



Szervezeti és Működési Szabályzat

2. sz. melléklet

Informatikai szabályzat

2011. szeptember 10.-i módosításokkal egységes szerkezetben

I.
ÁLTALÁNOS RENDELKEZÉSEK
A szabályzat célja
1. §

(1) Technológiailag előrehaladott és felgyorsult világunkban a gyors információhoz jutás elsődleges fontosságú. A Magyar Kolping Szövetség előtt álló újabb kihívásokat, feladatokat csak erős, fejlett informatikai háttérrel lehet hatékonyan megoldani.

(2) Az informatikai szabályzat (továbbiakban röviden szabályzat) célja a Magyar Kolping Szövetség informatikai berendezései, valamint azokon futó szoftverei (továbbiakban röviden: eszközök) használatának szabályozása. A szabályzat meghatározza az eszközök használatának módját, feltételeit, kitér a jogi és etikai kérdésekre is.

(3) A szabályzatban foglaltak ismerete és betartása az eszközöket igénybe vevő minden személy (továbbiakban felhasználó) számára kötelező. Az eszközöket csak olyan személy használhatja, aki a szabályzatot ismeri és betartja. A szabályzatot minden olyan személlyel ismertetni kell, aki az eszközök használatára engedélyt vagy utasítást kap.

Értelmező rendelkezések
2. §

(1) Informatikai rendszer: a Magyar Kolping Szövetség számítógép-hálózata, beleértve hálózati eszközöket, szervereket, általános célú számítógépeket, felhasználói és rendszerszoftvereket, sokszorosító, digitalizáló berendezéseket.

(2) Információs rendszer: az informatikai rendszer által szolgáltatott információk összessége.

(3) Informatikai szakértő (a továbbiakban rendszergazda): Egy számítógép rendszer-gazdájának nevezzük azt a szükséges számítástechnikai ismeretekkel rendelkező személyt, akit ezzel a feladattal a felhatalmazott szervezeti egység vezetője írásban megbíz. A rendszergazda a számítógép hardver és szoftver karbantartását, fejlesztését, hibáinak feltárását és – ha lehetséges – javítását végzi.

II.
AZ INFORMATIKAI RENDSZER MŰKÖDTETÉSÉNEK RENDJE
Informatikai eszközök
3. §

(1) A szabályzat alkalmazása tekintetében eszköznek tekintendők a:

- a) számítógépek
- b) a számítógép perifériák (pl. nyomtató, scanner, egér, stb.)
- c) a számítógép hálózat
- d) az irodatechnikai berendezések (pl. fénymásoló, fax, telefon)
- e) audio/video eszközök
- f) infó-kommunikációs eszközök
- g) a számítógépeken futó szoftverek
- h) a fenti berendezésekhez, szoftverekhez tartozó dokumentációk

(2) Az eszközök pontos jegyzékét az MKSZ leltár tartalmazza. A szabályzat elfogadása magában még nem jogosít fel senkit az eszközök használatára. A felhasználók által használható eszközök meghatározása a felhasználói jogosultság alapján történik.

Eszközök kezelése, használata

4. §

(1) A számítástechnikai eszközök telepítése, elhelyezése, az előírásoknak megfelelő üzembe helyezése kizárólag az informatikai munkatárs vagy megbízott feladata. Ezáltal érvényesíthető a beszerzéssel kapcsolatos garancia és jótállás. A gépek üzembe helyezése után az informatikai munkatárs vagy megbízott gondoskodik a gépekhez tartozó telepítő lemezek és dokumentációjuk átadásáról

(2) Az eszközök kezelése, használata során minden felhasználónak gondosan be kell tartani az alábbiakat:

- a) Minden olyan előírást, mely az eszközök kezelési útmutatójában szerepel.
- b) Ha egy eszközre nincs ilyen, akkor az intézmény által kiadott kezelési útmutatóban leírtakat.
- c) Minden eszközt csak a kezelési útmutatóban leírtak szerint lehet használni.
- d) A szoftverek, dokumentumok használata, létrehozása során a szerzői jogokra vonatkozó jogszabályokat.
- e) A munka és tűzvédelmi előírásokat, szabályokat.
- f) Tilos az eszközök közelében enni, inni, dohányozni.
- g) Tilos az eszközöket és azok részeit áthelyezni, burkolatukat, csatlakozásaikat megbontani.
- h) A felhasználóknak tilos az eszközök elektromos csatlakozásait megbontani. Elektromos meghibásodás, pl. zárlat gyanúja esetén az eszközt áramtalanítani kell. Ha a meghibásodás a gépterem elektromos hálózatában keletkezik, úgy az egész géptermet áramtalanítani kell a főkapcsolóval.

