IK4/2018/2106/1/1

MAGYAR TUDOMÁNYOS AKADÉMIA
CSILLAGÁSZATI ÉS FÖLDTUDOMÁNYI KUTATÓKÖZPONT

INFORMATIKAI BIZTONSÁGI SZABÁLYZAT

Összeállította és jóváhagyásra előterjesztette:
2018. szeptember 30.

Harnos Noémi
informatikai koordinátor

Jóváhagyom:
2018. október 19.

MAGYAR TUDOMÁNYOS AKADÉMIA

Dr. Szarka László Csaba
főigazgató

2018

Bevezető

A Neumann János Számítógéptudományi Társaság „IT Biztonság mindenkinek" c. kiadványa (http://njszt.hu/sites/default/files/NJSZT_IT_Biztonsag_kozerthetoen_v3.pdf-n) alapján megadjuk négy, sokszor nem egyértelműen használt fogalom definícióját.
Adatbiztonság: a számítógépes rendszerekben tárolt adatok bizalmasságának, sértetlenségének és rendelkezésre állásának megteremtése (nem foglalkozik az alkalmazások és a kisegítő berendezések – pl. szünetmentes áramforrás – biztonságával)
Informatikai biztonság: az információs rendszerekben tárolt adatok és a feldolgozáshoz használt hardveres és szoftveres erőforrások biztonságára vonatkozik.
Információbiztonság: tények, utasítások, elképzelések emberi vagy gépi úton formalizált, továbbítási, feldolgozási vagy tárolási célú reprezentánsai bizalmasságának, sértetlenségének és rendelkezésre állásának megteremtése.
Adatvédelem: személyes adatok jogszerű kezelését, az érintett személyek védelmét biztosító alapelvek, szabályok, eljárások, adatkezelési eszközök és módszerek összessége.

Az eszményi Informatikai Biztonsági Szabályzat kiterjed mindenre, amit az NJSZT „IT Biztonság mindenkinek" c. (http://njszt.hu/sites/default/files/NJSZT_IT_Biztonsag_kozerthetoen_v3.pdf-n elérhető) kiadványa tartalmaz, úgymint: *Biztonsági alapfogalmak* (Biztonság, Kibertér, Nemzeti Kibervédelmi Intézet, A biztonság koncepcionális megközelítése, Információkritériumok), *Információrendszerek* (Hardveres infrastruktúra, Alkalmazások, szolgáltatások [Ismeretszerzés és kapcsolatteremtés interneten, Elektronikus ügyintézés] Számítógép hálózatok), *Fenyegetések, támadások* (Rosszindulatú szoftverek, Jellemző támadási formák és módszerek), *Fenyegetettségi és támadási trendek* (Személyes adatokat érintő incidensek, E-mail fenyegetettségek, kártékony programok és botnetek, Mobileszközök fenyegetettségei, Zsarolóvírusok (Ransomware), *A védelem kialakítása* (Felhasználók felelőssége az incidensek, biztonsági események során, A bizalmasság [Bizalmasság az operációs rendszerben, Merevlemezek és USB-lemezek titkosítása, Titkosítás irodai programcsomagokban, Bizalmasság tömörített állományoknál], Hálózat és bizalmasság [Hozzáférés-védelem, jelszavak, hitelesítés, WiFi eszköz biztonsági beállításai, E-mail, Azonnali üzenetküldés, Tűzfalak], Adatvédelmi megfontolások [Védelem böngészés közben, A látogatott oldalak biztonsága, Aktív tartalmak és a biztonság, A böngészőben tárolt adatok biztonsága, Bizalmassági eszközök közösségi oldalakon, Az adatok végleges törlése], A sértetlenségről [Digitális aláírás, Kivonatok (hash-ek)], A rendelkezésre állás megteremtése [Fájlok biztonsági mentése, Védelem az áramellátás hibái ellen], Komplex megközelítést igénylő fenyegetettségek és védelmi megoldások [Végpontvédelem és vírusvédelem, Biztonságos Internet bankolás, Biztonságos bankkártya használat – internetes fizetés, Internetes zaklatás]).

A gyakorlatban az Informatikai Biztonsági Szabályzat nem tud teljes lenni. Az MTA CSFK Informatikai Biztonsági Szabályzata a kutatóközpont informatikusai által javasolt kérdésekre korlátozódik.

Adatnak tekinthetők a számokkal leírható dolgok, melyek számítástechnikai eszközökkel rögzíthetők, feldolgozhatók, és megjeleníthetők. Gyakorlatilag bármilyen jel potenciálisan: adat. Ebben a szabályzatban „adat"-nak a magyar jogi gyakorlat szerinti adat-definíciót tekintjük. A szabályzatban az ún. „védelmet élvező", „védendő" adatok közé a kutatási megfigyelési adatok csak akkor tartoznak bele, ha az intézetigazgató azt kifejezetten kéri.

Tartalomjegyzék

BEVEZETŐ

IT biztonság

INFORMATIKAI BIZTONSÁGI SZABÁLYZAT

A Magyar Tudományos Akadémia Csillagászati és Földtudományi Kutatóközpont (továbbiakban Kutatóközpont) Informatikai Biztonsági Szabályzatát (továbbiakban IBSZ) az információs önrendelkezési jogról és információszabadságról szóló 2011. évi CXII. törvény (Infotv.) vonatkozó rendelkezéseire figyelemmel – az informatikai hálózat üzemeltetésének, használatának, továbbá a megfelelő szintű informatikai biztonsági védelem biztosíthatóságának érdekében a következők szerint határozom meg:

1. Az Informatikai Biztonsági Szabályzat célja

Az IBSZ alapvető célja, hogy az informatikai rendszer alkalmazása során biztosítsa a Kutatóközpontnál az adatvédelem alkotmányos elveinek, az adatbiztonság követelményeinek az érvényesülését, s megakadályozza a jogosulatlan hozzáférést, az adatok megváltoztatását és jogosulatlan nyilvánosságra hozatalát. Az IBSZ alapvető célja továbbá az informatikai infrastruktúra bizalmasságának, sértetlenségének és folyamatos rendelkezésre állásának és funkcionalitásának a fenntartása.

Az IBSZ célja továbbá:

- a titok-, munka-, vagyon- és tűzvédelemre vonatkozó védelmi intézkedések betartása,
- az üzemeltetett informatikai rendszerek rendeltetésszerű használata,
- az üzembiztonságot szolgáló karbantartás és fenntartás,
- az adatok informatikai feldolgozása és azok további hasznosítása során az illetéktelen felhasználásból származó hátrányos következmények megszüntetése, illetve minimális mértékre való csökkentése,
- az adatállományok tartalmi és formai épségének megőrzése,
- az alkalmazott programok és adatállományok dokumentációinak nyilvántartása,
- a munkaállomásokon lekérdezhető adatok körének meghatározása,
- az adatállományok biztonságos mentése,
- az informatikai rendszerek zavartalan üzemeltetése,
- a feldolgozás folyamatát fenyegető veszélyek megelőzése, elhárítása,
- az adatvédelem és adatbiztonság feltételeinek megteremtése.

A szabályzatban meghatározott védelemnek működnie kell az informatikai rendszerek fennállásának egész időtartama alatt a megtervezésüktől kezdve az üzemeltetésükön keresztül a felhasználásig.

A jelen IBSZ az adatvédelem általános érvényű előírását tartalmazza, meghatározza az adatvédelem és adatbiztonság feltételrendszerét.

