásában közreműködő személyekkel, szervezeti egységekkel. A cselekvési terv elfogadása a Főigazgató feladata.

8 Az elektronikus információs rendszerek nyilvántartása

A CSFK részletes nyilvántartást vezet az általa használt rendszerelemekről, melyet az ECOSTAT nevű pénzügyi rendszerben és az IT vezető és az IBF által közösen kezelt dokumentumban tart nyilván. a Nyilvántartás naprakész és aktualizált.

A nyilvántartás tartalmazza a rendszerek:

- funkcióját,
- kinek az üzemeltetésében és melyik lokáción található,
- az érintett üzleti folyamatokat,
- bizalmasság, sértetlenség, rendelkezésre állás szerinti besorolást,
- biztonsági osztályba sorolást,
- érintett adatköröket és azok minősítéseit,
- az elvárt védelmi intézkedéseket.
- a rendszer felett felügyeletet gyakorló személy személyazonosító és elérhetőségi adatait,
- a rendszert szállító, fejlesztő és karbantartó szervezetek azonosító és elérhetőségi adatait, valamint ezen szervezetek rendszer tekintetében illetékes kapcsolattartó személyeinek személyazonosító és elérhetőségi adatait.

9 Üzletmenet-folytonosság

Az elektronikus információs rendszerek vonatkozásában kialakítandó Üzletmenet folytonosságra vonatkozó eljárásoknak az alábbi biztonsági osztályok szerint növekvő és egymásra épülő elvárásoknak kell megfelelni:

• 2-es biztonsági osztály: Üzletmenet-folytonosság terv (Business continuity plan, a továbbiakban: BCP) és Katasztrófa utáni helyreállítási terv (Disaster recovery plan, a továbbiakban: DRP) szabályzás és tervek kidolgozása és oktatása, kritikus rendszerelemek meghatározása.

9.1 Üzletmenet-folytonossági eljárásrend

A CSFK Üzletmenet-folytonosságra vonatkozó eljárásrendben szabályozza a működési folyamatait azon esetekre, mikor az azokat kiszolgáló elektronikus információs rendszerek valamilyen okból nem állnak rendelkezésre. Ezen eljárásrend kidolgozása, felülvizsgálata az IBF feladata, a jóváhagyás a *Főigazgató* felelőssége.

Az eljárásrend szabályozza:

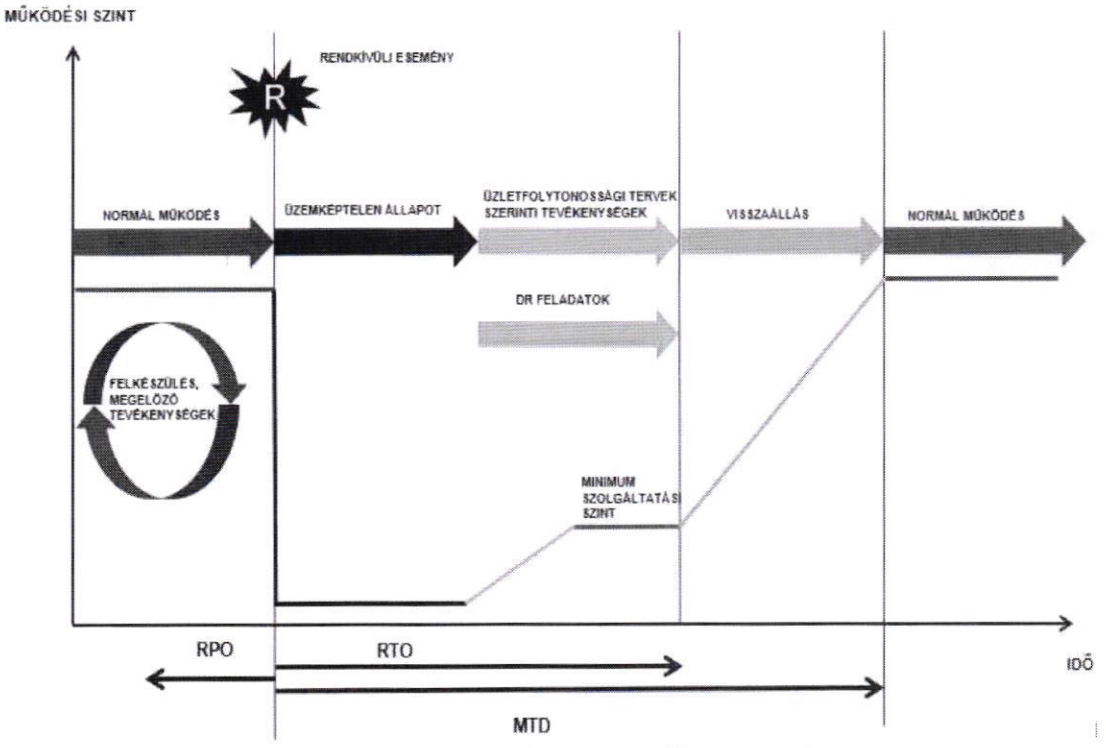
- az üzletmenet-folytonosságot sértő katasztrófahelyzetek esetén felmerülő feladatokat, és a hozzá rendelet felelősöket,
- a megfelelő kommunikációs folyamatok az elektronikus információs rendszer kiesésére, hogy kellő gyorsasággal legyen kommunikálva a szervezeteken belül és a szervezetek által kiszolgált ügyfelek felé is az ügymenet megszakadása és a megkerülő megoldás aktiválása, és
- a meghatározott követelmények és feladatok dokumentációs rendszerét.

