Előterjesztés Csákvár Város Önkormányzata Képviselő-testülete
2014. április 8-i nyilvános / zárt ülésének

5.napirend (TFB:----)(HEB:---) ((PJB:5.)

Tárgy: A Csákvári Közös Önkormányzati Hivatal informatikai biztonsági szabályzatának elfogadása
Az előterjesztést készítette: dr. Fillér László önkormányzati és társulási irodavezető, Wilmek Ferenc informatikus
Előterjesztő: Katonáné dr. Venguszt Beatrix polgármester

Tisztelt Humán Erőforrás Bizottság!
Tisztelt Pénzügyi és Jogi Bizottság!
Tisztelt Képviselő-testület!

„Az állami és önkormányzati szervek elektronikus információbiztonságáról" szóló 2013 évi L. törvény és a végrehajtására kiadott „ a Nemzeti Elektronikus Információbiztonsági Hatóság és az információbiztonsági felügyelő feladat- és hatásköréről, valamint a Nemzeti Biztonsági Felügyelet szakhatósági eljárásáról" szóló 301/2013.(VII.29.) Korm. rendelet hatálya kiterjed a helyi és nemzetiségi önkormányzatokra is.
Az elektronikai információs rendszereket biztonsági osztályba kell sorolni, a besorolást 3 évente felül kell vizsgálni. El kell fogadni az informatikai biztonsági szabályzatot és ezt, valamint az információs rendszer biztonságáért felelő személy adatait, elérhetőségét meg kell küldeni a Nemzeti Elektronikus Információbiztonsági Hivatalnak.
A fenti kötelezettségek elmulasztása bírságot vonhat maga után.

A fentiek alapján a mellékelt informatikai biztonsági szabályzat elfogadását indítványozom, továbbá felhatalmazást kérek az érintett személy adatainak bejelentésére, illetve a Közös Önkormányzati Hivatal biztonsági osztályba sorolására.

Csákvár, 2014. március 26.

Katonáné dr. Venguszt Beatrix sk.
polgármester

Határozati javaslat

Csákvár Város Önkormányzata Képviselő-testülete
…../2014. (IV. 08.) határozata
informatikai biztonsági szabályzat elfogadásáról

Csákvár Város Önkormányzatának Képviselő-testülete felhatalmazza a polgármestert, hogy a Csákvári Közös Önkormányzati Hivatal informatikai biztonsági besorolását végezze el és ennek eredményét valamint az informatikai biztonságért felelős személy adatait közölje az illetékes hatósággal.

A Képviselő-testület elfogadja a Csákvári Közös Önkormányzati Hivatal Informatikai Biztonsági Szabályzatát az alábbiak szerint:

1. sz. melléklet

CSÁKVÁRI KÖZÖS ÖNKORMÁNYZAI HIVATAL INFORMATIKAI BIZTONSÁGI SZABÁLYZATA

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény 15. § (1) bekezdés d) pontjában, az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény 24. § (3) bekezdésében, valamint a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992. évi LXVI. 30. § (1) bekezdésében kapott felhatalmazás alapján a Csákvári Közös Önkormányzati Hivatal (a továbbiakban: **Hivatal**) informatikai biztonsági szabályzatát az alábbiakban határozom meg:

A szabályzat célja

1.) A szabályzat célja, hogy az adatvédelmi törvény, az adatbiztonság érvényesítése, az egyes szoftverekhez való hozzáférési jogok meghatározása, az ellenőrzési mechanizmusok meghatározása, a felelősségi viszonyok tisztázása, az egyes adatkezelő műveletek részletezése az adatvédelmi szabályzattal, az iratkezelési szabályzattal, illetve a vonatkozó jogszabályi előírásokkal összhangban történjen.