2. Az Informatikai Biztonsági Szabályzat hatálya

2.1. Személyi hatálya

Az IBSZ személyi hatálya a Kutatóközpont valamennyi fő- és részfoglalkozású dolgozójára, a Kutatóközpontban tanuló, dolgozó egyetemi hallgatókra, együttműködő kutatókra, illetve az informatikai eljárásban résztvevő más szervezetek dolgozóira egyaránt kiterjed.

2.2. Tárgyi hatálya kiterjed

- a védendő adatok teljes körére, felmerülésük és feldolgozási helyüktől, idejüktől és az adatok fizikai megjelenési formájától függetlenül,
- a Kutatóközpont tulajdonában lévő (=leltárában szereplő), illetve az általa bérelt valamennyi informatikai berendezésre, valamint a gépek műszaki dokumentációira,
- az informatikai folyamatban szereplő összes dokumentációra (fejlesztési, szervezési, programozási, üzemeltetési),
- a rendszer- és felhasználói programokra,
- az adatok felhasználására vonatkozó utasításokra,
- az adathordozók tárolására, felhasználására.

A kutatási megfigyelési adatok abban az esetben kerülnek a védendő adatok közé, ha erre vonatkozóan az intézetigazgató írásbeli nyilatkozatot tesz.

3. Az adatkezelés során használt fontosabb fogalmak

Az adatkezelés során használt fontosabb fogalmak:

Adatbiztonság: Az adatok jogosulatlan megszerzése, módosítása és tönkretétele elleni műszaki és szervezési intézkedések és eljárások együttes rendszere.
Adatfeldolgozás: Az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől, feltéve hogy a technikai feladatot az adatokon végzik.
Adatgazda: Felelős az általa kezelt adatokért, továbbá jogosult az adatok minősítése vagy osztályba sorolása elvégzésére.
Adatkezelés: Az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése, megsemmisítése, valamint az adatok további felhasználásának megakadályozása, az adatokkal kapcsolatos fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők rögzítése.
Adatkezelő: Az a személy, aki vagy amely önállóan vagy másokkal együtt az adatok kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az általa megbízott adatfeldolgozóval végrehajtatja.
Aktív hálózati eszköz: Kapcsolók (switch-ek), forgalomirányítók (router-ek), vezeték nélküli hozzáférési pontok (Acces Pointok) és egyéb eszközök, amelyek segítségével a hálózat folyamatos üzemvitele biztosítható (bridge-ek, tűzfalak).
Bizalmasság: Az információ azon jellemzője, hogy csak egy előre meghatározott felhasználói kör (jogosultak) részére hozzáférhető, mindenki más számára titok. A bizalmasság elvesztése esetén a bizalmas információ arra jogosulatlanok számára is ismertté, hozzáférhetővé válik.
Biztonság: Az informatikai rendszerekben olyan előírások és szabványok betartását jelenti, amelyek a rendszer működőképességét, az információk rendelkezésre állását, sértetlenségét, bizalmasságát és hitelességét erősítik.
BYOD (Bring Your Own Device – BYOD): Saját mobileszközök (különösen: notebookok, tabletek, okos telefonok) munkahelyi környezetben való használata.

Csomópont: A szerver feladatokat ellátó és aktív eszközök csoportja az informatikai szolgáltatások ellátására.
Felhasználó: Az a természetes személy, aki a kutatóközponti informatikai infrastruktúrát használja.
Felhasználói azonosító: A kutatóközponti címtárban tárolt egyedi azonosításra szolgáló rövid karaktersorozat, amely általában a felhasználó teljes nevéből képződik.
Domain név: Tartománynév (műszaki azonosító), amely elsősorban a könnyebb megjegyezhetősége miatt, az internetes kommunikációhoz nélkülözhetetlen Internet cím tartományok (IP címek) helyett használatos. Az Internet egy meghatározott részét, tartományát egyedileg leíró megnevezés, a számítógépek (kiszolgálók) azonosítására szolgáló névtartomány (különösen: tf.hu).
DNS (Domain Name System): Az internet neveket és címeket egymáshoz rendelő adatbázis, amely általában külön kiszolgáló gépen fut.
Felhőszolgáltatás, felhőszolgáltató: A feladatvégzéshez használt adatállományok, programok, szolgáltatások, stb. fizikailag nem a felhasználó számítógépén, hanem az interneten, egy szolgáltatónál találhatók. Az adatok (e-mailek, címjegyzékek, naptárbejegyzések, és kedvenc linkek) felhőben való tárolásának előnye, hogy bárhonnan könnyen elérhetők, és akkor sem vesznek el, ha a felhasználó számítógépe tönkremegy.
Hálózat: Felhasználói számítógépek, illetve szerverek közötti adatátvitelt biztosító passzív elemekből és aktív eszközökből álló infrastruktúra.
Hálózati rendszergazda: A hálózati hardverrendszer hardver és szoftver üzemeltetője.
Központi címtár: A Kutatóközpont foglalkoztatottjainak felhasználói adatait tároló adatbázis.
Közérdekű adat: ld. Adatvédelmi és Adatbiztonsági Szabályzat
Közérdekből nyilvános adat: ld. Adatvédelmi és Adatbiztonsági Szabályzat
Megtévesztés (Social engineering): Megtévesztés, az emberek bizalomra való hajlamának manipulatív kihasználása, információgyűjtés számítógépes rendszerekbe történő behatolás érdekében.
Mobil eszközök: Notebook, netbook, tablet, palmtop, mobiltelefon.
Munkaállomás: A felhasználó rendelkezésére bocsátott számítástechnikai eszköz, amely alapvetően hordozható vagy asztali számítógépből és a hozzá tartozó kiegészítőkből, illetve más, a hálózathoz vagy a munkaállomáshoz csatlakoztatható számítástechnikai eszközökből (különösen: mikrofon, kamera, scanner, tablet, telefon stb.) állhat.
Passzív eszközök: Hálózati kábelezés, rendezők és csatlakozók.
Rendelkezésre állás: Annak biztosítása, hogy a szükséges információ a szükséges időben az arra jogosultak számára meghatározott formában hozzáférhető és elérhető legyen.
Szerverszoba: Fokozottan védett, naplózott bejutású, klimatizált, zárt helyiség, ahol a folyamatos működés feltételei az informatikai erőforrások számára biztosítottak.
Tűzfal: Olyan kiszolgáló eszköz (számítógép vagy program), amelyet a lokális és a külső hálózat közé, a csatlakozási pontra telepítenek annak érdekében, hogy az illetéktelen behatolásoknak ezzel is elejét vegyék. Ezzel együtt lehetővé teszi a kifelé irányuló forgalom, tartalom ellenőrzését is.
VLAN: A hálózat egy – a feladatoknak megfelelő, logikailag elkülönülő – meghatározott része. A VLAN-ok biztonsági feladatot is ellátnak, mivel elválasztják egymástól a részhálózatokat ezzel biztosítva, hogy sérülés, vagy támadás esetén csak az adott részterületre korlátozódjék az esetleges kár.
VPN szolgáltatás: Speciális hálózati elérés, amely az MTA CSFK hálózatához titkosított, és hitelesített kapcsolatot tesz lehetővé a világ bármely részéről. Két típusa létezik: felhasználói VPN (munkatársak távoli kapcsolódására), illetve siteto-site VPN (távoli telephelyek kapcsolódására).
WEB adminisztrátor: A honlap felügyeletét ellátó személy.
WiFi, WLAN: Szabványos vezeték nélküli adatátviteli technika.