Információszolgáltatás típusai

5. §

(1) Elektronikus levelezés (e-mail)

- a) A Magyar Kolping Szövetség minden dolgozója jogosult az elektronikus levelezés használatára. A különböző funkciókat betöltő személyek a funkcióhoz kapcsolódó e-mail címet is kaphatnak.
- b) Az e-mail címeket a Magyar Kolping Szövetség megbízott személye adja ki. A megbízott elvégzi a címek nyilvántartását, karbantartását. Lehetővé teszi ezen címek elérhetőségét a kolping honlapon.
- c) A központi e-mail cím: mksz@kolping.hu
- d) A felhasználó jogosult a cégen kívüli levelezését másként elérni, letölteni saját gépére, például outlook expressz levelezőrendszerrel.

(2) Honlap alapú World Wide Web (www)

- a) A Magyar Kolping Szövetség web szerverét megbízott üzemelteti., annak folyamatos fejlesztéséről, karbantartásáról gondoskodik. Az üzemeltetés személyi és tárgyi feltételeit a Magyar Kolping Szövetség biztosítja.
- b) A Magyar Kolping Szövetség hivatalos központi web-címe: a www.kolping.hu. A honlap informatikai szerkezetét, struktúráját a Magyar Kolping Szövetség tervezi meg az egységekkel együttműködve.
- c) A World Wide Web oldalak egységesen html formátumban készülnek. A szerkesztés szabályai:

- a fájl-, és könyvtárnevek megválasztásánál értelmes, kifejező elnevezésekre kell törekedni az áttekinthetőség érdekében, de értelmes rövidítések megengedhetők;

- a fájl-, és könyvtárnevek nem tartalmazhatnak ékezetes betűket;

- az állományok kiterjesztése mindig szabványos legyen;

- üres hivatkozások (linkek) használata tilos.

d) A honlap szervezeti egységgel kapcsolatos tartalmát az egység vezetője által írásban megbízott személy szerkeszti, tartja karban. Az egység vezetője (illetve az általa írásban megbízott személy) felel a szervezeti egység honlapján tárolt információkért, az ott tárolt adatbázisok tartalmáért. Amennyiben egyes információk érvényüket veszítették, köteles az információkért felelős személy azokat (néhány napon belül) az összes hivatkozással és segédállománnyal együtt törölni.

Hálózati szolgáltatások

8. §

(1) A Magyar Kolping Szövetség informatikai megbízottja az egység vezetőjével egyetértésben annak érdekében, hogy a Magyar Kolping Szövetség számítógépes rendszere védett legyen jogosulatlan használat, illetve károkozás ellen, fenntartja magának a jogot, hogy:

a) bárkit a hálózat használatából kizárjon erre utaló alapos gyanú felmerülése esetén;

b) megtekintsen, átmásoljon, megváltoztasson vagy töröljön bármely fájlt, amely kapcsolatban lehet a rendszer vagy a hálózat jogosulatlan használatával;

c) a számítógépes rendszereket, helyi hálózatokat bármikor ellenőrizze, indokolt esetben leállítsa vagy átkonfigurálja, illetve fenntart magának bármely egyéb intézkedési jogot, amely szükséges lehet a számítógépes erőforrásainak megvédéséhez, és a további működés biztosításához.

e) Tilos olyan tevékenységet kifejteni, amely célja mások adatainak jogosulatlan megszerzése, megváltoztatása, letörlése. Tilos más felhasználók nevében tevékenykedni. A felhasználó nem teheti lehetővé mások számára, hogy a nevében tevékenykedjenek. Ezért – többek között – mindent meg kell tennie a jelszavai titkosságának megőrzése érdekében, továbbá ezért, hogy a személyazonosító eszközeit (például, de nem kizárólag: VPN kulcs, azonosító kártya, mobil telefon) más ne használhassa. A felhasználó köteles törekedni arra, hogy az általa pillanatnyilag használatba vett rendszerekben más személy ne fejthessen ki aktivitást.