A szabályzat hatálya

2.) A szabályzat tárgyi hatálya kiterjed a Hivatal tevékenysége során keletkezett, kezelt, feldolgozott, tárolt adatokra és információkra, a számítástechnikai eszközbázisra, ezek okmányaira, leírására és környezetére, a szoftverekre, adatbázisokra és a kapcsolódó dokumentációkra, az adatbiztonsági nyilvántartásokra.

3.) A szabályzat személyi hatálya kiteljed a Hivatal köztisztviselőire, ügykezelőire, munkavállalóira, illetve egyéb munkavégzésre irányuló jogviszonyban álló személyekre, a Hivatallal szerződéses kapcsolatban álló vállalkozókra, azok alvállalkozóira és ezek alkalmazottaira. Ha a Hivatal más személynek (pl. Képviselő) is lehetőséget biztosít bármely informatikai rendszerének használatára, akkor rá nézve is kötelező a szabályzatban foglaltak betartása. (A továbbiakban együtt felhasználók.)

Alapfogalmak

Adat: mindazon számítástechnikai eszköz által, illetve annak közreműködésével üzemeltetett, rendszerezett információhalmaz, mely a Hivatal tevékenységét szolgálja.

Adatbiztonság: az elektronikus illetve egyéb úton tárolt információk hozzáférhetőségének szintjét határozza meg az adatok által képviselt érték szerint.

Adatfeldolgozás: azon munkafolyamatok összessége, melyek során a Hivatal a munkájában felhasznált információkat megalkotja, megszerzi és azokat rendszerezetten feldolgozza.

Adatvédelem: azon biztonsági tényezők összessége, melyek az adatok illetéktelenek általi hozzáférés, természeti csapás, rongálás, lopás kockázati tényezőit megszünteti (csökkenti), továbbá biztosítja az üzemfolytonosságot.

Veszély: a Hivatal informatikai területeit érő negatív hatások általi potenciális károkozás lehetősége.
Informatikai rendszer: azon eszközök (szoftver, hardver, dokumentáció) összessége, melyek fizikai tulajdonságaik alapján determinálják az információ feldolgozás képességét és minőségét.

Rendelkezésre állás: kifejezi az informatikai és információs rendszer adott szintjéhez való jogosult hozzáférés gyorsaságának és biztonságának mértékét.

Rendszergazda: a Hivatal a rendszergazdai tevékenységeit teljes állású informatikus látja el.

Upgrade: szoftver újabb verziója.

Inkrementális mentés: olyan mentés, amely egy teljes mentés után csak az ehhez képest történt változások mentését végzi el.

Log fájl: adott program eseménynapló bejegyzéseit tartalmazó fájl. OEM szoftver: adott számítógéphez kötött licencellésű szoftver.

Hálózat, számítógép hálózat: olyan speciális rendszer, amely a számítógépek egymás közötti kommunikációját biztosítja.

Monitorozás: rendszeres információgyűjtés és elemzés.

Szervezeti egység: osztály, Ellenőrzési Csoport.

4.) Szabályozási területek bontása

Intézkedés megnevezése	Megjegyzés:
Bevezető rész	Általános megfogalmazások és definíciók kerülnek benne kialakításra, mely a ráépülő, analitikus szabályrendszerek alapját képezi.
A szoftverhasználat rendje, szoftvernyilvántartás	I. fejezet
A hálózathasználat szabályai	II. fejezet
A jelszókezelés szabályai	III. fejezet
A levelezés szabályai	IV. fejezet
A vírusvédelem szabályai	V. fejezet
A távoli elérés szabályai	VI. fejezet
A' szerverek biztonsági szabályai	VII. fejezet
A felhasználók regisztrálásának szabályai	VIII. fejezet
A mentés és archiválás szabályai	IX. fejezet
Katasztrófakezelési terv	X. fejezet

I.fejezet A szoftverhasználat rendje, szoftvernyilvántartás

I.

1.) A szerzői jogról szóló 1999. évi LXXVI. törvény l.§ (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.