Ld. még a mindenkor érvényes Adatvédelmi és Adatbiztonsági Szabályzatot.

Az adatokat védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, nyilvánosságra hozás vagy törlés, illetőleg sérülés vagy a megsemmisülés ellen.

4. Az Informatikai Biztonsági Szabályzat biztonsági fokozata

A Kutatóközpont alapbiztonsági fokozatba tartozik, általános informatikai feldolgozást végez.

5. Kapcsolódó szabályozások

Az IBSZ-t az alábbiakban felsorolt előírásokkal összhangban kell alkalmazni:

- Szervezeti és Működési Szabályzat,
- Adatvédelmi és Adatbiztonsági Szabályzat (a személyes adatok védelméről és biztonságáról szóló szabályzat),
- Bizonylati rend,
- Iratkezelési szabályzat,
- Eszközök és források leltárkészítési és leltározási szabályzata,
- Felesleges vagyontárgyak hasznosításának és selejtezésének szabályzata,
- Számviteli Politika,
- Számlarend,
- Belső kontrollrendszer működési szabályzata,
- Tűzvédelmi szabályzat,
- Munkaerő-felvétel eljárásrendje
- A Kormányzati Informatikai Fejlesztési Ügynökség Nemzeti Információs Infrastruktúra Fejlesztési Program Felhasználói Szabályzata: https://niif.hu/sites/default/files/kifu_niif_program_felhasznaloi_szabalyzat.doc

6. Védelmet igénylő, az informatikai rendszerre ható elemek

Az informatikai rendszer egymással szervesen együttműködő és kölcsönhatásban lévő elemei határozzák meg a biztonsági szempontokat és védelmi intézkedéseket.
Az informatikai rendszerre az alábbi tényezők hatnak:

- a környezeti infrastruktúra,
- a hardver elemek,
- az adathordozók,
- a dokumentumok,
- a szoftver elemek,
- az adatok,
- a rendszerelemekkel kapcsolatba kerülő személyek.

6.1. A védelem tárgya

A védelmi intézkedések kiterjednek:

- az alkalmazott hardver eszközökre és azok működési biztonságára,
- az informatikai eszközök elhelyezésére szolgáló helyiségekre,
- az informatikai eszközök üzemeltetéséhez szükséges okmányokra és dokumentációkra,

- az adatokra és adathordozókra, a megsemmisítésükig, illetve a törlésre szánt adatok felhasználásáig,
- az adatfeldolgozó programrendszerekre, valamint a feldolgozást támogató rendszer szoftverek tartalmi és logikai egységére, előírásszerű felhasználására, reprodukálhatóságára,
- a személyhez fűződő és vagyoni jogokra.

6.2. A védelem eszközei

A mindenkori technikai fejlettségnek megfelelő műszaki, szervezeti, programozási, jogi intézkedések azok az eszközök, amelyek a védelem tárgyának különböző veszélyforrásokból származó kárt okozó hatásokkal, szándékokkal szembeni megóvását elősegítik, illetve biztosítják.

7. Az informatikai rendszer üzemeltetésének, fejlesztésének, védelemének felelősei

Az informatikai rendszer üzemeltetésének, fejlesztésének, védelemének felelősei – továbbiakban informatikusok - az informatikai koordinátor és a rendszergazdák.

7.1. Az informatikai koordinátor feladatai:

A kutatóközponti informatikusok szakmai feletteseként működteti és fejleszti a kutatóközpont informatikai rendszereit. Feladatainak részletes leírását a munkaköri leírás tartalmazza.

7.2. A rendszergazda feladatai:

- a rendszergazda a saját feladatkörébe tartozó rendszert felügyeli,
- felelős az informatikai rendszerek üzembiztonságáért, szerverek adatairól biztonsági másolatok készítéséért és karbantartásáért,
- gondoskodik a rendszer kritikus részeinek újraindíthatóságáról, illetve az újraindításhoz szükséges paraméterek reprodukálhatóságáról,
- feladata a védelmi eszközök működésének, szerviz ellátás biztosításának folyamatos ellenőrzése,
- felelős az informatikai rendszer hardver eszközeinek karbantartásáért, és időszakos hardver tesztjeiért,
- nyilvántartja a beszerzett, illetve üzemeltetett hardver és szoftver eszközöket,
- ellenőrzi a vásárolt szoftverek helyes működését, vírusmentességét, a használat jogszerűségét,
- gondoskodik a folyamatos vírusvédelemről,
- a vírusfertőzés gyanúja esetén gondoskodik a fertőzött rendszerek izolálásáról és vírusmentesítéséről,
- folyamatosan figyelemmel kíséri és vizsgálja a rendszer működésére és biztonsága szempontjából a lényeges paraméterek alakulását,
- ellenőrzi a rendszer adminisztrációját,
- tevékenységéről rendszeresen beszámol az informatikai koordinátornak.

8. Az Informatikai Biztonsági Szabályzat alkalmazásának módja

Az IBSZ megismerését az informatikusok oktatás formájában segítik. Az oktatás formája lehet élő előadás, személyes tájékoztatás vagy írásos – email vagy belső honlapra feltett tájékoztató – formátumú. A Kutatóközpontban évente legalább egy tájékoztatót kell tartani a felhasználók számára.

8.1. Az Informatikai Biztonsági Szabályzat karbantartása

Az IBSZ-t az informatikában illetve a Kutatóközpontban bekövetkező változások miatt időközönként aktualizálni kell.
Az IBSZ folyamatos karbantartása az informatikai koordinátor feladata.

8.2. A védelmet igénylő adatok és információk besorolása, hozzáférési jogosultság

- Az adatok és információk jelentőségük és bizalmassági fokozatuk szerinti osztályozását, az adatok kezelését a mindenkor hatályos MTA CSFK Adatvédelmi és Adatbiztonsági Szabályzata írja le.
- Az informatikai feldolgozás során keletkező adatok védelmi szintjét annak a szervezeti egységnek a vezetője határozza meg, amelynek védelme az érdekkörébe tartozik.
- A hivatali titoknak minősülő adatok feldolgozásakor meg kell határozni írásban és névre szólóan a hozzáférési jogosultságot.
- Alapelv, hogy mindenki csak ahhoz az adathoz juthasson hozzá, amire a munkájához szüksége van.
- A védett adatokhoz való hozzáférést a tevékenység naplózásával dokumentálni kell, ezáltal bármely számítógépen végzett tevékenység – adatbázisokhoz való hozzáférés, a fájlba vagy külső adathordozóra történő mentés, a rendszer védett részeibe történő illetéktelen behatolási kísérlet – utólag visszakereshető.
- A naplófájlokat rendszeresen át kell tekinteni, s a jogosulatlan hozzáférést vagy annak a kísérletét az intézmény vezetőjének azonnal jelenteni kell.
- A naplófájlok áttekintése és értékelése az informatikusok feladata.
- A titkot képező adatok védelmét, a feldolgozás – az adattovábbítás, a tárolás - során az operációs rendszerben és a felhasználói programban alkalmazott logikai matematikai, illetve a hardver berendezésekben kiépített technikai megoldásokkal is biztosítani kell (szoftver, hardver adatvédelem). A Gazdasági Igazgatóság belső hálózatának védelmét az 1. sz. melléklet írja le.

