MAGYAR MŰSZAKI ÉS KÖZLEKEDÉSI MÚZEUM

Informatikai Biztonsági és Üzemeltetési Szabályzat

Budapest 2015-03-25

Jóváhagyta

……..

Dr.Krámli Mihály Ph.D
főigazgató

A SZABÁLYZAT HATÁLYA

hatályba lépésével az addigi az Informatikai Biztonsági Szabályzat érvényét veszti.
A Számítástechnikai Üzemeltetési és Adatvédelmi Szabályzat rendelkezéseinek végrehajtásáról a műszaki-főigazgató helyettes, az anyagi feltételek biztosításáról a gazdasági igazgató gondoskodik.
A szervezeti egységek vezetői kötelesek biztosítani, hogy a vezetésük alatt álló beosztottak a szabályzatot megismerjék és betartsák.

Tevékenységek, amelyek a szabályzat hatálya alá tartoznak:

informatikai eszközök beszerzése, használata és védelme,
szoftverek telepítése és használata,
a számítástechnikai adathordozók védelme,
az adathordozókon tárolt adatok védelme és elérhetőségének biztosítása,
a belső és külső hálózatok használata.

Személyi hatály

A Számítástechnikai Üzemeltetési és Adatvédelmi Szabályzat személyi hatálya kiterjed a Magyar Műszaki és Közlekedési Múzeum szervezeti egységeire, illetve a Magyar Műszaki és Közlekedési Múzeum közalkalmazotti jogviszonyban és munkavégzésre irányuló egyéb jogviszonyban lévő személyekre, a jogviszonyban nem lévő vendég kutatókra.
Az intézmény számára számítástechnikai feladatokat bármilyen megállapodás alapján az intézmény területén végzőkre.
Fentieken kívüli személyek a Magyar Műszaki és Közlekedési Múzeum számítástechnikai berendezéseit csak külön engedéllyel használhatják.

Tárgyi hatály

A Szabályzat tárgyi hatálya kiterjed a Magyar Műszaki és Közlekedési Múzeum összes számítástechnikai információs rendszerére és egységére:
Az intézmény tulajdonában vagy használatában lévő valamennyi számítástechnikai eszközre és szoftverre;
az adatfeldolgozási folyamatokra és eljárásokra;
a számítástechnikai munkához kapcsolódó dokumentációkra
a feldolgozás során létrejött és tárolt számítástechnikai információkra;
számítástechnikai eszközökre és adathordozókra;
számítástechnikai hálózatra és hálózati berendezésekre.

ALAPFOGALMAK

Adat: a szabályzat szempontjából minden olyan információ, amelyet a Magyar Műszaki és Közlekedési Múzeum tevékenységével, gazdálkodásával stb. kapcsolatban számítástechnikai rendszereiben és alrendszereiben, illetve egyedi számítógépeken vagy egyéb adathordozón rögzítettek.

Védelem: az a tevékenység, amellyel a Magyar Műszaki és Közlekedési Múzeum szervezeti egységei és számítás-technikai apparátusa a rögzített információk minősítés szerinti kezelését, elmentését és tárolását (megőrzését) biztosítják, illetve illetéktelen hozzáférést megakadályozzák.

Szervezeti egység: a Magyar Műszaki és Közlekedési Múzeum szakmai vagy kiszolgáló egysége, amelynek a munkáját kinevezett (megbízott) vezető irányítja.

Számítástechnikai apparátus: az a szervezet, amely az egyes szervezeti egységek szakmai tevékenységét számítástechnikai szempontból kiszolgálja, és a működés szakmai feltételeit biztosítja.

Rendszergazda az a személy, aki az intézmény informatikai hálózatának biztonságos működéséért, a központi informatikai rendszerek üzemeltetéséért és a szervereken tárolt adatok védelméért felelős.

Titok: az a minősítési kategória, amelyet az 1995. évi LXVI. törvény és a vonatkozó jogszabályok meghatároznak.

Jelszó: számítástechnikai kulcs, amely a kijelölt személy részére lehetővé teszi a hozzáférést az adatokhoz (ezen belül a megkülönböztetendő jogosultsági szintekről a Szabályzat rendelkezik).

Felhasználó: az a személy aki az intézmény valamelyik munkaállomásán számítástechnikai tevékenységet végez.