2.) Aki másnak a szerzői jog által védett számítógépes szoftverén fennálló szerzői vagy szerzői joghoz kapcsolódó jogát haszonszerzés végett, vagy vagyoni hátrányt okozva megsérti, a Büntető Törvénykönyvről szóló 2012. évi C. törvény 385. § szerinti bűncselekményt valósítja meg.

3.) A Hivatal a szoftverhasználat feltételeit az alábbi alapelvek mentén valósítja meg:

- minden indokolt és engedélyezett szoftverigény kielégítésére a Hivatal jogtiszta szoftvert biztosít az összes számítógépre, a megfelelő időben és a szükséges mennyiségben,
- a Hivatal külső cégtől vásárolja meg a számítógépes szoftverek licenc (használati) engedélyét, a Hivatal a licencszerződéssel nem válik ezen szoftverek tulajdonosává és azok dokumentációját és adathordozóit a szoftver fejlesztőjének külön engedélye nélkül nem áll jogában reprodukálni,
- a Hivatal eleget tesz minden olyan licenc vagy vásárlási feltételnek, amely a beszerzett vagy használt szoftverek felhasználását szabályozza,
- a Hivatal felhasználói a lokális hálózatokon vagy a munkaállomásokon a szoftvereket kizárólag a licencszerződésnek megfelelően használhatják,
- amennyiben a Hivatal felhasználóinak tudomására jut, hogy valamely szoftvert, vagy azzal kapcsolatos dokumentációt nem a jelen szabályzatban foglaltak szerint használják, akkor azt kötelesek jelenteni felettes vezetőjüknek,
- a jogosulatlan szoftvermásolatok készítésének, illetve jogosulatlan szoftverhasználat megakadályozása érdekében a rendszergazda ellenőrzést végez.

4.) Tilos:

- a szoftvert, vagy annak dokumentációját, beleértve a programokat, alkalmazásokat, adatokat, kódokat és kézikönyveket a szerzői jog tulajdonosának engedélye nélkül lemásolni vagy terjeszteni;
- a szerzői jog által védett szoftvert egyidejűleg két vagy több gépen futtatni, hacsak ezt a szoftver licencszerződése külön nem engedélyezi;
- a Hivatal tulajdonában álló szoftvert más részére átadni, arról másolatot készíteni.

A szervezeti egység vezetője felel az érintett szervezeti egységeknél az ott elhelyezett eszközök tekintetében a legális szoftverhasználatért, amit jelen szabályzat betartásával és betartatásával valósít meg.

A Hivatal nevében beszerzett licencek hasznosításáról - amennyiben azt licencszerződés lehetővé teszi - az informatikáért felelős szervezeti egység vezetőjének javaslata alapján a jegyző dönt.

Az informatikáért felelős rendszergazda és irodavezető gondoskodik a jogtiszta szoftverhasználat érdekében történő alkalomszerű, - de legalább évenkénti - ellenőrzésről. Az ellenőrzésekről jegyzőkönyv készül, az esetleges intézkedések megtételre a jegyző részére javaslatot tesznek.

A rendszergazda szoftverhasználattal kapcsolatos kötelességei és jogai:

A rendszergazda kötelességei:

- a számítógép által futtatott szoftverek telepítése, konfigurálása a felhasználó(k) igényei szerint;
- a számítógépre az általa telepített szoftverek jogtisztaságáért a rendszergazda vállalja a felelősséget;
- a telepítés során tájékoztatja a felhasználót, a szervezeti egység vezetőjét a szoftver licencében rögzített jogokról és kötelezettségekről;
- amennyiben a szoftvert a gyártó telepíti, akkor ezt - amennyiben feltételei fennállnak - csak rendszergazda jelenlétében végezheti. Az egyedi fejlesztésű programok gyártó által történő telepítése esetén a rendszergazda ellenőrzi, hogy csak a szerződésben szereplő legális szoftverek kerülnek telepítésre;
- ~ a már meglévő szoftvereket azonnali hatállyal nyilvántartásba venni, a szoftverállományban történő változást a nyilvántartásban folyamatosan aktualizálni kell;

- a beszerzett új szoftver adatait az informatikai feladatok ellátásáért felelős szervezeti egység által karbantartott adatbázisba kell felvenni 30 napon belül a kötelező adatszolgáltatás eredményeképpen;
- a rendszergazda rendszeresen ellenőrzi e szabályzat rendelkezéseinek betartását.