A CSFK Katasztrófa utáni helyreállítási tervében (DRP) kidolgozta azon eljárásait, amelynek keretében az informatikai erőforrások kiesése esetén a helyreállítást megvalósítja. Ezen eljárásrend kidolgozása, felülvizsgálata az IBF feladata, a jóváhagyása a *Főigazgató* felelőssége.

A terv szabályozza:

- a helyreállítás folyamatának lépéseit, az érintett szerepköreit, felelőseit, és
- a meghatározott követelmények és feladatok dokumentációs rendszerét.

Az IBF a kritikus vagy fontos folyamatok/tevékenységek esetén, a kockázati besorolás alapján határozza meg a szolgáltatóktól elvárt üzletmenet-folytonossági és informatikai katasztrófa helyzet elhárítási terv(BCP/DRP) és a rendkívüli helyzetek kezelésére vonatkozó elvárásait és azok paramétereit.
A meghatározott folyamatokhoz/tevékenységekhez rendelt RTO/RPO/MTP értékek elvárásainál jobb értékek fogadhatóak el a szolgáltató részéről. Figyelembe kell venni az incidens/rendkívüli esemény észlelési képességből eredő észlelési idők eltérését.



RTO: Recovery Time Objective - mennyi idő alatt lehet helyreállítani a rendszert.
RPO: Recovery Point Objective - mennyi adatvesztés megengedhető.
MTP: Maximum Tolerable Period – összesen mennyi időre tolerálható a rendszer kiesése.

A releváns szolgáltató(k) a BCP/DRP teszteléseket legalább 12 havonta, de minden releváns változás esetén elvégzi és a CSFK-nak bemutatják a teszt jegyzőkönyveket, amelyre a szerződésben is garanciát kell vállalniuk. Az CSFK munkatársai, külső félként részt vehetnek a szolgáltatónál végzett BCP/DRP teszteléseken, amelyre a szerződésben audit tűrést kell vállalnia.

10 Az emberi erőforrások biztonsága

10.1 Toborzás és szerződéskötés

A felvételi folyamat során a CSFK a betöltendő szerepkör kritikusságával arányosan (kezelt informatikai erőforrások és adatkörök alapján), átvilágítja és ellenőrzi a jelentkező(ke)t az Mt.[1] adta lehetőségek erejéig.
A felvételt nyert munkavállalók esetén a munkaszerződésnek tartalmaznia kell:

- A betöltött szerepkörhöz tartozó szerepköri leírást, jogosultságokat és kötelezettségeket.

[1] 2012. évi I. törvény a munka törvénykönyvéről

- A beléptetési folyamat részeként meg kell ismernie a szerepkörhöz tartozó biztonsági előírásokat és a biztonságtudatosító tananyagot, amelyekből vizsgát is kell tennie.
- A munkavégzés és a biztonsági előírások ellenőrzésére irányuló kontroll folyamatok bemutatását.
- A fentiek megsértése esetén, milyen szankcióra számíthat (fegyelmi eljárás, rendőrségi feljelentés).
- A munkavállaló saját tulajdonú eszközére(BYOD) vonatkozó pontos előírásokat.
- A CSFK által a munkavégzéshez biztosított eszköz(ök), rendszer(ek) személyes célú használat egyértelmű engedélyezését vagy tiltását (az Mt. 11/A. § alapján).
- A kilépési folyamat bemutatását, a szerepkör és a biztonsági előírások által támasztott elvárásokat.