9. Az informatikai eszközbázist veszélyeztető helyzetek

Az információk előállítására, feldolgozására, tárolására, továbbítására, megjelenítésére alkalmas informatikai eszközök fizikai károsodását okozó veszélyforrások ismerete azért fontos, hogy felkészülten, megelőző intézkedésekkel a veszélyhelyzetek elháríthatók legyenek.

9.1. Környezeti infrastruktúra okozta ártalmak

Elemi csapás:
- földrengés,
- árvíz,
- tűz,
- villámcsapás, stb.

Környezeti kár:
- légszennyezettség,

- nagy teljesítményű elektromágneses térerő,
- elektrosztatikus feltöltődés,
- a levegő nedvességtartalmának felszökése vagy leesése,
- piszkolódás (pl. por),
- mechanikai sérülések, rágcsálók, ízeltlábúak – vezetékek átrágása, érintkezési zavarok, zárlat.

Közüzemi szolgáltatásban bekövetkező zavarok:

- feszültség-kimaradás,
- feszültségingadozás,
- elektromos zárlat,
- csőtörés.

9.2. Emberi tényezőre visszavezethető veszélyek

Szándékos károkozás:

- behatolás az informatikai rendszerek környezetébe,
- illetéktelen hozzáférés (adat, eszköz),
- adatok- eszközök eltulajdonítása,
- rongálás (gép, adathordozó),
- megtévesztő adatok bevitele és képzése,
- zavarás (feldolgozások, munkafolyamatok),
- elbocsátott dolgozó „bosszúja".

Nem szándékos, illetve gondatlan károkozás:

- figyelmetlenség (ellenőrzés hiánya),
- szakmai hozzá nem értés,
- a gépi és eljárásbeli biztosítékok beépítésének elhanyagolása,
- a megváltozott körülmények figyelmen kívül hagyása,
- illegális másolattal vírusfertőzött adathordozó behozatala,
- biztonsági követelmények és gyári előírások be nem tartása,
- adathordozók meghibásodása (rossz tárolás, kezelés),
- a karbantartási műveletek elmulasztása.

A szükséges biztonsági-, jelző és riasztó berendezések karbantartásának elhanyagolása veszélyezteti a feldolgozás folyamatát, alkalmat ad az adathoz való véletlen vagy szándékos illetéktelen hozzáféréshez, rongáláshoz.

10. Az adatok tartalmát és az informatikai feldolgozás folyamatát érintő veszélyek

Tervezés és előkészítés során előforduló veszélyforrások

- a rendszerterv nem veszi figyelembe az alkalmazott hardver lehetőségeit,
- hibás adatrögzítés, adatelőkészítés, az ellenőrzési szempontok be nem tartása.

A rendszerek megvalósítása során előforduló veszélyforrások

- hibás adatállomány működése,
- helytelen adatkezelés,
- programtesztelés elhagyása.

A működés és fejlesztés során előforduló veszélyforrások

- emberi gondatlanság,
- szervezetlenség,
- képzetlenség,
- szándékosan elkövetett illetéktelen beavatkozás,
- illetéktelen hozzáférés,
- üzemeltetési dokumentáció hiánya.

11. Az informatikai eszközök és környezetük védelme

11.1 Szerverek

- a szervereket szerverszobában kell tartani,
- a szerverszobát a legbiztonságosabb, legvédettebb területre kell telepíteni,
- a lehető legkevesebb nyílászáróval kell rendelkeznie,
- a szerverszobát az állandó hőmérséklet és páratartalom fenntartása érdekében lehetőség szerint klimatizálni kell,
- váratlan áramkimaradás, feszültségingadozás esetére a szervereket intelligens szünetmentes tápegységgel (UPS) kell ellátni, mellyel az áramellátás folyamatosságát biztosítani lehet,
- az UPS-re csatlakoztatott szervereket hosszabb áramszünet esetén automatikusan ki kell kapcsolni,
- a szerverszoba külső és belső helyiségeit biztonsági zárakkal kell felszerelni,
- a szerverszobába való be- és kilépés rendjét szabályozni kell (2. sz. melléklet),
- a szerverszobában csak az illetékes dolgozók tartózkodhatnak,
- a szerverszobába történő illetéktelen behatolás tényét az intézmény vezetőjének azonnal jelenteni kell.

11.2 Munkaállomások

- Munkaállomást csak zárható helyiségben szabad tárolni. Ha a helyiségben nem tartózkodik senki, az ajtót bezárva kell tartani.
- Az informatikai eszközöket csak a kijelölt dolgozók használhatják.
- Az informatikai eszközök rendeltetésszerű használatáért a felhasználó felelős.

11.3 Adathordozók

- Az adathordozókat könnyen tisztítható, jól zárható szekrényben kell elhelyezni úgy, hogy tárolás közben ne sérüljenek, károsodjanak,
- az adathordozókat a gyors hozzáférés érdekében azonosítóval kell ellátni,
- a használni kívánt adathordozót (CD, DVD, külső diszk stb.) a tárolásra kijelölt helyről kell kivenni, és oda is kell visszahelyezni,
- adathordozót más szervezetnek átadni csak engedéllyel szabad,
- a munkák befejeztével a használt berendezést és környezetét rendbe kell tenni.

11.4 Számítógépes hálózat

- A hálózat üzemeltetéséért a rendszergazda felelős.

- A hálózat bővítésekor, fejlesztésekor felmerülő munkákat a rendszergazda végzi, vagy vezetője egyetértésével, szakértő céggel végezteti.
- A hálózat aktív eszközeit a rendszergazda tartja karban. Az aktív eszközökhöz hozzányúlni, azokat felszültség mentesíteni és újraindítani, a hálózati csatlakozásokat megbontani csak a rendszergazda vagy az általa megbízott személyek jogosultak.
- Tilos a hálózati rendszergazda engedélye nélkül hálózati eszközt a hálózatra csatlakoztatni.
- A hálózati csatlakozáshoz szükséges hálózati címek felett a rendszergazda rendelkezik. Tilos önkényesen hálózati címeket megadni vagy megváltoztatni. Szükség esetén a rendszergazda jogosult a már kiadott hálózati címek visszavonására vagy megváltoztatására.
- A rendszergazda bármikor jogosult ellenőrizni a Kutatóközpont eszközeinek szabályos használatát. Az ellenőrzés tényét nem köteles előre bejelenteni, de törekednie kell arra, hogy lehetőség szerint ne zavarja a napi munkamenetet.

11.5 Rosszindulatú számítógépes programok elleni védelem

A rosszindulatú számítógépes programok (malware) közé tartoznak a vírus, féreg, kémprogram (spyware), zsarolóprogram (ransomware), agresszív reklámprogram (adware), és a rendszerben láthatatlanul megbúvó, egy támadónak emelt jogokat biztosító eszköz (rootkit). A mindennapokban elterjedt „vírus" megnevezés ma már az összes rosszindulatú programra vonatkozik.