(4) A Magyar Kolping Szövetség informatikai megbízottjának feladatai:

a) a hálózati szolgáltatások folyamatos működtetése;

b) a hálózat, az Internet használatának rendszeres ellenőrzése;

c) a Magyar Kolping Szövetség tulajdonában lévő számítógépek, hálózati eszközök részére szervezeti egységenként legalább egy hálózati végpontot biztosít;

d) központi hálózati funkciókat ellátó számítógépek rendszerkarbantartása és rendszeradminisztrációja;

e) Magyar Kolping Szövetség kolping családjainak és vezetőinek részére e-mail cím (azonosító) kiadása igénylőlap alapján;

f) a hálózat használatával kapcsolatos ismeretekről a felhasználókat folyamatosan tájékoztatja;

g) hálózati problémákkal kapcsolatban segítségnyújtás.

(5) Minden e-mail címmel, azaz azonosítóval rendelkező felhasználó:

a) leveleket küldhet, fogadhat;

- b) a szerveren az azonosító név alatti tárterületen dolgozhat;
 - c) honlapját az alapértelmezett "public_html" alkönyvtárban elhelyezheti;
 - d) használhatja a szerveren futó szoftvereket;
 - e) nem használhatja a központi hálózati funkciókat ellátó számítógépeket munkaállomásként (pl.: szövegszerkesztés, levelezés),
- (6) A felhasználónak a hálózat biztonsága és a saját adatainak védelme érdekében a több felhasználós rendszereken használt erőforrásait (fájljait, leveleit, adatbázisait) védeni kell az illetéktelen felhasználóktól.

a) A hálózati jelszavakat úgy célszerű megválasztani, hogy azokat ne lehessen kitalálni (a jelszó nem lehet nyelvhelyesen leírt, értelmes szó vagy nem kötődhet a felhasználó személyéhez);

b) A jelszavakat nem szabad mások tudomására hozni;

c) A jelszavakat ajánlatos legalább háromhavonta cserélni;

d) A hálózatba beléptetett terminált, munkaállomást nem szabad kilépés nélkül elhagyni;

e) A felhasználónak tilos más felhasználók erőforrásait illetéktelenül használni;

f) Tilos a hálózati erőforrásokat védő technikai korlátozások feltörése, más felhasználók jelszavainak megszerzése;

g) Tilos a rendszer, és más felhasználók adatait, fájljait – engedély nélkül - másolni, törölni vagy módosítani.

(7) Tilos az informatikai infrastruktúra etikátlan használata, azaz

a) más felhasználókat a munkában üzenetekkel, levelekkel vagy más módon zavarni;

b) az informatikai infrastruktúra erőforrásainak nagymértékű terhelése (nagyméretű fájl vagy egyéb adathalmaz hálózaton való átjuttatását, letöltését lehetőleg munkaidőn kívül kell elvégezni).

Kapcsolódás a Magyar Kolping Szövetség hálózatához

9. §

(1) Magyar Kolping Szövetség gerinchálózat

a) A Magyar Kolping Szövetség számítógépes hálózata CAT5 kábelgerincen alapszik. A csomópontokban, fali szekrényekben elhelyezett hálózati eszközök (hub-ok, switch-ek) teszik lehetővé a csatlakozást a gerinchálózathoz.

b) A Magyar Kolping Szövetség hálózat üzemeltetéséért az informatikai megbízott a felelős.

c) A hálózat bővítésekor, fejlesztésekor felmerülő munkákat az informatikai megbízott végzi vagy végezteti szakértő céggel.

d) Az MKSZ hálózatának aktív eszközeit az informatikai megbízott tartja karban. Az aktív eszközökhöz hozzányúlni, azokat feszültség mentesíteni, újraindítani, vagy hálózati csatlakozásokat megbontani csak az informatikai megbízott által megbízott személyek jogosultak.

e) Tilos az MKSZ gerinchálózatra történő közvetlen rácsatlakozás.

f) Tilos a kábeleztést a fali csatlakozónál megbontani, és közvetlenül a kábelre gépet csatlakoztatni. A fali csatlakozó és a számítógép között lengőkábel kell használni.

g) A hálózathoz való csatlakozáshoz szükséges címek felett az informatikai megbízott rendelkezik. Tilos önkényesen címeket megadni, vagy megváltoztatni. Szükség esetén az informatikai megbízott jogosult a már kiadott címek visszavonására vagy megváltoztatására.

h) A hálózat használatához szükséges szoftverek beállítását, telepítését az informatikai megbízott végzi a szervezeti egységek számára. Az installálás során az informatikai megbízott munkatársa bemutatja a használathoz szükséges programok működését. A továbbiakban a felhasználó önállóan dolgozik az adott szoftverekkel.