10.2 Beléptetés

A felvételt nyert személyek az IBF által elkészített biztonság tudatosító képzés elvégzése és eredményes visszamérését követően vehetik át a CSFK által biztosított eszközöket és kaphatnak hozzáférést a CSFK informatikai rendszereihez

A CSFK törekszik a kutatóközpont tulajdonában álló eszközök munkacélú használatára a Back Office környezetben az egyenszilárd biztonság és felügyelet kialakítása és fenntartása miatt. A Kutatók által használt rendszerekben, hálózati szegmensekben nem életszerű az ilyen biztonsági szabályozás, mert kontraproduktív és a kezelt kutatási adatok sem indokolják.

10.3 A munkaviszony során

Az informatikai biztonság tudatosítására irányuló képzéseken a jelen szabályzat alanyi hatálya fejezetben meghatározott személyeknek évente egy alkalommal kötelezően részt kell vennie. A képzést az IBF állítja össze és web alapú, e-learning vagy élő prezentáció formájában valósítja meg. A képzéseket követően az IBF visszaméri kontroll kérdések segítségével a tanultakat. A képzésen résztvevők körét és az visszamérés eredményét az IBF dokumentálja és megőrzi.

Indokolt esetben a Főigazgató utasítása alapján a biztonság tudatosság visszamérése megvalósulhat gyakorlati teszteléssel. Szimulált biztonsági incidens(ek) keretében (adathalász kampány).

10.4 Kilépés

10.4.1 Normál

A munkavállaló kilépését a HR jelzi. Az utolsó aktív munkában töltött napon az IT vezető megszünteti az összes felhasználói hozzáférést, jogosultságot, törli a központi jogosultságkezelő rendszerből(AD) és vissza veszi a kiadott eszközöket. Abban az esetben, ha engedélyezve volt a kilépő munkavállaló számára a CSFK által biztosított eszközökön a magán célú használat, úgy a munkavállalónak lehetőséget biztosít az IT vezető, hogy a saját adatait, dokumentumait kimentse egy saját adathordozóra. A kimentett adatokat az IBF ellenőrizheti, ha a munkavállaló kritikus rendszerekhez,

adatkörökhöz rendelkezett hozzáféréssel. A munkavállaló email címe megszüntetésre kerül az adatvédelmi elvárásoknak megfelelően. A munkaviszonnyal összefüggő adatait archiválják az IT vezető által kijelöl helyre. Az eszközeiről minden adatot törölnek és „alap" helyzetbe állítja az IT üzemeltetés.

10.4.2 Egyedi megállapodás

A CSFK munkatársai és kutatói részét képezik a nemzetközi kutatóhálózatoknak, így elfogadott gyakorlat, hogy a CSFK egyedi megállapodások alapján szolgáltatásokat(levelezés, web felület) biztosít a nem munkaviszonyban lévő kutatók számára. Jelen IBSZ-ben szabályozott biztonsági elvárások egyenszilárd módon vonatkoznak az ilyen esetekre is.

10.4.3 Rendkívüli (fegyelmi intézkedések)

A Főigazgató jelzése alapján az IT vezető azonnal megszünteti a felhasználó vagy szolgáltató minden hozzáférését a CSFK rendszereihez és zárolja az eszközeit. Az IBF párhuzamosan nyomozati eljárást indít, melynek során megkísérli rekonstruálni a felhasználó múltbeli aktivitásait, közben minden érdemi bizonyítékot begyűjt és dokumentál. Az IBF tájékoztatja a Főigazgatót és átadja a vizsgálatának eredményét, aki döntést hoz a további lépésekről.

11 Külső elektronikus információs rendszerek szolgáltatásai

A CSFK szerződéses kötelezettségként követeli meg, hogy az igénybe vett informatikai szolgáltatások megfeleljenek a jelen IBSZ-ban definiált követelményeknek. A megfelelő szintű védelmi intézkedések megvalósulását jogi kötelezettséggel és audit tűrési kötelezettséggel biztosítja. A kritikus rendszerek esetén, exit stratégiát dolgoz ki, amely magába foglalja a kockázatarányos anyagi kártérítési és biztosítási feltételek kikényszerítését.