ÁLTALÁNOS ELŐÍRÁSOK

A Magyar Műszaki és Közlekedési Múzeum bármely területén a hálózatban és munkaállomásokon egyaránt csak olyan számítógépes programok használhatók, amelyek jogtisztaságát hivatalos dokumentumok igazolják, szabad felhasználású szoftverek vagy amelyek szabad használatát a szerzők írásban rögzítették.

A létfontosságú adatok és programok többszörös megőrzését (és az ezzel kapcsolatos kimentését), a Szabályzatnak megfelelően kell megszervezni (ld. 5.6. pont)

A számítástechnikai hálózat külső kapcsolatának használatakor a Hungarnet szabályzatát is be kell tartani.

A Magyar Műszaki és Közlekedési Múzeum három elkülönített felhasználási területe van a számítástechnikai berendezéseknek, melyeket adatvédelmi szempontból megkülönböztetetten kell kezelni:

Működési (gazdasági, pénzügyi, adminisztratív stb.) adatok kezelése esetén a felhasználó és a szervezeti egység vezetője egyaránt felelős az adatok biztonságáért.

.

Azokon a gépeken, ahol a kétféle adat együtt fordul elő, ott a gép általános adatbiztonságáért a szervezeti egység vezetője a felelős.

A SZÁMÍTÁSTECHNIKAI RENDSZEREK ÉS EGYSÉGEK ÜZEMELTETÉSÉNEK FELELŐSSÉGI RENDSZERE

Szervezeti felépítés

A számítástechnikai rendszerek és egységek üzemeltetési és adatvédelmi feladatainak összehangolása a műszaki főigazgató-helyettes feladata. E feladata körében folyamatosan gondoskodik a szabályzatnak az információfeldolgozás és a számítástechnika korszerűsítésével összhangban történő karbantartásáról és módosításáról.

Felelősségi rendszer

A szakmai szervezetek felelőssége

Az előírások megtartása a szabályzat hatálya által érintett valamennyi szervezeti egységre és személyre kötelező.

A szabályzatban előírtak betartásáért valamennyi érintett szakmai szervezeti egység vezetője fegyelmileg felelős, aki a munkaköri leírások elkészítésénél alkalmazza a szabályzat előírásait.

Az üzemeltetésért felelős szervezet feladatai

A Magyar Műszaki és Közlekedési Múzeum programjában és éves feladattervében szereplő szolgáltatási feladatok maradéktalan ellátása.

Háttérkapacitás biztosítása és működtetése a tartós kiesések pótlására.

Az üzemképesség folyamatos fenntartása — az igények, a kockázat és a költségek mérlegelésével — saját vagy szerződéses karbantartási, javítási, felügyeleti kapacitással.

A tervezett megelőző karbantartás teendőinek, mélységének, gyakoriságának meghatározása

saját erőforrás alkalmazása esetén ügyviteli utasításban, külső szervezet igénybevétele esetén szerződésben.

A SZÁMÍTÁSTECHNIKAI ÜZEMELTETÉS BIZTONSÁGI SZABÁLYAI

A számítástechnikai rendszerek üzembiztonsága

A számítástechnikai rendszerek üzemeltetése akkor biztonságos, ha a rendszer különböző elemei (emberi, hardver- és szoftverténye zők) egymással összefüggő, egységes rendszert alkotva, együttesen és külön-külön is rendeltetésüknek, feladatuknak megfelelően, kiesés nélkül megbízhatóan működnek.

A rendszer (alrendszer) működését az üzemeltetésért felelős szervezetnek kell biztosítania, különös tekintettel az alábbiakra:

A számítástechnikai rendszerek üzembe állíthatóságának feltételei

A Magyar Műszaki és Közlekedési Múzeumban csak szabályszerűen tesztelt és dokumentált, adatvédelmi eljárásokkal intézményesen biztosított és regisztrált számítógépes rendszerek, alrendszerek illetve gépi egységek üzemeltethetők.

A számítógépes rendszert a kidolgozója a teszt és üzemi próbafutások sikeres elvégzése, valamint a felhasználóval való egyeztetés, illetve elfogadási teszt után, az üzemeltetési (felhasználói) dokumentációval együtt adja át az üzemeltetésért felelős szervezeti egységnek.