A szerverek és munkaállomások védelmére az alábbi szabályokat kell betartani:

- Minden munkaállomásra és szerverre vírusellenőrző szoftvert kötelező telepíteni.
- A vírusellenőrző programnak minden újonnan érkezett állománnyal kapcsolatos fájlművelet esetén meg kell vizsgálni az adathordozó tartalmát. Ha az adathordozón a vírusellenőrző program vírust talált, nem engedhet másolást, futtatást, amíg a vírusoktól nem mentesítik az adathordozót.
- Biztosítani kell a vírusvédelmet ellátó programok, valamint a vírusok adatait tartalmazó állományok rendszeres, gyártó által kibocsátott verziók telepítésével történő mielőbbi frissítését.
- A kizárólag tudományos számítások céljából működő kiszolgáló munkaállomásokra és szerverekre, illetve az adatgyűjtő eszközökkel közvetlenül kapcsolatban álló adatfeldolgozó számítógépekre a számolás és az adatfeldolgozás lassulása miatt eltekintünk a vírusirtó használatától, amennyiben azokon a felhasználói hozzáférés és internet elérés korlátozott.

Teendők fertőzés esetén:

- Azonnal tájékoztatni kell a vírusvédelemért felelős személyt (rendszergazdát) a fertőzésről vagy annak gyanújáról.
- Az ethernet hálózati csatlakozót ki kell húzni vagy a vezeték nélküli csatlakozást le kell tiltani.
- A számítógépet újra kell indítani egy előkészített, vírusmentes, a használt operációs rendszert és a vírusvédelmi program legfrissebb változatát tartalmazó lemezről. Ha ez nem lehetséges, akkor védett módban kell újraindítani a gépet csak a legszükségesebb szolgáltatásokkal – hálózati kapcsolat nélkül.
- Elindítjuk a vírusvédelmi szoftvert, és megszüntetjük a vírusfertőzést. Ez történhet elsődlegesen fertőzött állomány javításával, ha erre nincs lehetőség, a fertőzött állomány törlésével.
- A víruskeresést addig kell folytatni, amíg a víruskereső program az összes állományt le nem ellenőrizte, és nem talált több fertőzött állományt.

- Ezek után a rendszer a szokott módon újraindítható.

11.6 Tűzvédelem

- A szerverszoba a „D" tűzveszélyességi osztályba tartozik, amely mérsékelt tűzveszélyes üzemet jelent.
- A tűzvédelem feladatait, sajátos előírásokat a szerverszobára és hálózatra vonatkozóan az Kutatóközpont Tűzvédelmi szabályzata tartalmazza.
- A menekülési útvonalak szabadon hagyását minden körülmények között biztosítani kell.
- A szerverszobában tilos gyúlékony anyagot tárolni.
- A szerverszobában dohányozni tilos!
- A Kutatóközpont azon helyiségeiben, ahol informatikai eszközöket használnak vagy tárolnak, a tűzvédelmet a Tűzvédelmi szabályzat előírásainak megfelelően kell biztosítani.
- A nagy fontosságú, pl. törzsadat-állományokat, mérési adatokat 2 példányban kell őrizni, lehetőséget kell teremteni a központi rendszerekről földrajzilag elkülönített megbízható helyen – de legalább másik épületben – biztonsági mentés készítésére. Ezen adatállományok kijelölése annak a vezetőnek a feladata, akinek a szervezeti egysége ezekkel az adatokkal dolgozik.

12. Az informatikai rendszer alkalmazásánál felhasználható védelmi eszközök és módszerek

12.1. A szerverszoba védelme

Elemi csapás, rongálás stb. esetén a hálózati és számítóközpontban bekövetkezett részleges vagy teljes károsodáskor az alábbiakat kell sürgősen elvégezni:

- a még használható anyag mentése,
- biztonsági mentésekről, háttértárakról a megsérült adatok visszaállítása,
- új adatfeldolgozási helyiségek kialakítása,
- archivált anyagok (ill. eszközök) használatával folytatni kell a feldolgozást.

12.2. Hardver védelem

- A berendezések hibátlan és üzemszerű működését biztosítani kell.
- A működési biztonság megóvását jelenti a szükséges alkatrészek beszerzése.
- Az üzemeltetést, karbantartást és szervizelést rendszergazdák végzik, illetve rendelik meg szakértő vállalkozástól.
- A karbantartási munkákat tervezetten, körültekintően és gondosan kell elvégezni.
- A munkák szervezésénél figyelembe kell venni:
    - a gyártó előírásait, ajánlatait,
    - a tapasztalatokat,
    - a hardver tesztek által feltárt hibákat.
- Alapgép szétbontását csak a rendszergazda engedélyével lehet elvégezni.

12.3. Számítógépes hálózat védelme

A rendszergazda – annak érdekében, hogy a Kutatóközpont számítógépes rendszere károkozás ellen védett legyen – a főigazgató jóváhagyásával jogosult arra, hogy:

- bárkit a hálózat használatából kizárjon károkozásra utaló alapos gyanú felmerülése esetén,

- megtekintsen, átmásoljon, megváltoztasson, vagy töröljön bármely fájlt, amely kapcsolatban van a rendszer vagy a hálózat jogosulatlan használatával,
- ellenőrizze a számítógépes rendszereket, helyi hálózatokat és a Kutatóközponti hálózatot, indokolt esetben leállítsa vagy átkonfigurálja, illetve bármely egyéb szükséges intézkedést megtegyen a működés biztosításához.
- A vírusos, a hálózat biztonságát veszélyeztető email-ek bejutása ellen spam- és egyéb levélszűrők üzemeltetésére, bizonyos csatolmány típusok letiltására.
- A legmagasabb szintű védelem érdekében szigorú tűzfal szabályok beállítására.
- A felhasználó a tűzfalon kívül eső hálózatról VPN-nel kizárólag a rendszergazda által előírt szabályokkal konfigurált és a munkaállomásra telepített védelmi szoftverrel ellátott munkaállomásról, saját kulccsal és felhasználói azonosítóval érheti el a Kutatóközpont belső hálózatát. A kívülről való elérés során is köteles betartani az MTA CSFK IBSZ-t. Nem megfelelően beállított munkaállomásról való bejelentkezés esetén a rendszergazda jogosult felfüggeszteni a felhasználó CSFK hálózati hozzáférését a hiba kijavításáig.

12.4. Az informatikai feldolgozás folyamatának védelme

A szerverek rendszergazda jelszavát lezárt borítékban, zárható szekrényben kell tárolni. A boríték felbontását dokumentálni kell.

A védendő adatokra kiterjedően:

- az adatbevitel hibátlan műszaki állapotú berendezésen történjen,
- tesztelt adathordozóra lehet adatállományt menteni,
- a bizonylatokat és adathordozókat csak e célra kialakított és megfelelő tároló helyeken szabad tartani,
- lehetőség szerint olyan szoftvereket kell alkalmazni, amelyek rendelkeznek ellenőrző funkciókkal és biztosítják a rögzített tételek visszakeresésének és javításának lehetőségét is.
- a bejelentkezési azonosítók használatával kell szabályozni, hogy ki milyen szinten férhet hozzá a kezelt adatokhoz. (alapelv: a tárolt adatokhoz csak az illetékes személyek férjenek hozzá).
- az adatok bevitele során alapelv: azonos állomány rögzítését és ellenőrzését ugyanaz a személy nem végezheti.

A védendő adatok adatrögzítési folyamatához kapcsolódó dokumentációk lehetnek:

- adatrögzítési utasítások,
- ellenőrző rögzítési utasítások,
- tesztelő és törlő programok kezelési utasításai,
- megőrzési utasítások,
- gépkezelési leírások.
- A dokumentációk előállításáért és megőrzéséért az adott szervezeti egység vezetője felelős.