A CSFK részletes nyilvántartást vezet a külső szolgáltatókról, melyben vezeti:

- az adott szolgáltató nevét , elérhetőségeit, feladatát,
- a CSFK oldali kapcsolattartó nevét, szerepét, feladatait,
- a szolgáltatás minőségére(SLA) vonatkozó külső és belső ellenőrzés módját.

A külső szolgáltatók nyilvántartása „CSFK_BIA_Adatvagyon_nyilvántartás_v01_20230922" dokumentumban érhető el.

12 Az elektronikus információs rendszer mentései

A CSFK napi rendszerességű mentéseket készít a felhasználói adatokról, ezzel 24 órás helyreállítási időre (RTO) rendezkedik be. A rendszerek mentése frissítés vagy jelentős konfigurációs változás esetén valósul meg.

A CSFK védi a mentett állományok bizalmasságát, sértetlenségét és rendelkezésre állását mind az elsődleges, mind a másodlagos tárolási helyszínen.

Megbízhatósági és sértetlenségi tesztek alkalomszerűen valósulnak meg, mert a kezelt adatkörök statikussága nem indokolja.

Helyreállítási tesztet a CSFK éves rendszerességgel végez, melynek során egy teljes rendszer és felhasználói adatvisszaállítás valósul meg.

A mentések, beleértve a kritikus információk mentését is, elkülönítve kerülnek tárolásra.

13 Fizikai biztonság

A szervezet fizikai biztonsági zónákat alakított ki. Megkülönböztet irodai környezetet és gépterem /szerverterem környezetet. Az irodai környezet védelmét csak a telephelyeken működtetett beléptető rendszer jelenti. A gépterem /szerverterem környezet védelmét biztonsági zárral védett ajtók fokozzák a beléptető rendszeren túl.
Vezetett látogatói túrák esetén a CSFK bemutatja a belső működésének publikus részét és a kutatási környezetet, az épületet, amelyben kifejti működését. Ilyen esetekben az iroda helyiségek zárása és a vendégek folyamatos felügyelete jelenti a védelmet.

14 Rendszer és szolgáltatás beszerzés

Az informatikai rendszer fejlesztésével kapcsolatos szolgáltatások és termékek beszerzése az IT vezető és az IBF bevonásával valósulhat meg kizárólag. A két szerepkör biztosítja a változások helyes megvalósítását és felkészíthetik a CSFK rendszerét a fejlesztésekre.

15 Konfigurációkezelés

Az IT vezető jóváhagyását követően lehetséges módosítani a Back Office folyamatait érintő kiszolgáló rendszerek konfigurációján. A módosításokat lehetőség szerint tesztelni kell, majd a sikeres tesztet követően kerülhet sor az élesítésre. A változásokat minden esetben precízen dokumentálni kell a végrehajtónak.
Minden új rendszer esetében a CSFK IT vezetője által jóváhagyott alapkonfigurációt kell alkalmazni és szükség esetén azon módosításokat elvégezni.
A felhasználók nem jogosultak szoftvereket telepíteni a rendszerekre, még a szabad felhasználású szoftvereket sem, mert azok valódi tartalmának ellenőrzése aránytalanául nagy költséggel járna.

A Kutatók rendszereiben nem szükséges és indokolt a konfigurációkezelés erős kontrollja.

A CSFK naprakész rendszerelem leltárt vezet, amiért az IT vezető a felelős.
Minden CSFK munkavállalóra igaz, hogy nem valósíthatja meg a szerzői[2] és szomszédos jogok megsértését és nem használhat munkavégzésével összefüggésben olyan szoftvereket, amelyek illegális forrásból lettek beszerezve.

[2] 1999. évi LXXVI. törvény a szerzői jogról

16 Szoftver életút

A CSFK által használt szoftvereket naprakész verzióban kell tartani. Rendszeresen ellenőrzi az IT üzemeltetés az elérhető frissítéseket és rendszer kritikusságától függően, teszt rendszerben végrehajtja a frissítést, majd ellenőrzést követően az éles rendszeren is végrehajtja a frissítést. Kevésbé kritikus rendszer esetén végrehajtható a frissítés az éles rendszeren is.

17 Egyedi fejlesztések

Egyedi szoftverkomponensek illesztése a CSFK rendszerébe kizárólag az IT vezető és az IBF engedélyével valósulhat meg. Az egyedi programok bevezetését megelőzően lehetőség szerint forráskód elemzés és a teszt környezetben történő viselkedés alapú vizsgálatokkal szükségesek. Az egyedi programok esetén elvárás, hogy mindenre kiterjedő rendszerdokumentáció kerüljön átadásra.