i) Az adatokhoz, információkhoz való hozzáférést a számítógépes felhasználói rendszerben a bejelentkezési azonosítók használata teszi lehetővé. Az azonosítókkal kell elhatárolni, hogy ki milyen adatokhoz férhet hozzá. A felhasználói rendszerben tárolt adatok hozzáférésehez, csak az adott szervezeti egység munkatársai jogosultak. A különböző jogosultsági szinteket szervezeti egységen belül az adott vezető határozza meg, különböző szervezeti egységek közötti hozzáféréseket az érintett vezetők közösen határozzák meg. A hozzáférési lehetőségeket mindenkor a titok és adatvédelmi előírásoknak megfelelően kell meghatározni. A beállításokat kizárólag az informatikai munkatársak végezhetik el a központi gépen. A hozzáférési jogosultságokat, azok változásait folyamatosan rögzíteni kell, és titkosan kell kezelni.

Felhasználók kötelességei

10. §

(1) A felhasználók a számítógépes infrastruktúrát csak rendeltetésszerűen használhatják.

(2) Az üzemeltető, hálózatot érintő esetekben az MKSZ külön engedélye nélkül az eszközöket csak az MKSZ ügyvitelére, az ezekhez kapcsolódó tevékenységeik folytatására vehetik igénybe. Különösen engedélyhez kötött külső hálózati kapcsolatok létesítése, a hálózaton átalakítások végrehajtása, a felhasználó számára jövedelmet hozó, nem a munkaköréhez tartozó munkavégzés. Csak személyre és csak időszakra engedélyezhető hálózatra dolgozó program fejlesztése, tesztelése.

(3) Nem engedélyezhető még saját tulajdonú eszközön sem a szórakozás (hálózati játékprogramok futtatása, hálózati forgalmat jelentősen növelő szórakoztató kép- és hanganyagok továbbítása), továbbá olyan tevékenység folytatása vagy szolgáltatás indítása, amely a MKSZ erőforrásait igénybe veszi és nem MKSZ céljait szolgálja. Különösen nem engedélyezhető azonosító rendszer nélkül üzemeltetett, de a hálózati szolgáltatásokra konfigurált eszköz jogosulatlan személy használatába átadása (pl. PC mail, web kliens), kapcsolt vagy bérelt vonali csatlakozás létesítése, szerver üzemeltetése.

(4) A felhasználónak az általuk karbantartott adatokat, fájlokat és adatbázisokat védeniük kell technikai és egyéb hibákból eredő károsodás ellen.

(5) Az adatfájlokat, dokumentumokat és adatbázisokat az adathordozó sérülésének veszélye miatt több különböző adathordozón ajánlott tárolni. Különösen veszélyes és kerülendő az adatoknak egyetlen hajlékonylemezen történő tárolása. A szervezeti egységeknél a szükséges mentési tervet az informatikai megbízott írásban dolgozza ki.

A felhasználónak rendszeresen vírusellenőrzést kell végrehajtani. A vírus ellenőrzéssel és vírusirtással kapcsolatban az informatikai megbízott segítséget nyújt.

(6) Az MKSZ elvárja az összes felhasználótól, hogy munkájuk magas szinten történő végzéséhez a szükséges számítástechnikai ismeretekkel rendelkezzen.

Netikett

11. §

(1) Az MKSZ felhasználói az Internet és az intranet használata során tanúsított magatartásukkal feleljenek meg a hivatalosnak elfogadott Netikett (RFC 1855) előírásainak.

(2) Az MKSZ felhasználói kötelesek továbbá oly módon használni a hálózatot, hogy magatartásukkal az MKSZ hitelét, jó hírét és érdekeit ne sértsék.

Szankciók

12. §

(1) Az informatikai megbízott bármikor jogosult ellenőrizni az intézmény eszközeinek szabályos használatát. Az ellenőrzés tényét nem köteles előre bejelenteni, de törekednie kell, hogy az ne zavarja feleslegesen a napi munkamenetet.

(2) Ha felhasználó az intézmény eszközeit nem a szabályzat előírásainak megfelelően használja, úgy fegyelmi vétséget követ el. A szabályok megszegése esetén a jogosultság megvonható, illetve a minimum szintre csökkenthető. A jogosultság megvonása az elkövetett szabálytalanság függvényében lehet

ideiglenes, vagy végleges. Az informatikai megbízott az általa hozott korlátozó intézkedéseket a felhasználó felettesének jelenti, aki dönt annak jóváhagyásáról, illetve a továbbiakban szükséges intézkedésekről. Mivel a szabályok megszegése az MKSZ informatikai rendszerének, s így mások munkájának biztonságát is veszélyeztetheti, ezért az informatikai megbízott indokolt esetben saját hatáskörében akár azonnali kitiltást is alkalmazhat.

