8-7/2016

7/2016. (I.4.) számú szabályzat
A Magyarországi Románok Országos Önkormányzat hivatal informatikai eszközeinek alkalmazásáról és az adatbiztonság biztosításáról

A Magyarországi Románok Országos Önkormányzat Hivatal nevében az állami és önkormányzati szervek információbiztonságáról szóló 2013. évi L. törvény 2. § (1) bekezdés k) pontja, és további rendelkezéseinek végrehajtása érdekében az Önkormányzati Hivatal (a továbbiakban: MROÖ Hivatal) információs rendszerei biztonságos üzemeltetésének biztosítása érdekében a következő szabályzatot teszem közzé és rendelem alkalmazni:

I. Bevezető rendelkezések

Az **Informatikai és adatbiztonsági szabályzat (továbbiakban: ISz)** alapvető célja, hogy a számítástechnikai berendezések, és eszközök alkalmazása során biztosítsa az MROÖ Hivatalnál:

a) a hardver- és szoftvereszközök rendeltetésszerű használatát;
b) az adatbiztonságot;
c) az üzemszerű működés fenntartásához a karbantartást és folyamatos fejlesztést;
e) az önkormányzat honlapjának működtetését;
f) a hardver- és szoftvereszközök üzemeltetéséhez szükséges dokumentációk nyilvántartását.

A Szabályzat hatálya kiterjed az MROÖ Hivatal épületében dolgozó valamennyi munkatársra, akik a hivatal számítástechnikai rendszereinek működése során a rendszerrel kapcsolatba kerülhetnek.

II. Számítógépek, számítógépes rendszerek, hardverek

Beszerzés, telepítés

1) A számítógépek, hardverek beszerzését az MROÖ Hivatal igényei és a hozzájuk kapcsolódó feladatok pontos ismeretében kell elvégezni. Körültekintően kell felmérni a jelenlegi feladatokon kívüli , a jövőben jelentkező teendőket.

2) A számítástechnikai eszközök telepítése, elhelyezése, az előírásoknak megfelelő üzembe helyezése a hivatalvezető, vagy az általa megbízott személy feladata.
A gépek elhelyezésekor figyelembe kell venni a tűzvédelmi és az elektromos berendezések elhelyezésére vonatkozó előírásokat, valamint az ergonómiai szempontokat is. Ahol lehetséges külön erre a célra kialakított számítógép-asztalokat kell beszerezni.

3) A gépek üzembe helyezése után a kijelölt munkatárs gondoskodik a gépekhez tartozó telepítő lemezek és dokumentációjuk gondos megőrzéséről.

4) A számítógépeket, azok részegységeit függetlenül attól, hogy üzemeltetésük során jelentkeznek-e működési üzemzavarok vagy sem, rendszeresen ellenőrizni kell. A karbantartási munkát évente legalább egyszer el kell végezni. A karbantartási munkák elvégzése az informatikai feladatokkal megbízott munkatárs feladata.

III. Szoftverek

A programok beszerzése, telepítése

A programok beszerzése előtt először meg kell vizsgálni azokat a feladatokat, amelyeket a programmal kívánunk megoldani. A feladat nagyságától függően ki kell kérni az érintett terület szakembereinek véleményét. A programok árban, tudásban, szakmai, működési biztonságban eltérőek lehetnek, ezért a beszerzés gondos előkészületet kíván.

Beszerzésnél minden esetben figyelembe kell venni:

- a szoftvergyártó cég rendelkezik-e megfelelő referenciákkal,

- funkcionálisan a program kielégíti-e a feladat igényeit, nem tartalmaz-e felesleges egyéb funkciókat,
- milyen létszámú és milyen felkészültségű személyzetre van szükség,
- biztosított-e a szoftver követése, azaz a jogszabályi változásokat követik-e, az így született verziókat milyen feltételek mellett bocsátják az MROÖ Hivatal rendelkezésére,
- amennyiben az MROÖ Hivatalnak egyedi programmódosítási igényei lennének, azt a gyártó vállalja-e és milyen feltételekkel,
- a gyártó cég milyen segítséget tud nyújtani a program bevezetésében, az üzemeltetés során felmerülő hibák, üzemzavarok elhárításában,
- milyen hardvert igényel a program üzemeltetése,
- a program nyújtotta szolgáltatások arányban vannak-e a szoftver árával.

Telepítés, üzemeltetés biztonsági szabályai: A beszerzett szoftverek telepítését kizárólag az MROÖ Hivatal kijelölt informatikai munkatársa, vagy a szoftvergyártó cég szakemberei végezhetik.
Új szoftver bevezetésekor nagy hangsúlyt kell fektetni a programot működtető személyek feladatainak leírására, szakszerű kiképzésére, oktatására, egyúttal el kell készíteni a kezelési útmutatókat és működési szabályzatokat, amelyeket a programot kezelő személyeknek be kell tartani.

IV. Titok és adatvédelem

Titokvédelem: Az adatokhoz, információkhoz való hozzáférést a számítógépes felhasználói rendszerben a bejelentkezési azonosítók használata teszi lehetővé.
1) Azonosítókkal kell elhatárolni, hogy ki milyen adatokhoz férhet hozzá. A jogosultságok megváltozását és betartását a hivatalvezető ellenőrzi.