18 Adathordozók védelme

Az adathordozókkal szembeni általános védelmi intézkedések alapján a munkatársak egyedi felelősséggel tartoznak a rájuk bízott eszközök helyes használatért és az állagmegóvásért. A CSFK tevékenységével össze nem egyeztethető célokra nem szabad használni az eszközöket. A személyes és üzletileg kritikus adatokat tartalmazó adathordozókat titkosítással kell ellátni, amelynek megvalósításában az IT vezető nyújt támogatást. Az Ilyen adatokat tartalmazó adathordozókat meghibásodás esetén tilos kiadni szerviz részére vagy visszaállíthatatlan adatmegsemmisítést követően lehetséges csak.

A CSFK által használt adathordozók több csoportra oszthatók:

18.1 Központi kiszolgáló szerver infrastruktúrában használt adathordozók.

Fizikai és hálózati szeparáció révén (zárható szerverszoba), védett környezetben funkcionálnak. Meghibásuk esetén a garanciális feltételeket biztosító szervezettel kapcsolatban szerződéses garanciák biztosítanak védelmet.

18.2 Back Office környezetben használt adathordozók

Szeparált hálózati szegmensben működtetett eszközök esetén a vírusvédelmi rendszer és a felhasználók tudatos viselkedése jelentik a valós védelmet. Meghibásodásuk esetén a garanciális feltételeket biztosító szervezettel kapcsolatban szerződéses garanciák biztosítanak védelmet.

18.3 Kutatói környezet adathordozói

A kezelt adatok bizalmassága nem indokol további védelmi intézkedést, ellenben a sértetlenség és a rendelkezésre állás az adatok egyedisége miatt kiemelten fontos. Az adatok egyedisége miatt tilos törlést végrehajtani az adathordozókon.

19 Azonosítás és hitelesítés

Az IT és a Gazdasági terület kezeli a jogosultságokat. A belső levelező rendszer segítségével történnek az igénylések, amelyeket a kijelölt munkatársak végrehajtanak. A felettes és/vagy a HR területtől érkezik az első, belépéskori igény a felhasználó és a hozzá párosított jogosultságok létrehozására. Minden felhasználó egy felhasználói névvel és egy első körben generált jelszóval lesz képes belépni a CSFK rendszereibe. Az első belépést követően természetesen meg kell változtatni a kezdeti jelszót.
A felhasználók kötelesek bizalmasan kezelni a felhasználói adataikat és fél évente meg kell változtatniuk a jelszavakat.
A jelszavaknak legalább 10 karakter hosszúságúnak kell lennie, tartalmazniuk kell kis és nagy betűt, számot és speciális karaktert, a minél nehezebb visszafejthetőség érdekében.

A CSFK felhasználók az alábbi csoportra oszthatók:

19.1 Back Office felhasználók

Ők kizárólag korlátozott felhasználói jogkörrel rendelkezhetnek.

19.2 Kutatók

A munkájukból kifolyólag szükséges, hogy rendelkezzenek a kutatási területekhez kapcsolódó rendszerek esetén rendszergazdai jogkörökkel. A kutatási tevékenység során rendszereket építenek, módosítanak, amihez elengedhetetlen az emelt jogkör. Az ilyen rendszereken kezelt adatok nem indokolnak erősebb felügyeleti kontrollt.

19.3 Üzemeltetők, rendszergazdák

Két jogosultsági szinttel rendelkeznek egy korlátozott felhasználóval ,amellyel a sztenderd munkát látják el és rendelkeznek rendszergazdai jogosultságokkal, amellyel a központi rendszerek beállításait és üzemeltetését valósítják meg.

A szervezeten kívüli felhasználók hozzáférése VPN és SSH csatorna segítségével valósulhat meg az IT felügyelete mellett, ami azt jelenti ,hogy csak előzetes jelzés esetén kerül aktiválásra a VPN csatorna.

20 Hozzáférés ellenőrzése

Az IBF évente egy alkalommal ellenőrzi a jogosultság nyilvántartásban szereplő és a rendszerekben beállított jogosultságokat. Minden eltérésről jegyzőkönyvet vesz fel és kivizsgálja mi okozta az eltérést.