Számítástechnikai eszközök telepítésénél figyelembe veendő eljárások

A számítástechnikai rendszerek általános vagyon- és tűzvédelmét

az Országos Építésügyi Szabályzat

a 4/1980. (XI. 23.) BM rendelet és

a Magyar Műszaki és Közlekedési Múzeum Tűzvédelmi szabályzata írja elő. A tervek előkészítésénél figyelemmel kell lenni

az elemi károk miatt esetleg fellépő kockázatra;

az adott munkaterületre való belépés ellenőrzésére;

a távközlési vonalak lehallgatására, rosszhiszemű használata elleni védelemre;

a létfontosságú adatok megőrzési helyének kialakítására;

az ezzel kapcsolatos szállítás, illetve táv-adatfeldolgozás biztonságára.

Infrastrukturális előírások

Környezetre vonatkozó előírások

Nagyteljesítményű, speciális környezetet és működési feltételeket igénylő eszközöket (energia, klíma, pormentesség, statikus védelem stb.) szaktervezés alapján kialakított helyiségben vagy központban kell elhelyezni. A berendezések telepítése és környezeti feltételei tekintetében — ha a feldolgozott adatok minősítése kiemelt technikai védelmet nem igényel — a gyártómű előírásai az irányadók. A nagyobb forgalmú vagy ügyfélforgalommal érintett helyekre telepített számítástechnikai eszközök esetén a "fizikai" védelmet is biztosítani kell.

Elemi csapás, katasztrófa esetére a teendőket az intézmény katasztrófaterve tartalmazza. A különleges események kapcsán keletkező feladatokat ezen szabályzat … melléklete tartalmazza.

Kiszolgálók (szerverek

Annak a helyiségnek, ahol a szerverek működnek (a továbbiakban: szerverterem), biztonságosan zárhatónak kell lennie. A szerverteremben az ott illetékes dolgozókon kívül mások munkaidőben is csak a műszaki igazgató tudtával és beleegyezésével tartózkodhatnak, munkaidőn kívül csak a Főigazgatóság engedélyével.

A szerverterem áramellátása elkülönül a többi munkaszobáétól, az áramellátásnak akkor is biztosítottnak kell lennie, ha karbantartás, javítás miatt a többi helyiségben nincs áram. Áramkimaradás esetén a szervereknek szünetmentes tápegységről kell üzemelniük. Ha az áramszünet hosszabb ideig tart, a gépeket mielőbb biztonságosan le kell állítani.

Az elektromos elosztó egységeknek védeniük kell a túlárammal szemben, így elkerülhető a szerverek tápegységeinek korai meghibásodása.

A szerverteremben az eszközöknek ideális páratartalmat és hőmérsékletet klíma szabályozza.

Munkaállomások és perifériák

Számítástechnikai eszközt erősen poros, nyirkos, nagy hőingadozásnak kitett, az emberi tartózkodásra alkalmas hőmérséklettől tartósan eltérő hőmérsékletű helyen üzemeltetni nem szabad.

A számítástechnikai adathordozókat (beleértve a számítógépek merevlemezét is) tároló helyiség zárhatóságát biztosítani kell.

Tűzvédelem

A tűzvédelem speciális feladatairól a Magyar Műszaki és Közlekedési Múzeum Tűzvédelmi szabályzata rendelkezik. A tűzvédelmi felelős központilag — szükség esetén szakértő(k) bevonásával — gondoskodik az előírások betartásáról és betartatásáról.

A szerverterem a "D" tűzveszélyességi osztályba tartozik. Az erre vonatkozó

részletes előírásokat a *Tűzvédelmi utasítás* tartalmazza.
Az intézmény azon helyiségeiben, ahol számítástechnikai eszközöket használnak vagy tárolnak, a bejárat előtt min. 1-1 db 2-5 kg-os csak halonnal oltó tűzoltó készüléket kell elhelyezni.

A számítástechnikai eszközök rendeltetésszerű használata

Munkavégzés csak olyan számítástechnikai és elektromos eszközzel történhet, amely rendeltetésszerű használat során megbízhatóan, üzemszerűen működik. Bármilyen rendellenes működést azonnal jelenteni kell az üzemeltetésért felelős szervezeti egységnél. A számítástechnikai eszközöket, berendezéseket csak rendeltetésszerűen szabad használni:

- letakarásuk csak a saját porvédőjükkel lehetséges,
- szellőző nyílásaik elzárása szigorúan TILOS,
- azokra ételt, italt, virágot helyezni TILOS.
- a különböző számítástechnikai berendezések közelében dohányozni TILOS.
- Az UPS-re (szünetmentes áramforrás) bármilyen más eszközt (lámpa, ventillátor, számológép, porszívó stb.) csatlakoztatni TILOS.
- Tilos az eszközöket és azok részeit áthelyezni, burkolatukat, csatlakozásaikat megbontani.