12.5 Adathordozók védelme

Az adathordozók logikai védelmét az operációs rendszer és az ehhez tartozó ellenőrző, file-kezelő rutinok alkalmazásával lehet biztosítani.
A központi informatikai eszközök üzemeltetéséért az informatikai koordinátor a felelős.

- Köteles gondoskodni a feldolgozások igényeinek megfelelő adathordozók biztosításáról, beleértve a biztonsági másolatok eszközigényeit, illetve az üzemeltetés biztonságát növelő generációs adatállományok alkalmazását is.

- Az adathordozókat a gyors és egyszerű elérés, a nyilvántartás és a biztonság érdekében azonosítóval kell ellátni. Az azonosítókat mind emberi, mind informatikai olvasásra alkalmas formában kell feltüntetni.
- Az operációs rendszer adta lehetőségek figyelembe vételével biztosítani kell a külső és belső címek azonosságát.

A védendő adatok tárolására szolgáló adathordozók elhelyezése:

- a védendő adatok tárolására szolgáló adathordozók elhelyezésére a géptermen kívüli műszaki-, tűz- és vagyonvédelmi előírásoknak megfelelő helyiséget kell kijelölni, illetve kialakítani.
- adathordozót a részlegből ki-, illetve oda bevinni csak az informatikai koordinátor vagy rendszergazda engedélye alapján lehet.

A védendő adatok tárolására szolgáló külső adathordozókról nyilvántartást kell vezetni.

- Az azonosító adaton kívül a felírás és megőrzés dátumát, védettség tényét, jogosultsági és illetékességi adatokat, valamint az adathordozó kiadására és visszavételezésére vonatkozó információkat kell tartalmaznia.
- A nyilvántartásnak naprakészen követnie kell az adathordozók fizikai mozgását.
- A nyilvántartás vezetéséért az a részlegvezető felel, akinél az adathordozók felhasználásra kerültek.

A védendő adatok tárolására szolgáló adathordozók megőrzése:

- Az adathordozók megőrzési idejét a köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről szóló többször módosított 1995. évi LXVI. törvényben foglaltak, továbbá a Kutatóközpont Bizonylati rendjében és Iratkezelési szabályzatában foglaltak alapján az adatkezelő határozza meg.

A védendő adatok tárolására szolgáló adathordozók karbantartása:

- A védendő adatokat tartalmazó adathordozókat évenként tisztítani kell és ellenőrizni azok állapotát, elöregedését.

Selejtezni kell:

- a fizikailag sérült, javíthatatlan, a gyári, raktározási hibából követően felhasználásra alkalmatlan (deformálódott) belső vagy külső adathordozót.

Adatmegsemmisítés:

- A selejtezésre leadott, adattárolásra alkalmatlan adathordozókat fizikai roncsolással használhatatlanná kell tenni.
- Bizalmas adatokat, felhasználói és rendszerprogramokat tartalmazó adathordozókról, törlő programokkal kell az adatokat törölni, vagy fizikailag kell megsemmisíteni az adathordozót.

A selejtezést a Kutatóközpont felesleges vagyontárgyak hasznosításának és selejtezésének szabályzata, valamint iratkezelési szabályzata alapján kell lefolytatni.

Sokszorosítás, másolás:

- Sokszorosítást, másolást csak az érvényben lévő rendeletek szerint szabad végezni. (Az üzemi másolás nem minősül másolásnak.)

- Biztonsági illetve archív adatállomány előállítása másolásnak számít.

Leltározás:

- Az adathordozókat az Eszközök és források leltárkészítési és leltározási szabályzatában foglaltaknak megfelelően kell leltározni.

12.6. Mentések, file-ok védelme

Szerverek mentése:
Az informatikában a legnagyobb értéket a számítógépen tárolt adatok jelentik. Ezek védelmében meghatározó jelentőségű a biztonsági másolatok készítése a központi szervereken.
A mentések folyamata:

- A mentéseket meghatározott időközönként a szerverekről központi mentő szoftverrel kell végrehajtani.
- A mentésből a rendszerek, a szoftverkörnyezet beállításainak, valamit a tárolt adatoknak teljes körűen visszaállíthatónak kell lennie a mentés pillanatának állapotára.
- A szerverek esetében az adatokat lehetőség szerint a számítógépteremtől fizikailag elkülönült helyiségben lévő helyre kell menteni, és a szerverterem tűzterétől elkülönülő térben, tűzbiztos helyen kell tárolni.
- A szerverek mentését legalább hetente, illetve a hálózati aktív eszközökét a beállítás változtatásakor kell elvégezni.
- A mentett adatokhoz csak az arra jogosultak férhetnek hozzá.
- A személyi anyagok, a főkönyvi könyvelés, a pénztári könyvelés és az egyéb analitikus nyilvántartások adatainak mentését a Kutatóközpont Számviteli Politikája és Számlarendje szabályozza.

Munkaállomások mentése:

- A munkaállomásokon a mentéseket meghatározott időszakonként el kell végezni. Ezért a gép leltár szerinti használója felel. Az archiválásban az informatikusok segítséget nyújtanak.
- A munkák során keletkezett adatok, illetve létrehozott dokumentumok mentése az azokat létrehozó munkatársak (felhasználók) feladata.
- Az adatállományok file-védelme során gondoskodni kell arról, hogy azok ne károsodjanak. A fontosabb file-okat tartalmazó adathordozókról másolatot kell időnként készíteni.

12.7. Szoftver védelem

Rendszerszoftver védelem:

- Rendszerszoftver alatt az informatikusok által üzemeltetett szervereken installált szoftvereket értjük.
- Az üzemeltetésért felelős vezetőnek biztosítani kell, hogy a rendszerszoftver naprakész állapotban legyen és a segédprogramok, programkönyvtárak mindig hozzáférhetők legyenek a felhasználók számára.
- Az üzembiztonság érdekében tartalék operációs rendszerrel kell rendelkezni, amely szükség esetén azonnal betölthető legyen.
- A rendszerszoftver módosításához az üzemeltetésért felelős vezető engedélye szükséges.
- Név szerint kell kijelölni azokat a személyeket, akik a rendszerszoftverben módosításokat végezhetnek.

- A változtatásokról nyilvántartást kell vezetni.

Felhasználói programok védelme:

- A felhasználó az általa használt munkaállomásra csak indokolt esetben kaphat rendszergazdai jogosultságot.
- A felhasználói programok védelméről az azokat létrehozó illetve telepítő dolgozónak kell gondoskodnia az operációs rendszer lehetőségeit kihasználva.
- A munkaállomásokra csak jogtiszta programokat szabad telepíteni.

13. Felhasználó- és jogosultságkezelés

Az informatikai rendszer használatával való visszaélés kizárása érdekében a Kutatóközpont hálózatán minden felhasználónak egyedi felhasználói azonosítóval és az ahhoz tartozó jelszóval kell azonosítania magát.