21 Kártékony kódok elleni védelem

Minden informatikai eszközön gondoskodni kell az aktív vírusvédelemről, ahol az értelmezhető. Fokozott védelemmel kell ellátni azon klienseket, amelyekről aktív kommunikáció zajlik a CSFK-án kívülre. A vírusvédelmi rendszer minden komponensének biztosítani kell a rendszeres frissítés lehetőségét.

22 Naplózás és elszámoltathatóság

Az Informatikai rendszerben minden eszközön (kliens számítógép, kiszolgáló számítógép, hálózati aktív eszköz, hálózati nyomtató, Active Directory), amely lehetőséget biztosít rá, aktiválni kell legalább az alap szintű naplózási funkciót. Kritikus rendszerek esetében az alap szinten túl, az IBF egyedi utasításai alapján, ennél részletesebb naplózási elvárások is elvárhatók. Minden kritikus/fontos rendszer esetén szükséges elegendő tárhelyet biztosítani a legalább 2 hét időintervallumot lefedő naplóbejegyzéseinek megőrzésére.
Jelenleg még nem elvárt a központi naplógyűjtés és elemzés, de ennek szükségessége/indokoltsága felülvizsgálat alatt van.
A kritikus/fontos rendszerek esetében elvárás, hogy az alábbi események naplózása ki legen kényszerítve technológiai módon:

- Új felhasználó létrehozása,
- felhasználó jogosultság módosulása,
- felhasználó helyes belépési folyamata,
- illetéktelen felhasználók belépési kísérlete,

A létrejött napló állományokat a rendszergazdák nem törölhetik és nem módosíthatják, azt vizsgálati/nyomozati céllal kizárólag az IBF másolhatja le.
Minden informatikai eszközön egységes rendszeridő kikényszerítése az elvárt, mert így biztosítható a napló események összefésült kiértékelése.

23 Rendszer- és kommunikáció védelem

Az informatikai rendszerek védelmét a rendszeres technológiai vizsgálatok és felhasználói monitoring rendszerek biztosítják. Az IBF-t és az IT vezetőt kell értesíteni minden rendellenes működés esetén, akik megteszik a szükséges lépéseket.

24 A határok védelme

Fejlett határvédelmi kontrollok segítségével felügyeli és ellenőrzi a külső határain történő, valamint a rendszer kulcsfontosságú belső határain történő kommunikációt. A nyilvánosan hozzáférhető rendszerelemeket fizikailag vagy logikailag alhálózatokban helyezi el, elkülönítve a belső szervezeti hálózattól. Csak az érintett szervezet biztonsági architektúrájával összhangban elhelyezett határvédelmi eszközökön felügyelt interfészeken keresztül kapcsolódik külső hálózatokhoz vagy külső elektronikus információs rendszerekhez.

25 A folyamatok elkülönítése

A CSFK elkülönített fejlesztői, teszt és éles üzemi környezetet tart fenn, melyek szeparációját hálózati szegmentálással valósítja meg.

26 Kockázat nyilvántartás

A kockázatelemzési folyamatából származó folyamatokra és rendszer elemekre vetített alap és maradvány kockázati értékek.

A nyilvántartással kapcsolatos tartalmi elvárás:

- Rendszer elem neve, azonosítója, alap és maradvány kockázati értéke
- Folyamat neve, azonosítója, alap és maradvány kockázati értéke

A kockázatelemzés és annak részletes paraméterei a **„Kockázatelemzés CSFK 2023 v10"** dokumentumban érhetők el.

27 Adatvagyon nyilvántartás – GDPR 30. cikk elvárásai alapján

Érvényre kell juttatni az adatvédelmi elvárásokat. Ehhez szükséges a kezelt adatvagyon részletes ismerete.

A nyilvántartással kapcsolatos tartalmi elvárás:

- Adatvagyon elem/adatkör neve, azonosítója
- Bizalmasság, sértetlenség, rendelkezésre állási elvárások
- Mely üzleti folyamatokban érintett
- Adatkezelő vagy adatfeldolgozói minőségben kezelt, adatfeldolgozás esetén kinek a nevében
- Adatkezelési tevékenység leírása
- Kezelés jogalapja
- Kezelés célja
- Kezelt személyes adatok kategóriái és az érintettek kategóriái
- Címzettek kategóriái
- EGT-én kívüli továbbítás
- Elvárt, kialakított védelmi intézkedések, kontrollok
- Adatkör mérete, kezelt adatok számossága
- Adatok életciklusa, tervezett tárolási idő, törlés idejének elvi meghatározása

Az adatvagyon nyilvántartás **„CSFK_BIA_Adatvagyon_nyilvántartás_v01_20230922"** dokumentumban érhető el.