2) A számítógép felhasználók részére, az egyes szakrendszerekhez – különösen a pénzügyi jellegű rendszerekhez - történő hozzáférést biztosító azonosító kódokat és jelszavakat, elkülönített módon zárt borítékban, a pénztár páncélszekrényben kell elhelyezni.
A boríték felbontására kizárólag a munkavállaló, illetőleg ellenőrzés esetén a hivatalvezető jogosult a felbontás tényének jegyzőkönyvben való rögzítése mellett. A jelszó, azonosító kód tulajdonosának betegsége, tartós távolléte esetén a helyettesítő személynek új azonosítót kell adni; a helyettesített munkatárs azonosítójának felhasználása semmilyen körülmények között nem megengedett.

4) A pénzügyi-számviteli szoftverek felhasználói jelszavait a vonatkozó előírásoknak megfelelően kötelező cserélni. Az új jelszavakat borítékban gyűjtik, majd azt követően aktualizálják a pénzügyi rendszeren belül. A borítékban tárolt új jelszavakat a pénztár páncélszekrényében kell elhelyezni, az előző időszak lejárt jelszavainak megsemmisítése mellett.
Pénzügyi és számviteli adatokat kizárólag védett, csak erre a célra szolgáló internet-vonalon keresztül lehet továbbítani. Az adatkezelést és feldolgozást kijelölt pénzügyi munkatárs végzi, hozzáférési jogosultságait az adatkezelő szerv védi és biztosítja. A pénzügyi/számviteli adatok tárolásáról, védelméről az adatkezelő szerv gondoskodik.

Mentések (adatvédelem): Az adatok, adathordozók fizikai és logikai védelméről fokozottan kell gondoskodni. A mentések automatikusan történnek, a teljes szerverállomány háttértárolóra való mentésével.

Vírus és kéretlen levél védelem: A hatékony vírusvédelem érdekében megfelelő vírusirtó programot kell üzembe helyezni, amely a hálózati munka sajátosságainak megfelelőn képes vírusvédelemre.
A vírusvédelem kiterjed az MROÖ Hivatal minden számítástechnikai berendezésére. A vírusvédelem, illetve a vírusmentesítés az informatikai feladatokkal megbízott munkatárs feladata.
A vírusfertőzések elkerülése érdekében be kell tartani az alábbi szabályokat:
- szoftvert az informatikus munkatárs vagy a hivatalvezető telepíthet. Semmilyen magánjellegű, előzetesen nem engedélyezett program nem futtatható az MROÖ Hivatal berendezésein;

- az internetről kizárólag a feladat ellátáshoz szükséges anyagok tölthetők le a származási hely gondos ellenőrzése mellett. Kétség esetén az informatikai feladatokat ellátó munkatárs segítségét kell kérni;
- minden számítógépen megfelelő tűzfalnak és aktív vírusvédelemnek kell üzemelnie. A vírusvédelem frissítését automatikus üzemmódra kell állítani;
- az elektronikus levelezést, központi felügyelettel, automata vírusszűréssel és automata kéretlenlevél szűréssel un. (SPAM) kell megvalósítani.
- vírus fertőzés észlelése esetén haladéktalanul abba kell hagyni a munkát, és szólni kell az informatikai munkatársnak, aki gondoskodik a vírus szakszerű eltávolításáról;
- az elektronikus levelekhez csatolt nem hitelesített állományokat azonnal, elolvasás nélkül törölni kell, hasonlóképpen az ismeretlen forrásból származó levelekhez.
- a géppark operációs rendszereinek frissítését automatikusan kell megoldani.

V. Információs rendszerbiztonság

1) Az MROÖ Hivatal információs rendszerének biztonságáért a hivatalvezető felel. Feladata az informatikai szabályzatok elkészítése és kiadása, adatszolgáltatás a Nemzeti Elektronikus Információbiztonsági Hatóság és más, ellenőrzést végző szervezetek felé.
Feladata továbbá az elért információs rendszerbiztonsági szint fenntartása, továbbfejlesztése, megoldások kidolgozása, kidolgoztatása, alkalmazása, bevezetése.

2) Az MROÖ Hivatalban a következő információs rendszerek működnek:
- Nemzeti jogszabálytár,
- Köznevelési Információs Rendszer (KIR),
- Integrált Költségvetési Gazdálkodási Rendszer (CQR) CGR
- DMSone Professional iktató program,
- Központi Illetményszámfejtő rendszer (KIR),
- Költségvetési Gazdálkodási Rendszer (KGR),
- E- adat rendszer
- Integrált Költségvetési Gazdálkodási Rendszer (CGR) ?
- Vállalati elektronikus csatorna (ELEKTRA)
- szerződés és kötelezettség nyilvántartó rendszer.

Bizalmasság: az elektronikus információs rendszer azon tulajdonsága, hogy a benne tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról.

Rendelkezésre állás: annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek.

Sértetlenség: az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az az elvárt forrásból származik (hitelesség) és a származás ellenőrizhetőségét, bizonyosságát (letagadhatatlanságát) is, illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható.

VI. Hatályba léptető rendelkezések

Jelen szabályzat 2016. január 4. napján lép hatályba.

Gyula, 2016. január 4.

Kozma György
hivatalvezető

Magyarországi Románok Országos Önkormányzata Hivatala GYULA

Elolvasta és az abban foglaltakat tudomásul vette
2016.01.04.

2016.01.25