13.1. Felhasználó

- a Kutatóközpont dolgozója, de igazgatói engedéllyel külső személy is kaphat felhasználói azonosítót („vendégkutató").
- A felhasználói azonosítók kiadása központilag történik minden rendszer esetében.
- Felhasználói azonosítót a rendszergazdától írásban kell igényelni (3. sz. melléklet).
- Azonosító igénylésekor egyértelműen meg kell határozni a jogosultságot birtokló, azért felelősséggel tartozó személyt. Ellenőrizni kell, hogy az igénylő jogosult-e a felhasználói azonosító igénylésére.
- A felhasználónak aláírásával kell igazolnia, hogy a használat feltételeit és szabályait megismerte, és azokat magára nézve kötelezőnek tekinti.
- A munkahelyi vezetőnek aláírásával kell igazolnia, hogy az igénylő jogosult az informatikai rendszer használatára.
- „Vendégkutató" esetében a munkahelyi vezető szerepét a vendéglátó tölti be és felelősséget vállal a felhasználói azonosítóért. A vendégkutató igénylő lapját az engedélyező igazgatóval is alá kell íratni. A „vendégkutató" távozása után a felhasználói azonosítót meg kell szüntetni.
- Adminisztrátori – rendszergazda – feladatokat ellátó személyek részére a normál felhasználói feladatok ellátására és adminisztrációs célokra külön azonosítót kell létrehozni.
- A felhasználói azonosítót le kell tiltani, ha azzal visszaélés történt, és az esetet ki kell vizsgálni.
- A felhasználói azonosítókat a rendszerből törölni kell, ha a felhasználó már nem a Kutatóközpont dolgozója, illetve egyéb okok miatt már nincs a rendszer használatához joga. A munkahelyi vezető kötelessége a rendszergazdát értesíteni, aki elvégzi a szükséges teendőket – adatállományok mentése, felhasználói azonosító törlése.
- A Kutatóközpontban a sokféle tevékenység miatt az egyes felhasználók számítástechnikai igényei eltérnek, ezért egyedi megfontolás alapján a munkahelyi vezető a rendszergazda segítségével határozza meg a rendelkezésre bocsátott eszközöket.
- A Kutatóközpont informatikai rendszerében a felhasználói szerepkört betöltő munkatársak számára biztosított egyedi számítástechnikai környezet elemeinek listáját a rendszergazda folyamatosan karbantartja.
- A kiadott informatikai eszköz illetve jogosultság személyhez és munkakörhöz kötődik. A munkakör megváltozását vagy a munkavállaló munkaviszonyának megszűnését, illetve tartós szünetelését a munkahelyi vezető köteles a rendszergazdának jelenteni, aki – a

munkahelyi vezető jóváhagyásával – intézkedik az eszközök kezeléséről és szükség esetén áthelyezéséről.

- Az egyéni használatú informatikai erőforrásokhoz csak az a felhasználó férhet hozzá, aki azt név szerint megkapta.
- A jogosultságok kiosztását a vezető kezdeményezi a felhasználó felvételekor, illetve amikor ezt a munka- és/vagy feladatkörében bekövetkezett változások indokolják. Ennek beállításától kezdve kizárólag az adott felhasználó felel az egyéni használatú erőforrás használatáért, arra további jogosultság nem adható.

13.2. Speciális felhasználó

- A speciális – pl. hálózati adminisztráció, jogosultság kiosztás, stb. – feladatokhoz tartozó jogok alapértelmezésben a rendszergazdát illetik meg, de hivatalos megállapodás alapján – igazgatói engedéllyel, munkaköri leírásban is megfogalmazva - más személynek átadhatók.
- Amennyiben a rendszergazda úgy ítéli meg, hogy a speciális feladatokat ellátó személy a rendszer biztonságát veszélyezteti, joga van a kiemelt jogok használatának lehetőségét felfüggeszteni, és köteles haladéktalanul beszámolni az igazgatónak vagy helyettesének.

13.3. Felhasználó megszüntetése, megtartása

A Kutatóközpont általi alkalmazás megszűnése maga után vonja a felhasználói azonosító megszűnését is. Ezek alól azonban igazgató engedéllyel az alábbi esetben lehetnek kivételek:

- nyugdíjazás,
- MTA-hoz vagy másik MTA intézményhez átigazolás,
- létező projekt fenntartása miatt.

Ezekben az esetekben a jogosultságot évente felül kell vizsgálni és ki kell jelölni egy munkahelyi vezetőt, aki aláírásával igazolja, hogy a felhasználóért felelősséget vállal. Az így megtartott felhasználói azonosítók tulajdonosaira is vonatkozik az IBSZ, aminek tudomásul vételét aláírásával kell igazolnia.

Teendők felhasználói azonosító megszüntetése esetén:

- gondoskodni kell az adatok mentéséről és átadásáról,
- a rendszerhez való hozzáférés megszüntetéséről.
- Minősített kutató munkaviszonyának megszűnése esetén lehetőséget kell adni a beérkező email-ek átirányítására. A felhasználó írásban rögzíti, hogy milyen email címre kéri az átirányítást és aláírásával igazolja, hogy a megadott email cím az ő kizárólagos használatában van. A megadott email címből egyértelműen ki kell derülnie, hogy a postafiók az aláíróhoz tartozik (4. sz. melléklet).
- A postafiók megszűnéséről való tájékoztatásként javasolt válaszüzenet beállítása, melyben leírásra kerül a munkát átvevő email címéről illetve a távozó munkatárs új email címéről.
- Korábban létező felhasználói azonosítót a Kutatóközpont 5 évig nem adhat újra ki.

13.4. A felhasználói azonosítók kezelésének szabályai

- A felhasználók csak saját azonosítóval használhatják a hálózatot.
- A felhasználó felel a rábízott felhasználói azonosító és az ahhoz rendelt jogok biztonságáért. Az azonosító használata másnak még a tulajdonos jelenlétében sem engedhető át.

- A felhasználói azonosítóhoz tartozó jelszót csak annak birtokosa és a rendszergazda ismerheti. Jelszavakat (password) úgy kell megválasztaniuk és kezelniük, hogy ahhoz más ne juthasson hozzá.
- A felhasználót jelszavának átadására más felhasználó számára senki sem kérheti.
- Amennyiben felmerül a gyanú, hogy a jelszó mások tudomására jutott, úgy azt azonnal meg kell változtatni.
- Amennyiben valaki észleli, hogy mások kísérletet tesznek a felhasználói jelszavaik megszerzésére, azt azonnal jelezni kell a rendszergazdának.
- Más személy jelszavának vagy adatainak megszerzésére irányuló cselekedet súlyos fegyelmi vétség.
- A felhasználói azonosító tulajdonosa elsődlegesen felel az azonosító használatával elkövetett szabálytalanságokért. Akkor is felelősségre vonható, ha bebizonyosodik, hogy azt nem ő használta, de gondatlansága folytán jutott jelszava illetéktelen kezekbe.
- A felhasználó a számítógépes munkahely elhagyásakor köteles kilépni a hálózatból, és az utolsónak távozó a helyiséget bezárni

13.5. Felhasználó személyiségi jogai

- A felhasználó személyiségi jogait és a levéltitkot a hálózat üzemeltetője tiszteletben tartja, ettől eltérni csak a törvény által meghatározott esetekben lehet.
- A felhasználók védett adataihoz hozzáférni csak technikai vagy biztonsági okokból szabad, de ilyenkor is csak a feltétlenül szükséges mértékben, és az érintettek megfelelő tájékoztatásával. Erre csak a rendszergazda jogosult, aki az ily módon tudomására jutott információkat nem hozhatja nyilvánosságra, valamint másokkal nem közölheti.