28 Mellékletek

28.1 Fogalmak

(1) alapvető adat: a kutatóhely szempontjából jelentős értékkel bíró információs adatvagyonelem; alapvető adatok különösen: személyes adatok, üzleti titkok, államháztartással vagy gazdálkodással kapcsolatos adatok, továbbá azok az adatok, amelyeket a kutatóhely vezetője vagy az adatgazdák alapvető adatnak nyilvánítanak (pl.: nem nyilvános új kutatási vagy tudományos adatok);
(2) alapvető információs eszköz: olyan eszköz, amely alapvető adatot kezel, vagy alapvető információhoz biztosít hozzáférést (vagy azon eszközök, melyek az alapvető adatok információs vagyonához vannak rendelve);
(3) alapvető szolgáltatás: alapvető információs eszköz szolgáltatása;
(4) alkalmazás: meghatározott célfeladatot megvalósító szoftverekkel nyújtott szolgáltatás, amely támogatja a feladatellátással összefüggő és a szervezeti folyamatok lebonyolítását, valamint az azokhoz szükséges adatok, információk rendszerezett tárolását, feldolgozását és visszakereshetőségét;
(5) bizalmasság: az információs eszköz azon tulajdonsága, hogy a benne tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, továbbá rendelkezhetnek a felhasználásáról;
(6) biztonsági esemény: nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat, amely az információs adatvagyonban kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, és amelynek hatására az információs eszköz által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész vagy megsérül;
(7) célnak megfelelő használat biztosítása: az adat kezelésének, valamint az információs eszköz ezzel összefüggő funkciójának megvalósíthatósága;
(8) MKH Titkárság: központi finanszírozású, az MKH kutatóhálózat irányítására és működtetésére létrehozott, az Országgyűlés által alapított központi költségvetési szerv;
(9) észlelés: a biztonsági esemény bekövetkezésének felismerése;
(10) felhasználó: a kutatóhely információs adat- és eszközvagyonához hozzáférő természetes személy vagy természetes személyhez közvetlenül nem köthető gépi ügyfél (technikai felhasználó);
(11) felhasználói dokumentáció: az információs eszköz, annak eleme vagy a rendszerszolgáltatás biztonságos és hatékony használatának módszereit tartalmazó leírás;
(12) fenyegetés: olyan lehetséges művelet vagy esemény, amely sértheti az információs adatvagyon vagy az információs eszköz biztonságát, továbbá olyan mulasztásos cselekmény, amely sértheti az információs adatvagyon biztonságát;
(13) fizikai védelem: a fizikai térben megvalósuló fenyegetések elleni védelem, amelynek fontosabb részei a természeti csapás elleni védelem, a mechanikai védelem, az elektronikai jelzőrendszer, az élőerős védelem, a beléptetőrendszer, a megfigyelőrendszer, a tápáramellátás, a sugárzott és vezetett zavarvédelem, klimatizálás és a tűzvédelem;
(14) folytonos védelem: az időben változó körülmények és viszonyok között is megszakítás nélkül megvalósuló védelem;
(15) hitelesség: annak bizonyossága, hogy az adat egy elvárt forrásból származik;