(3) Amennyiben az elkövetett vétség a Büntető Törvénykönyv szerint bűncselekménynek minősül, úgy az informatikai megbízott a tudomására jutást követően azonnal köteles teljes kitiltást foganatosítani, a felhasználó adatait zárolni, s az intézmény vezetőjének a cselekményt jelenteni.

(4) A felhasználó minden olyan általa okozott kárért teljes körű kártérítési kötelezettséggel tartozik, mely az eszközök rendeltetés vagy előírás szerinti használatának megszegése miatt történik.

A szoftverhasználat rendje

13. §

(1) Szoftverrel kapcsolatos fogalmak

a) Az Sztj.- Szerzői jogi törvény- 1.§ (2) bekezdés c) pontja szerint szoftver: a számítógépi programalkotás és a hozzá tartozó dokumentáció (a továbbiakban: szoftver) akár forráskódban, akár tárgykódban vagy bármilyen más formában rögzített minden fajtája, ideértve a felhasználói programot és az operációs rendszert is.

b) A szoftverek beszerzése és használata során figyelembe kell venni a Büntető törvénykönyv szerzői jogra vonatkozó rendelkezéseit, és a szoftvert kísérő licencszerződés feltételeit. Ezért tudnia kell, hogy a licencszerződés megsértésével törvényt sértést követ el:

- aki a szoftvert, vagy annak dokumentációját, beleértve a programokat, alkalmazásokat, adatokat, kódokat és kézikönyveket a szerzői jog tulajdonosának engedélye nélkül lemásolja vagy terjeszti;

- aki szerzői jog által védett szoftvert egyidejűleg két vagy több gépen futtat, hacsak ezt a szoftver licencszerződése külön nem engedélyezi;

- az a szervezet, amely tudatosan vagy akaratlanul munkatársait arra ösztönzi, kötelezi, vagy számukra megengedi, hogy illegális szoftvermásolatokat készítsenek, használjanak, vagy terjesszenek;

- aki az illegális szoftvermásolást tiltó törvényt megsérti azért, mert valaki erre kéri vagy kényszeríti;

- aki szoftvert kölcsön ad úgy, hogy arról másolatot lehessen készíteni, vagy aki a kölcsönkért szoftvert lemásolja;

- aki olyan eszközöket készít, importál, vagy birtokol, amelyek lehetővé teszik a szoftver védelmét szolgáló műszaki eszközök eltávolítását, vagy ilyen eszközökkel kereskedik.

(2) Értelmező rendelkezések

a) Szellemi tulajdon: A törvény szerint az eredeti számítógépes program az azt létrehozó személy vagy vállalat szellemi tulajdona. A számítógépes programokat

szertői jogi törvény védi, amely kimondja, hogy az ilyen művek engedély nélküli másolása törvénybe ütköző cselekedet.

b) Szoftver licencszerződés: Egy adott szoftver esetében a licencszerződés határozza meg a szerzői jog tulajdonosa által megengedett szoftverhasználat feltételeit. A szoftverhez adott licencszerződésre külön utalás történik a szoftver dokumentációjában, vagy a program indításakor megjelenő képernyőn is. A szoftver ára tartalmazza a szoftver licencét, és megfizetése kötelezi a vevőt, hogy a szoftvert kizárólag a licencszerződésben leírt feltételek szerint használja.

c) Jogosulatlan másolás: A szoftver licencszerződés, amennyiben eltérően nem rendelkezik, a vevőnek csak egyetlen "biztonsági" másolat készítését engedélyezi, arra az esetre, ha az eredeti szoftver lemeze meghibásodna, vagy megsemmisülne. Az eredeti szoftver bármely további másolása jogosulatlan másolásnak minősül, és megsérti a szoftvert védő és használatát szabályozó licencszerződést, valamint a szerzői jogi törvényt.

d) Illegális szoftverhasználat: Az illegális szoftverhasználat azt jelenti, hogy valaki egy számítógépes programot jogosulatlanul másol le és használ, ezzel megsértve a szerzői jogi törvényt, valamint a szerzőnek a szoftver licencszerződésben leírt feltételeit. Aki szoftvert illegálisan használ, az a szerzői jogi törvény értelmében büntetőjogi törvénybe ütköző cselekedetet követ el.

e) Új szoftver beszerzések: Az egyedi beszerzéssel, ajándékozással, pályázat útján megszerzett szoftver. Amennyiben egy eszköz beszerzése során az ár már tartalmazza (OEM- Originál Equipment Manufacturer) a szoftver árát. Már meglévő termék frissítése (UPGRADE), vagy bármilyen más törvényes módon megszerzett szoftver.