14. Ellenőrzés

Az ellenőrzésnek elő kell segíteni, hogy az informatikai rendszerben meglévő veszélyhelyzetek ne alakuljanak ki. A kialakult veszélyhelyzet esetén cél a károk csökkentése illetve annak megakadályozása, hogy az megismétlődjön.
A munkafolyamatba épített ellenőrzés során az IBSZ rendelkezéseinek betartását az adatkezelést végző szervezeti egység vezetői folyamatosan ellenőrzik.

15. Záró rendelkezések

Az Informatikai Biztonsági Szabályzat 2018. október 15-től hatályos. E napon a 2012. évi Informatikai Szabályzat hatályát veszti.

Mellékletek

1. sz. melléklet

Magyar Tudományos Akadémia Csillagászati és Földtudományi Kutatóközpont

Gazdasági Igazgatóság hálózatának védelme

Az Gazdasági Igazgatóság (GI) hálózatát fokozottan védeni kell.
A GI részére kialakított virtuális helyi hálózatot (VLAN) kizárólag a GI munkatársai használhatják a részükre kiosztott jogosultságokkal.
A GI VLAN-ba tilos hordozható eszközöket csatlakoztatni – notebook, pendrive, külső adathordozó -, amiket más hálózatokban is használnak.
A GI számítástechnikai eszközein kivétel nélkül folyamatosan frissített víruskereső programnak kell futnia.
A GI VLAN-ra csatlakoztatott eszközöknek szigorúan beállított tűzfal mögött kell lenniük.
A GI munkatársainak a használat kezdetekor illetve a változások esetén külön oktatásban kell részesülniük, amit dokumentálni kell.
A GI VLAN hálózatára csatlakoztatott számítógépek internet használatát kizárólag Kutatóközponti munkavégzésre szabad használni, egyéb honlapok felkeresése szigorúan tilos.

2. sz. melléklet

A szerverszoba rendje

1. A szerverszobában az oda munkavégzésre beosztottakon kívül csak az alábbi személyek tartózkodhatnak:
    a. az intézmény vezetője
    b. a tűz- és vagyonvédelemért felelős reszortfelelősök.
2. Más személyek benntartózkodását csak az intézményvezető, vagy az informatikai koordinátor engedélyezheti.
3. Üzemeltetés alatt az ajtókat állandóan becsukva, üzemidőn kívül pedig zárva kell tartani és a kulcsokat le kell adni.
4. A gépterem kulcsát csak az informatikai koordinátor által összeállított külön listán szereplő személyek kaphatják meg.
5. Munkaidőn kívül idegen személy csak az intézmény vezetőjének (távollétében helyettesének) engedélyével tartózkodhat a gépteremben.
6. A gépterembe ételt, italt bevinni és ott elfogyasztani TILOS!
7. SZIGORÚAN TILOS a gépterembe égő cigarettával belépni, illetve ott dohányozni!
8. A gépterem takarítását csak az arra előzőleg kioktatott személyek végezhetik.
9. A berendezések belsejébe nyúlni TILOS! Bármilyen nem a gépkezeléssel összefüggő beavatkozást csak a rendszergazdák végezhetnek. Ez alól csak a szervizek szakemberei kivételek.
10. Az informatikai eszközöket csak rendeltetésszerűen és kizárólag az ütemezett munkák elvégzésére lehet használni.
11. A gépteremben elhelyezett adathordozókhoz rendszergazdákon kívül, illetve azok engedélye vagy jelenléte nélkül senki nem nyúlhat.
12. A gépterembe adathordozókat csak rendszergazdák vihetnek be, illetve hozhatnak ki onnan.
13. Az elektromos hálózatba más - nem a rendszerekhez, illetve azok kiszolgálásához tartozó - berendezéseket csatlakoztatni nem lehet!
14. A gépteremben elhelyezett jelzőberendezések (klíma, tűz- és betörésjelző) műszaki állapotát folyamatosan figyelni kell az ott dolgozóknak, és bármilyen rendellenességet észlelnek, azonnal jelenteni kell a működésükért felelős megbízottaknak.
15. A javításoknak, illetve bármilyen beavatkozásoknak minden esetben ki kell elégíteni a szükséges műszaki feltételeken kívül a balesetmentes használat, a szakszerűség, a vonatkozó érintésvédelmi szabványok és az esztétikai követelményeket. Nem végezhető olyan javítás, szerelés, átalakítás vagy bármilyen beavatkozás, amely nem elégíti ki a balesetvédelmi előírásokat.

A fenti rendelkezések megsértése esetén fegyelmi felelősségre vonás kezdeményezhető.

3. sz. melléklet

Felhasználói név és jelszó igénylés az MTA CSFK informatikai rendszerének használatához

(Application for user name and password for the CSFK information system)

Csak munkahelyi vezető aláírásával érvényes! Kérjük olvashatóan kitölteni!
(Valid only with the signature of the workplace supervisor! Please write legibly!)

Felhasználó teljes neve (full name)*: Szöveg beírásához kattintson vagy koppintson ide.
Intézet (institute)*: Jelöljön ki egy elemet.
Munkahelyi vezető vagy vendéglátó (workplace supervisor or host)*: Szöveg beírásához kattintson vagy koppintson ide.
Munkavégzés helye – telephely (site)*: Jelöljön ki egy elemet.
Iroda v. labor (office): Szöveg beírásához kattintson vagy koppintson ide.
Elérhetőség (munkahelyi telefon vagy mobil) (phone number)*: Szöveg beírásához kattintson vagy koppintson ide.
Munkakör (scope of activities)*: Jelöljön ki egy elemet.
Munkakör betöltésének kezdete (starting date)*: Dátum megadásához kattintson vagy koppintson ide.
Foglalkoztatás jellege (status)*: Jelöljön ki egy elemet.

Igényelt hozzáférések, jogosultságok (requested access and authorisation) – rendszergazda tölti ki:
CSFK címtár azonosító (username in CSFK): Szöveg beírásához kattintson vagy koppintson ide.
Email cím (email address): Szöveg beírásához kattintson vagy koppintson ide.@csfk.mta.hu
Eduroam, eduID
Egyéb (other):
Kelt (date): .....

.....	.....
Munkahelyi vezető*	igazgató (vendég esetében kötelező)
(workplace leader)	(director, obligatory for guests)

Dolgozói nyilatkozat (Statement of employee)
Tudomásul veszem az MTA CSFK Informatikai Biztonsági Szabályzata elveit, előírásait elolvastam, azokat magamra nézve kötelezőnek fogadom el. (I take notice and accept the Regulation of Information Security of CSFK.)
Hozzájárulok, hogy az MTA CSFK a fenti adataimat tárolja, azokat az informatikai szolgáltatások használata során azonosításhoz felhasználja, de azokat harmadik félnek ki nem adja. (I agree that MTA CSFK stores my information above, uses it for identification with the use of IT services but does not give it to third parties.)

.....
Felhasználó (user)

4. sz. melléklet

Igénylés emailek átirányítására az csfk.mta.hu levelező szerverről privát email címre munkaviszony megszűnése esetén

..... (név) kérem, hogy a .....
felhasználói azonosítómra érkező emaileket az alábbi privát email címemre továbbítsák:

email cím*: .....
*A megadott email címből egyértelműen ki kell derülnie, hogy az aláíróhoz tartozik (pl. szerepel benne az aláíró neve).

Aláírásommal igazolom, hogy a megadott email postafiókhoz kizárólagos hozzáférésem van.

dátum:

....
felhasználó aláírása engedélyező aláírása (igazgató)