A rendszergazda jogai:

- az a) pontban meghatározott tevékenységek elvégzésére csak a rendszergazda - vagy az általa megbízott személy (vállalkozó, alvállalkozó) - jogosult;
- rendszergazda a számítógép használójának felügyelete mellett rendszeresen és alkalomszerűen ellenőrzi az adott szervezeti egységen belül a szoftverek legalitását, e szabályzat rendelkezésének betartását. Az ellenőrzésről jegyzőkönyvet készít, amelyet az informatikai feladatok ellátásáért felelős szervezeti egység vezetőjének ad át.
- Amennyiben a rendszergazda jogait korlátozzák, annak okait az informatikáért felelős szervezeti egység vezetőjének írásban be kell jelenteni.

A szoftver 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 szoftver azonosító 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, stb.);
k) ezen szoftver alapján frissített szoftver tétel azonosítójának sorszáma; 1) a dokumentációt, illetve az eredeti adathordozót birtokló szervezeti egység megnevezése.

II. fejezet A hálózathasználat szabályai

1.) A hálózat használatának szabályai:

A Hivatal hálózata nem használható az alábbi tevékenységekre:

- a mindenkor hatályos jogszabályokba ütköző cselekmények előkészítése vagy végrehajtása, így különösen mások személyiségi jogainak megsértése, tiltott haszonszerzésre irányuló tevékenység, szerzői jogok megsértése;
- -profitszerzést célzó, üzleti célú tevékenység és reklám;

- a hálózat, a kapcsolódó hálózatok, illetve ezek erőforrásainak rendeltetésszerű működését és biztonságát megzavaró, veszélyeztető tevékenység, ilyen információknak és programoknak a terjesztése;
- a hálózatot, a kapcsolódó hálózatokat, illetve erőforrásokat indokolatlanul igénybevevő tevékenységek;
- a hálózat erőforrásaihoz, a hálózaton elérhető adatokhoz történő illetéktelen hozzáférés, azok illetéktelen használata, gépek/szolgáltatások - akár tesztelés céljából történő - túlzott mértékben való szisztematikus próbálgatása;
- a hálózat erőforrásainak, a hálózaton elérhető adatoknak illetéktelen módosítása, megrongálása, megsemmisítése vagy bármely károkozásra irányuló tevékenység;
- másokra nézve sértő, vallási, etnikai, politikai vagy más jellegű érzékenységét bántó, zaklató tevékenység;
- hálózati üzenetek, hálózati eszközök hamisítása: olyan látszat keltése, mintha egy üzenet más gépről vagy más felhasználótól származna.

2.) Felelősök:

A rendszergazda kontrollálja a hálózat egyes részeinek, szolgáltatásainak működését, rendeltetésszerű és szabályos használatát, valamint felelnek a biztonsági előírások betartásáért és betartatásáért. A szabályzat megsértőit, a szabályzat megsértésének bizonyítékaival együtt az informatikáért felelős szervezeti egység vezetőjének be kell jelenteni.

3.) A felhasználók kötelességei:

- A felhasználók kötelessége a szabályzat megismerése és az abban foglaltak betartása, valamint együttműködés a hálózat üzemeltetőivel a szabályzat betartatása érdekében.
- A felhasználó viseli a felelősséget minden műveletért, amely az adott felhasználói azonosítóval kerül végrehajtásra.