Be kell tartani minden olyan előírást, mely az eszközök kezelési útmutatójában szerepel.

Elektromos meghibásodás, pl. zárlat gyanúja esetén az eszközt áramtalanítani kell. Ha a meghibásodás a helyiség elektromos hálózatában keletkezik, úgy az egész szobát áramtalanítani kell a főkapcsolóval.

Az asztali számítástechnikai eszközök épségéért, rendeltetésszerű használatáért a használó, az eszközt leltárilag is átvevő munkatárs felelős. Más az eszközt csak az elsődleges használó tudtával, belegyezésével és felelősségvállalásával használhatja.

Kiszolgálók (szerverek)

Szerver elindítására és leállítására, a szerveren könyvtárak nyitására, könyvtárak és fájlok módosítására vagy törlésére jogosult a rendszergazda.

Meghibásodás esetén a szerver hálózati szolgáltatásai karbantartási céllal szünetelhetnek. Ha a szerverek leállása előre látható, a műszaki osztály köteles a dolgozókat erről időben tájékoztatni.

Munkaállomások és perifériák

A számítógépet (hardver és szoftver szempontból) az azzal megbízott személy – a rendszergazda – felügyeli.

A felhasználók a számítógépes infrastruktúrát csak rendeltetésszerűen használhatják.

Adatvédelmi szabályok

Illetéktelen hozzáférés elleni védelem

A számítástechnikai rendszereknél az illetéktelen hozzáférés elleni védelmet az üzemeltetésért felelős szervezetnek kell biztosítania. Az adatokhoz való hozzáférés szabályozásánál, illetve a rendszerek üzemeltetésénél a következőket kell figyelembe venni:

Az adott szakmai terület (központi, illetve területi) vezetőjének kell meghatároznia azt az esetet, illetőleg az információk azon körét, amikor a Magyar Műszaki és Közlekedési Múzeum alkalmazottainak csak szűkebb köre juthat a kérdéses adathoz.

A hozzáférések szabályozásának gyakorlati megvalósítására a számítástechnikai rendszerek esetében elsősorban a jelszóvédelem áll rendelkezésre. A speciális védelmet igénylő adatokat jogosultság-kezeléssel is kell védeni. A védett tartalomhoz csak az engedélyezett személyek férhetnek hozzá

A Magyar Műszaki és Közlekedési Múzeum szolgáltató gépeinek helyiségeit a felügyeletet ellátó személyek távollétében zárva kell tartani.

A hozzáférések korlátozására hardveres védelem csak speciális célra és külön engedély alapján alkalmazható.

Jelszóvédelem

A jelszóval való védelem biztonságtechnikai szempontból alapvető feladat. Az így biztosítható jogosultsági szintek:

A munkaállomásokon dolgozó felhasználók korlátozott hozzáférési joggal rendelkeznek

A munkaállomásokon dolgozó felhasználók indokolt esetben rendszergazdai jogosultságot kaphatnak az általuk használt munkaállomásra korlátozva. A jogosultsági szint megváltoztatását a redszergazdai végzi el.

A munkaállomásokra a rendszergazda teljes körű hozzáférési joggal rendelkezik (rendszergazda jogosultság).

A jelszavaknak egyedieknek, személyhez kötöttnek kell lenniük. Minden jelszóval rendelkező felel azért, hogy az általa használt jelszó illetéktelen személyek tudomására ne jusson.

Az intézmény valamennyi közalkalmazottja és megbízott munkatársa személyesen felelős azért, hogy a napi munka során keletkező vagy archivált adatot, információt minősítése szerint kezeljen.

Adatmentés

A számítógépes alkalmazási rendszerek adatállományainak mentését rendszeresen el kell végezni. Minden szervezeti egységben gondoskodni kell arról, hogy megfelelő számú és minőségű mentésre alkalmas eszközzel rendelkezzenek.

A mentéshez rendszeresített adathordozók és a mentésre alkalmas egységek írhatóságát/olvashatóságát, a szabad terület méretét a mentést végző munkatársnak ellenőriznie kell. A mentett adatokat tartalmazó adathordozók állapotát 2 évente felül kell vizsgálni.