(3) Szoftverek nyilvántartása

Az egységek nyilvántartásának tételesen fel kell sorolnia – amennyiben licencszerződés nem tiltja - a rendelkezésére álló szoftver licenceket az alábbi adatok feltüntetésével:

- a) tételazonosító sorszám;
- b) a szoftver gyártója;
- c) a szoftver neve;
- d) a szoftver verziószáma;
- e) a szoftver leírása;
- f) a szoftverazonosító sorszáma, szériaszáma;
- g) a szükséges hardver környezet;
- h) a szükséges operációs rendszer, szoftverkörnyezet;
- i) a licenc feltételei: Kik, hányan, hány számítógépen, mettől, meddig használhatják;
- j) a szoftver típusa (OEM, frissítés);
- k) ezen szoftver alapján frissített szoftver tételazonosítójának sorszáma;
- m) a dokumentációt, illetve az eredeti adathordozót birtokló szervezeti egység megnevezése.

Adatbiztonsági rendszabályok

14. §

(1) Általános rendelkezések

a) Az üzemeltetői jogosultságok által megszerezhető, ill. a tevékenységek naplózásával, a forgalom ellenőrzésével, továbbá más számítástechnikai eszközökkel gyűjtött információk csak az MKSZ működésének javítására, a rendellenes használat kiszűrésére, a szabálysértő magatartás felderítésére

használhatók. Egyéb célokra való információgyűjtésre vagy felhasználásra az MKSZ elnöke adhat utasítást.

b) Adatvédelmi tv. 10. § (1) Az adatkezelő, illetőleg tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek e törvényt, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.

c) Az adatokat - kiemelten az államtitokká és a szolgálati titokká minősített személyes adatot - védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, nyilvánosságra hozás vagy törlés, illetőleg sérülés vagy a megsemmisülés ellen.

d) Az adatbiztonsági rendszabályok érvényesítése érdekében a szükséges intézkedéseket meg kell tenni mind a manuálisan kezelt, mind a számítógépen tárolt és feldolgozott személyes adatok biztonsága érdekében.

(2) Számítógépen tárolt adatok

A számítógépen, illetve hálózaton tárolt személyes adatok biztonsága érdekében, különösen az alábbi intézkedéseket kell fogatosítani:

a) Tükrözés: A hálózati kiszolgáló gépeken a tárolt adatok biztonsága érdekében minimum RAID 1-et kell biztosítani..

b) Biztonsági mentés: A személyes adatokat tartalmazó adatbázisok aktív adataiból rendszeresen, havonta kell külön adathordozóra biztonsági mentést készíteni. A biztonsági mentést tartalmazó adathordozót tűzbiztos fémkazettában kell őrizni.

c) Archiválás: A személyes adatokat tartalmazó adatbázisokat időtálló adathordozón kell rögzíteni, melyet évente minimum egyszer el kell végezni. Az archivált adatokat tartalmazó adathordozót tűzbiztos fémkazettában kell őrizni.

d) Tűzvédelem: Az adatokat és adatbázisokat tűzvédelmi és vagyonvédelmi berendezésekkel ellátott helyiségben kell elhelyezni.

e) Vírusvédelem: Minden – az MKSZ hálózatára bármilyen módon csatlakozó – számítógépen a felhasználónak biztosítani kell a vírusvédelmet. Az intézményben található számítógépeken működtetni kell vírusvédelmi szoftvert. A felhasználó nem akadályozhatja az MKSZ munkatársai által beállított automatizált frissítést. AZ MKSZ kijelölt munkatársa (i) gondoskodik a levelezőrendszer vírus- és spam szűréséről.

f) Hozzáférés-védelem: Az adathozzáféréshez csak érvényes, személyre szóló, azonosítható jogosultsággal - legalább felhasználói névvel és jelszóval - lehet hozzáférni. Hálózati erőforrásokhoz csak érvényes felhasználói névvel és jelszóval lehet hozzáférni.

g) Hálózati védelem: A mindenkor rendelkezésre álló számítástechnikai eszközök felhasználásával meg kell akadályozni, hogy adatokat tároló, hálózaton keresztül elérhető szerverekhez illetéktelen személy hozzáférjen.

Laczhegyi László
világi elnök