- A felhasználók jogai:

- Minden hivatali dolgozónak joga van saját felhasználói fiókhoz és levelezéshez (e- mail címhez) és a munkavégzéshez szükséges web szolgáltatáshoz.
- A felhasználónak joga van a felhasználói fiókhoz való hozzáféréshez. A Hivatal ezt a hivatali munkaállomásokon teszi lehetővé.
- A felhasználó személyiségi jogait és a levéltitkot a hálózat üzemeltetői tiszteletben A felhasználók kötelessége a szabályzat megismerése és az abban foglaltak betartása, valamint együttműködés a hálózat üzemeltetőivel a szabályzat betartatása érdekében.
- tartják, ettől eltérni csak jogszabály által meghatározott esetekben lehet. A rendszer technikai karbantartásairól (tervezett vagy rendkívüli eseményekről) tájékoztatni kell a felhasználókat, tervezett karbantartás esetében *ezt* úgy kell megtenni, hogy elegendő idő maradjon a felhasználók felkészülésére. A karbantartásokat lehetőleg hivatali munkaidőn kívül kell lebonyolítani.

4.) Szankciók:

A szabályzat megsértésének gyanúja esetén az esetet ki kell vizsgálni, és a kijelölt felelősnek meg kell tennie a szükséges intézkedéseket, amelyre a következők az irányadók:

-a szabályzat gondatlan megszegése esetén az elkövetőt írásbeli figyelmeztetésben kell részesíteni.

- a szabályzat szándékos megsértése esetén az elkövető a hálózat használatából ideiglenesen vagy véglegesen kizárható.
- a elkövető köteles megtéríteni az általa okozott károkat a Polgári Törvénykönyv előírásai szerint.

III. fejezet A jelszókezelés szabályai

1.) A jelszó a hozzáférés kezelés alapvető eszköze, így az informatikai biztonság fontos része. Az informatikai rendszer minden felhasználójának tisztában kell lennie a jelszó fontosságával és a nem megfelelő jelszókezelés következményeivel, mert egy rosszul megválasztott, könnyen kitalálható jelszó nemcsak a jelszó tulajdonosára, hanem a Hivatal informatikai rendszerére is negatív következményekkel járhat.
2.) A jelszavak két csoportja szerint adminisztrátori vagy egyszerű felhasználói jogú azonosítót véd a jelszó, a szabályozás ennek függvényében eltérhet, az adminisztrátori jelszavakhoz mindig a szigorúbb szabályok érvényesek.

3.) Alapelvek

- Tilos könnyen kitalálható jelszavakat választani.
- A jelszavakat titokban kell tartani.
- Az induló jelszót az első bejelentkezéskor meg kell változtatni.
- Ha a felhasználónak gyanúja támad, hogy jelszava kompromittálódhatott, azonnal meg kell változtatnia.
- 5 sikertelen próbálkozás után a felhasználói fiók zárolandó.
- A jelszavakat nem szabad kódolatlanul tárolni.
- Azon személyeknek, akik különböző rendszerekhez, illetve több felhasználói azonosítóval is rendelkeznek, a különböző rendszerekhez, azonosítókhoz különböző jelszavakat kell használniuk.
- Ahol lehetséges, a jelszavakra vonatkozó alapszabályokat (jelszóhossz, jelszócsere, előző jelszavak megadásának tilalma) az adott informatikai rendszer segítségével ki kell kényszeríteni, amely beállítások elvégzéséért az adott szakrendszer rendszergazdája felelős.
- A jelszavakat félévente (adminisztrátori jelszavaknál 3 havonta) cserélni kell.
- Új jelszónak nem szabad az utolsó 2 régi közül egyiket sem megadni.

4.) Helyes jelszóválasztás

- Tilos könnyen kitalálható, személyre jellemző jelszavakat használni.
- A jelszónak legalább 7 karakter hosszúnak kell lennie.
- Tilos sorozatokat használni (pl. abcdefg, 7654321, asdfghj).
- Kerülni kell a szótári szavak használatát (ezek egy számjeggyel kiegészített változatai sem biztonságosak).
- A jelszó tartalmazzon kis- és nagybetűket, számokat és speciális karaktereket is.
- A jelszónak könnyen megjegyezhetőnek kell lennie.