A mentett adatokat tartalmazó adathordozókat a számítógéptől elkülönített, kulccsal zárható helyiségben, tűzbiztos, zárható kazettában vagy páncélszekrényben kell tárolni a következő felhasználásukig.

Mozgatható mágneses adathordozók kezelése

Használati rend

Az üzemeltetésért felelős szervezetnek az előírásoknak megfelelően gondoskodnia kell a feldolgozás igényeinek megfelelő adathordozókról

Nyilvántartás

A programot, adatbázist, vagy a szolgáltatás részét képező dokumentumot tartalmazó mágneses adathordozókról naprakész nyilvántartást kell vezetnie minden szakmai szervezeti egységnek.

Tárolás

A tárolás minden esetben az előírt műszaki paraméterek szerint tűz és vagyonvédelmi előírásoknak megfelelően történjen.

A tároláskor minden esetben figyelemmel kell lenni, a mágneses adathordozók elektromágneses tér elleni védelmére is.

Megőrzés

A mágneses adathordozókon tárolt adatok megőrzési idejét azok minősítése és a bizonylati, iratkezelési szabályzatok alapján kell meghatározni és előírni. Ezek alapján kerül be az adatok megőrzési ideje a számítástechnikai dokumentációba és üzemeltetési utasításokba.

A megőrzési időt mágneslemez esetében a belső címkén, CD esetén az adathordozón egységesen fel kell tüntetni. A megőrzési idők nyilvántartásáért az üzemeltetésért felelős szakmai szervezet vezetője, vagy megbízottja a felelős.

Vírus elleni védelem

A feladatokat részletesen a 3. sz. melléklet tartalmazza.

1. Melléklet

A SZÁMÍTÓGÉPES BERENDEZÉSEK FEJLESZTÉSE ÉS VÁSÁRLÁSA SORÁN ÉRVÉNYESÍTENDŐ SZEMPONTOK

Fejlesztés

Tervezés

A számítástechnikai hálózat fejlesztésekor figyelembe kell venni a Magyar Műszaki és Közlekedési Múzeum hosszútávú érdekeit és célkitűzéseit.

Az elkészült rendszert teljes mértékig dokumentálni kell, kitérve az egyes elemek helyettesíthetőségének (kompatibilitás, szabványos felületek alkalmazása) kérdéseire.

Nem szabványos, vagy a számítástechnikai rendszereknél nem megszokott, egyedi gyártású elemeket csak ott szabad alkalmazni, ahol előre látható, hogy a fizikai vagy műszaki amortizáció a teljes rendszer cseréjét fogja jelenteni (pl.: egyedi kiállítási installáció).

Beszerzés

Vásárlás

A vásárláskor különös figyelmet kell fordítani a berendezések gazdaságos üzemeltethetőségére. Nem alkalmazható olyan berendezés, amely működése során aránytalanul nagy terheket ró az üzemeltetőre, speciális kezelést igényel és nagyfokú környezetszennyezéssel jár, vagy működése során veszélyes anyagnak számító melléktermékek keletkeznek.

A vásárláskor előnyben kell részesíteni a hosszú távon gazdaságosabban üzemeltethető (energia, kellékanyagok) berendezéseket.

Ajándék

A Magyar Műszaki és Közlekedési Múzeum más szervezetektől vagy magánszemélyektől csak úgy fogadhat el ajándékként számítástechnikai berendezéseket, hogy azok eredete dokumentált, és üzemeltetésük nem ró aránytalanul nagy terheket az üzemeltetőre.

Nem fogathatók el ajándékként olyan berendezések, amelyek részei veszélyes hulladéknak számítanak, vagy kezelésük különleges eljárást igényel.

Dokumentálás

Igények felmérése: rendszeres igényfelmérés, soron kívül felmerült igények, valamint a javítások során felmerülő igények.

A beszerzés folyamatának dokumentálása (ajánlatkérés,

megrendelés, számla rendezése, leltárba vétel, felhasználói átvétel)

Igények és beszerzések nyilvántartása

Ajándékozás esetében ajándékozási szerződést kell kötni.

2. sz. melléklet

A VÍRUS ELLENI VÉDELEMMEL KAPCSOLATOS ELŐÍRÁSOK

A vírusvédelem rendszere

A Magyar Műszaki és Közlekedési Múzeum informatikai rendszereinek vírusvédelmét egy központi vírusvédelmi programcsomag biztosítja, amely az Internet kijárattól a szerverek és a munkaállomások szintjéig központilag menedzselt, házirend-alapú, elosztott frissítési séma szerint üzemel.
Hetente egyszer a munkaállomásokon teljes körű vírusellenőrzés fut le, naponta több alkalommal frissül a vírusadatbázis a víruskereső szerveren és a munkaállomásokon is.