(16) informatikai biztonsági incidens: olyan informatikai biztonsági esemény, amely bekövetkezése esetén az alapvető adat bizalmassága, sértetlensége vagy rendelkezésre állása sérülhet, bizalomvesztés következhet be az érintett szervezettel szemben;
(17) informatikai veszélyhelyzet (katasztrófahelyzet): olyan informatikai üzemzavar, amely nem szüntethető meg az elvárt visszaállítási időn belül, vagy nyilvánvalóan katasztrófahelyzet alakult ki (tűz, robbanás stb.);
(18) információs adatvagyon: a kutatóhely által, annak tevékenységi körében kezelt kutatási adatok, valamint a kutatóhely által, annak jogszerű működése során kezelt adatok összessége;
(19) információs eszköz: az információs eszközvagyon egy eleme; Az Ibtv. hatálya alá tartozó kutatóhelyek esetében az információs eszköz szélesebb körben értelmezendő, az elektronikus információs rendszer értendő alatta.
(20) információs eszközvagyon: a kutatóhely által vagy annak érdekében működtetett informatikai eszközök (hardver, szoftver, kommunikációs hálózat), ezen informatikai eszközök által nyújtott vagy igénybe vett szolgáltatások, valamint a kutatóhely által igénybe vett külső (pl.: felhőalapú) informatikai szolgáltatások összessége;
(21) kockázat: a fenyegetettség mértéke, amely egy fenyegetés bekövetkezése gyakoriságának (bekövetkezési valószínűségének) és az ez által okozott kár nagyságának a függvénye;
(22) kockázatelemzés: az információs adatvagyon értékének, sérülékenységének (gyenge pontjainak), fenyegetéseinek, a várható károknak és ezek gyakoriságának felmérése útján a kockázatok feltárása és értékelése;
(23) kockázatokkal arányos védelem: az információs eszköz vagy adat olyan mértékű védelme, amelynek költségei arányosak a fenyegetések által várhatóan okozható károk összesített mértékével;
(24) kutatóhely vagy kutatóhelyek: az MKH kutatóközpontjai és önálló kutatóintézetei, valamint az MKH Titkárság;
(25) kriptográfia (titkosítás): az adatok valamely matematikai algoritmus szerinti megváltoztatása abból a célból, hogy csak a jogosultak ismerhessék meg azok tartalmát; a kriptográfia valamely adat sértetlenségének és hitelességének a bizonyítására is szolgál;
(26) letagadhatatlanság: az adat származásának ellenőrizhetősége, bizonyossága;
(27) logikai védelem: az információs adatvagyonban információtechnológiai eszközökkel és eljárásokkal (programokkal, protokollokkal) kialakított védelem;
(28) meghibásodás: minden olyan felhasználói számítógépet érintő hiba vagy a hálózati eszközök, valamint központi munkaállomások rövid idejű leállása, amely számottevően nem zavarja a normális munkavégzést, és a napi üzemeltetési feladatok során gyorsan kijavítható;
(29) méretarányosság: az információbiztonsági védelmi intézkedések adott szervezet méretéhez, műszaki és gazdasági lehetőségeihez, valamint személyi erőforrásaihoz illeszkedő megvalósítása;
(30) reagálás: bekövetkezett biztonsági esemény terjedésének megakadályozására vagy késleltetésére, a további károk mérséklésére tett intézkedés;
(31) rendelkezésre állás: az információs eszközök szolgáltatásai, valamint az ezek által kezelt adatok az arra jogosultak számára a szükséges időben elérhetők;
(32) sértetlenség: az adat azon tulajdonsága, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, valamint az információs eszköz azon tulajdonsága, hogy az rendeltetésének megfelelően használható;

(33) sérülékenységvizsgálat: az információs adatvagyon gyenge pontjainak (biztonsági rések) és az ezeken keresztül fenyegető biztonsági eseményeknek a feltárása;
(34) személyes adat: az Info tv. által a személyes adatok körébe sorolt adat vagy információ;
(35) teljes körű védelem: az információs eszköz valamennyi elemére kiterjedő védelem;
(36) törzsadat: olyan kiegészítő adatok, melyek az objektumok azon tulajdonságait írják le, melyek menet közben jellemzően nem változnak;
(37) zárt védelem: az összes számításba vehető fenyegetést figyelembe vevő védelem.

28.2 Releváns jogszabályok, rendeletek, határozatok, ajánlások

- 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról
- 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről
- 2023. évi XXIII. törvény a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről
- 23/2022. (XII. 15.) elnöki határozat az MKH informatikai biztonsági keretszabályzatáról
- 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról
- AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE(2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet)
- 2012. évi C. törvény a Büntető Törvénykönyvről (Btk.)

28.3 Hatóságok

- **Szabályozott Tevékenységek Felügyeleti Hatósága (SZTFH) -2024-től**
  - 2023. évi XXIII. törvény a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről szerinti Hatóság.
- **Nemzeti Kibervédelmi Intézet – 2024-től**
  - NIS2 irányelv szerinti CSIRT
- **Nemzeti Adatvédelmi és Információszabadság Hatóság(NAIH)**
  - a 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról(Info.tv.) és a General Data Protection Regulation (GDPR) szerinti Hatóság.

29 Záró rendelkezés

Jelen szabályzatban nem szabályozott kérdések tekintetében az MKH Titkársága iránymutatásai érvényesek. Amennyiben a keretszabályzat és az Ibtv. biztonsági követelményei között eltérés tapasztalható, az Ibtv. hatálya alá tartozó kutatóhelyeknek az Ibtv. és a Bmr. rendelkezéseit kell alkalmazni.