5.) Jelszó védelem

A felhasználók különös figyelmet kell, hogy fordítsanak az alábbiakra:

- A jelszót tilos másoknak elmondani, a jelszóról mások előtt beszélni.
- A jelszót a felhasználón kívül kizárólag a rendszergazda ismerheti.
- Tilos közös jelszavakat használni.
- A jelszót nem szabad leírni, és elérhető helyen tárolni.

- A jelszót nem szabad semmilyen számítógépes rendszeren titkosítás nélkül tárolni.
- A jelszót nem szabad telefonon vagy e-mail-ben továbbítani.
- Ne használjuk a programok jelszó megjegyző funkcióját.
- A jelszavunkat ne írjuk be kérdőívekbe, űrlapokba.
- Ha a jelszó kompromittálódott, vagy erre utaló jeleket lehet észlelni, azonnal meg kell változtatni a jelszót és értesíteni kell a rendszergazdát.

6.) Felelősök, dokumentálás

- Azon informatikai rendszerek esetében, melyek támogatják a jelszavakra vonatkozó alapszabályok kikényszerítését a szükséges szabályok, paraméterek beállításáért az érintett informatikai rendszer rendszergazdája felel. A dokumentáció ebben az esetben az informatikai rendszer napló állománya.
- Azon informatikai rendszerek esetében, melyek nem támogatják a jelszavakra vonatkozó alapszabályok kikényszerítését az e fejezetben meghatározott elvek, szabályok betartásáért, valamint a jelszócserék dokumentálásáért a szervezeti egység vezetője a felelős.

IV. fejezet A levelezés szabályai

1.) A fejezetben foglaltak célja, hogy biztosítsák az elektronikus levelezés zavartalanságát, valamint védjék a Hivatal érdekeit. Minden felhasználónak és szervezeti egységnek lehetősége van <felhasznalo.nev>@csakvar.hu, illetve <szervezeti.egyseg.neve>@csakvar.hu című postafiókot igényelni, és ezt kizárólagosan hivatalos célra használni. A Hivatal e szabályokra figyelemmel monitorozhatja a hálózatából küldött, illetve ide érkező levelek tartalmát, az adatvédelmi szabályok és ajánlások figyelembevételével.

2.) A Hivatal hálózatán átmenő leveleken központilag vírus- és kémprogram ellenőrzés történik, ami különböző védelmi és szűrési funkciókkal egészül ki.

3.) A Hivatal hálózatán átmenő leveleken központilag SPAM ellenőrzés történik.

4.) A fejezetben foglaltak érvényesek minden levélre, amit a csakvar.hu tartományba eső e- mail címről küldtek.

5.) Alapelvek:

- A levelek nem tartalmazhatnak a hatályos magyar jogszabályokba ütköző tartalmat.
- A levelek nem sérthetik mások becsületét, emberi jogait, faji, nemzetiségi hovatartozását, vallási, politikai világnézetét.
- A levelek tartalma nem sérthet szerzői és szomszédos jogokat.
- A levelek nem ronthatják a Hivatal hírnevét, megítélését, nem terjeszthetnek róla szándékosan valótlan információkat.
- A levelezés nem veszélyeztetheti a hálózati infrastruktúra működését.

6.) Szabályok:

- Tilos kéretlen leveleket, hirdetéseket küldeni.
- Tilos a levélbombák, levelezési láncok küldése, illetve továbbküldése.
- Tilos a levelek fejlécének megváltoztatása, hamis levelek küldése.