Fertőzött számítógépek vírusmentesítése

Lokalizálás

A legfontosabb teendő a vírus észlelése után a vírus további terjedésének megakadályozása.

Értesíteni kell vírusfertőzés gyanújáról, tényéről a gép használóit, hálózatos gép esetén a hálózatban lévő összes felhasználót, , hogy a további teendők ellátásában kellő szakmai segítséget nyújtsanak.

Lokális winchesterrel rendelkező számítógép esetén a gépet azonnal le kell választani a hálózatról.

El kell különíteni azokat az adathordozókat (floppy lemezek, cserélhető winchesterek) további vizsgálat (vírusellenőrzés) céljára, amelyek az adott géppel kapcsolatba kerültek. Ezeket az adathordozókat más számítógépen sem lehet használni!

A feladat elvégzésének felelőse a rendszergazda.

Felderítés

A lokalizálás után meg kell győződni a vírus jelenlétéről, pontosan be kell határolni a helyét és jellegét.

Fel kell térképezni a hatást és a következményeket.

Elhárítás

A lokalizálás és felderítés után a gépet meg kell tisztítani a vírustól, ezután újra alaposan ellenőrizni kell a vírusmentességet.
Szükség esetén a hálózati elemeket is mentesíteni kell a vírustól.

El kell végezni az elkülönített adathordozók vírusmentesítését is.

Értesíteni kell a gép használóit, valamint a hálózatban lévő összes felhasználót a vírusmentességről.

3. sz. melléklet

Melléklet a 20/2004. (VI.21.) IHM rendelethez

A NEMZETI INFORMÁCIÓS INFRASTRUKTÚRA FEJLESZTÉSI PROGRAM FELHASZNÁLÓI SZABÁLYZATA

Bevezetés
1. §

A jelen dokumentum (a továbbiakban: Szabályzat) a Nemzeti Információs Infrastruktúra Fejlesztési Program működtetéséről szóló 95/1999. (VI. 23.) Korm. rendeletben (a továbbiakban: Kormányrendelet) meghatározott, a Nemzeti Információs Infrastruktúra Fejlesztési Program (a továbbiakban: NIIF Program) keretében működtetett számítógép-hálózat (a továbbiakban: NIIF hálózat) használatát szabályozza a NIIF tagintézmények és a NIIF felhasználók számára.

Értelmező rendelkezések
2. §

Jelen Szabályzat alkalmazásában:

"NIIF felhasználók": a NIIF tagintézményekben a NIIF hálózat használói.

a) "NIIF Iroda": a Kormányrendelet 2. §-ának (3) bekezdése alapján a NIIF Program végrehajtására alapított teljes jogkörrel rendelkező önállóan gazdálkodó központi költségvetési szerv.

b) "NIIF szolgáltatások": a Kormányrendelet 9. §-ának (3) bekezdése alapján a NIIF Iroda illetve a NIIF tagintézmények között létrejött csatlakozási és szolgáltatási szerződés vagy megállapodás keretében meghatározott, a NIIF tagintézményeknek nyújtott hálózati csatlakozás, hálózati és információs szolgáltatások, valamint a szolgáltatásokhoz a NIIF Iroda vagy szerződéses partnerei által biztosított infrastruktúra.

c) "NIIF tagintézmények": felső- és közoktatási intézmények, kutató-fejlesztő helyek, közgyűjtemények és egyéb oktatási, tudományos és kulturális szervezetek, amelyek a Kormányrendelet 9. §-ában meghatározott módon NIIF tagintézményekké váltak.

A NIIF hálózat célja

3. §

A NIIF hálózat célja a Kormányrendelet 1. §-ának megfelelően országos és nemzetközi számítógépes hálózati kapcsolatok és információs szolgáltatások nyújtása felső- és közoktatási, kutatás-fejlesztési, közgyűjteményi, oktatási, tudományos és kulturális célokra.

4. §

A NIIF hálózatot a NIIF tagintézmények a 3. §-ban meghatározott célokra használhatják. Ebbe beleértendő a hálózatnak a tagintézmények tevékenységéhez kapcsolódó adminisztratív és információs feladataival összefüggő használata is.

5. §

Azon intézmények, amelyek nem tagintézményei a NIIF Programnak, azonban valamely NIIF tagintézménnyel oktatási, kutatás-fejlesztési, közgyűjteményi, tudományos vagy kulturális tevékenységre irányuló szerződéses munkakapcsolatban (projektben) együttműködnek, a NIIF hálózat szolgáltatásait használhatják ezen szerződés fennállásának tartama alatt, kizárólag ezen szerződéses munkakapcsolat céljaira. Ilyen együttműködési szerződést NIIF tagintézmény csak meghatározott időtartamra köthet. A NIIF tagintézmény az ilyen szerződés megkötéséhez köteles a NIIF Iroda jóváhagyását kérni, és köteles a munkakapcsolat befejezését a NIIF Irodának bejelenteni. Amennyiben a NIIF Iroda úgy találja, hogy a szerződés nem a fenti tevékenységre irányul, indokolt esetben megtilthatja a nem NIIF tagintézmény számára a NIIF hálózat használatát.

6. §

A NIIF hálózat a 4. és 5. §-ban meghatározott kereteken belül minden tevékenységre használható, amely nem ütközik a 7. §-ban foglalt rendelkezésekbe.

A NIIF hálózat használata

7. §

A NIIF hálózat nem használható az alábbi tevékenységekre, illetve ilyen tevékenységekre irányuló próbálkozásokra, kísérletekre:

d) a mindenkor hatályos magyar jogszabályokba ütköző cselekmények előkészítése vagy végrehajtása, így különösen mások személyiségi jogainak megsértése (pl. rágalmazás), tiltott haszonszerzésre irányuló tevékenység (pl. piramisjáték), szerzői jogok megsértése (pl. szoftver nem jogszerű terjesztése);

e) nem NIIF tagintézmények egymás közötti forgalmának bonyolítása, kivéve, ha azt az 5. §-ban meghatározott szerződéses munkakapcsolat indokolja;

f) a NIIF szolgáltatásoknak nem NIIF tagintézmények számára való továbbítása, beleértve a jóhiszemű továbbadást is, kivéve az 5. §-ban meghatározott szerződéses munkakapcsolatokat; a NIIF hálózatba kapcsolt rendszereket a működtetőknek a lehetőségek szerint úgy kell konfigurálniuk, hogy az ilyen használatot megakadályozzák (pl. nyílt levelezési átjáró stb.);

g) profitszerzést célzó, direkt üzleti célú tevékenység és reklám;

h) a NIIF hálózat, a kapcsolódó hálózatok, illetve ezek erőforrásainak rendeltetésszerű működését és biztonságát megzavaró, veszélyeztető tevékenység, ilyen információknak és programoknak a terjesztése;

i) a NIIF hálózatot, a kapcsolódó hálózatokat, illetve erőforrásaikat indokolatlanul, túlzott mértékben, pazarló módon igénybevevő tevékenység (pl. levélbombák, hálózati játékok, kéretlen reklámok);

j) a hálózat erőforrásaihoz, a hálózaton elérhető adatokhoz történő illetéktelen hozzáférés, azok illetéktelen használata, gépek/szolgáltatások – akár tesztelés céljából történő – túlzott mértékben való szisztematikus próbálgatása (pl. TCP port scan);

k) a hálózat erőforrásainak, a hálózaton elérhető adatoknak illetéktelen módosítására, megrongálására, megsemmisítésére vagy bármely károkozásra irányuló tevékenység;

l) másokra nézve sértő, vallási, etnikai, politikai vagy más jellegű érzékenységét bántó, zaklató tevékenység (pl. pornográf/pedofil anyagok közzététele);

m) mások munkájának indokolatlan és túlzott mértékű zavarása vagy akadályozása (pl. kéretlen levelek, hirdetések);

n) a hálózati erőforrások magáncélra való túlzott mértékű használata;

o) a hálózati erőforrások, szolgáltatások olyan célra való használata, amely az erőforrás/szolgáltatás eredeti céljától idegen (pl. hírcsoportokba/levelezési listákra a csoport/lista témájába nem vágó üzenet küldése);

p) hálózati üzenetek, hálózati eszközök hamisítása: olyan látszat keltése, mintha egy üzenet más gépről vagy más felhasználótól származna (spoofing).

A felhasználók kötelességei

8. §

A NIIF felhasználók kötelesek jelen Szabályzat megismerésére és megtartására.

9. §

Az a felhasználó, aki a NIIF hálózaton keresztül más hálózati szolgáltató szolgáltatásait is igénybe veszi, az idegen hálózatra érvényes szabályokat is köteles megtartani.

10. §

A NIIF felhasználó a polgári jog általános szabályai szerint felel minden általa – a NIIF Irodának vagy harmadik félnek – okozott kárért.

11. §

A NIIF felhasználó köteles a NIIF Irodát, illetve a NIIF tagintézményeket a Szabályzat megsértése és az esetleges káresetek kiderítésében, valamint lehetőség szerint a bekövetkezett károk következményei felszámolásában segíteni.

A Szabályzat betartatása, a Szabályzat megsértésének szankcionálása

12. §

A Szabályzat megsértésének gyanúja vagy erre vonatkozó – a NIIF Irodához vagy a NIIF tagintézményhez tett – bejelentés esetén az érintett NIIF tagintézmény az esetet kivizsgálja és megteszi a szükséges intézkedéseket. A NIIF tagintézmény a Szabályzat gondatlan megsértése esetén az elkövetőt figyelmeztetésben részesíti. A Szabályzat figyelmeztetést követő ismételt megsértése szándékos elkövetésnek minősül. A NIIF felhasználó a Szabályzat szándékos megsértése esetén a NIIF szolgáltatásokból ideiglenesen vagy véglegesen kizárható.

13. §

A NIIF tagintézmények kötelesek a Szabályzat több intézményt érintő súlyos megsértése esetén a NIIF Irodát tájékoztatni. Az ilyen esetet a NIIF Iroda és az érintett NIIF tagintézmény közösen vizsgálja ki. Amennyiben a Szabályzat több intézményt érintő súlyos megsértése más hálózatot is érint, akkor annak illetékeseivel a NIIF Iroda és az érintett NIIF tagintézmény együttműködni köteles.

14. §

A NIIF Irodának a Szabályzat súlyos megsértése esetén joga van a NIIF tagintézmény hálózati hozzáférését azonnal korlátozni. A hálózathoz való hozzáférés korlátozása esetén a NIIF tagintézményt kártérítési igény nem illeti meg, ugyanakkor a NIIF Iroda a korlátozás okáról az érintett NIIF tagintézményt a lehető legrövidebb időn belül tájékoztatni köteles.

15. §

A NIIF Iroda a Szabályzat megsértéséből eredő károkozás megelőzésére és a bekövetkezett károk következményeinek mielőbbi és minél eredményesebb felszámolására törekszik, illetve a Szabályzat megsértése esetén – amennyiben annak feltételei fennállnak – a polgári jog szabályai szerint felelősségre vonást kezdeményez.

16. §

A NIIF Iroda és a NIIF tagintézmények a mindenkori műszaki lehetőségeknek megfelelően törekednek arra, hogy a hálózaton áthaladó, illetve a hálózaton elérhető információkhoz, adatokhoz illetéktelenek ne férjenek hozzá.

17. §

A NIIF Irodában, illetve a NIIF tagintézményekben a NIIF hálózat működtetéséért felelős személyek a felhasználók adataihoz csak technikai vagy biztonsági okokból férhetnek hozzá, illetve akkor, ha a Szabályzat megsértésének gyanúja merül fel. Az adatokhoz való hozzáférés csak a szükséges mértékben és az érintettek megfelelő tájékoztatásával megengedett. A hálózat működtetéséért felelős személyek az ilyen módon tudomásukra jutott információkat másokkal nem közölhetik, azokat nem hozhatják nyilvánosságra. Kivételt képez, ha a Szabályzat megsértésének gyanúja merül fel, ebben az esetben az információk a kivizsgálásra illetékes személyekkel közölhetők.

A NIIF Műszaki Tanács által létrehozott NIIF Etikai Bizottság a NIIF Iroda, a NIIF tagintézmény vagy a NIIF felhasználó kérésére állást foglal a Szabályzatot érintő vitatott kérdésekben. Az Etikai Bizottságnak nem feladata a konkrét esetekben hozott döntések felülvizsgálata.

Záró rendelkezések
19. §

Jelen Szabályzat közzétételét követően a Hungarnet hálózat használatáról szóló szabályzatot ("Acceptable Use Policy" – 1997. május 23., 1.0 verzió) nem lehet alkalmazni.