- Tilos a levelezési címet olyan kereskedelmi listára feltenni, amelyről a hivatali levelező rendszert e-mail szeméttel (spam) terhelhetik meg.
- A Hivatal hálózatán belül maximum 35 Mb méretű levelek küldhetők. A Hivatal hálózatán kívülre küldött levelek esetében a továbbító és a fogadó szolgáltatók által beállított méretkorlátok érvényesülnek.
- Ismeretlen feladótól érkezett, különös témájú, csatolt fájlt tartalmazó leveleket körültekintéssel kell kezelni, ha a jelek vírusfertőzésre utalhatnak, törölni kell a levelet.
- Nagyméretű fájlokat tilos sok címzettnek küldeni, mert ez túlzott mértékben terheli a hálózat forgalmát, helyette publikus helyen kell elérhetővé tenni.

V. fejezet A vírusvédelem szabályai

1.) A számítógépes vírusok a számítógépen tárolt adatok és programok kártevői. A vírus a megfertőzött program futása közben másolja, többszörözi önmagát. Rendszerbe kerülésük történhet fertőzött lemeztől történő rendszerindítási kísérlet (bootvírusok), egy fertőzött program elindítása (fájlvírusok), egy vírusos makrókat tartalmazó dokumentum megnyitása (makróvírusok), egy fertőzött weboldal megnyitása vagy e-mail-ben csatolt állományként terjedő makró-, illetve script vírusok, férgek megnyitásának eredményeként. A vírusok gépről gépre terjednek, többnyire észrevehetetlenek, amíg nem aktivizálódnak. Ekkor azonban nagy kárt okozhatnak pótolhatatlan adatok megsemmisítésével, a rendszer bénításával, bizonyos esetekben hardveres károkozással. Ez a fejezet az előbbiekben felsorolt káros hatások megelőzésére, és a vírusfertőzés esetén-elvégzendő teendők leírására szolgál.

2.) Mivel a vírusok írói általában igyekeznek elkerülni a feltűnő viselkedést, a felhasználó nem feltétlenül találkozik az alább felsorolt - vírusfertőzésre utaló - jelenségekkel:

- A víruskereső program névvel azonosított vírust jelez. A lehető legerősebb vírusjegy.
- Fájl másolása esetén az újonnan keletkezett és az eredeti 'példány hossza eltérő. Nagyon erős vírusjegy.
-Szokatlan és váratlan képernyő tevékenység (szokatlan üzenetek, ablakok megjelenése). Erős vírusjegy.
- Szokatlan számítógép- vagy programviselkedés (pl. programok maguktól elindulnak). Általánosan erős vírusjegy.
- A rendszer működése többszöri újraindítás után is egyértelműen lassabb a megszokottnál. Átlagosan erős vírusjegy. Helytelen rendszerkonfiguráció is okozhatja.

3.) Vírusvédelmi teendők, a vírusfertőzések megelőzése, illetve azok kockázatának csökkentése érdekében betartandó szabályok:

- A Hivatal a vírusvédelmi feladatokat ingyenes, illetve fizetős szoftver (Norton) segítségével látja el.
- A vírusvédelemért felelős rendszergazda köteles minden hivatali számítógépen a szoftvert telepíteni és megfelelő konfigurálásáról gondoskodni.

~ A vírusvédelmi programnak rezidens módban kell futnia, így az minden egyes rendszerindításkor aktivizálódik, és állandó háttérvédelmet biztosít. A felhasználóknak tilos kikapcsolni ezt a védelmet.

- Havonta minden gépen teljes vírusellenőrzést kell végrehajtani időzített keresési funkció beállításával. Az időzített ellenőrzés beállításáért és a futási naplófájlok rendszeres ellenőrzésért a vírusvédelemért felelős rendszergazda felel.

- A vírusvédelmi program vírusdefiníciós adatbázisát a lehető leggyakrabban frissíteni kell (automatikus frissítés funkció beállításával).
- Idegen helyről származó adattárolókon használat előtt vírusellenőrzést kell végezni.
- Soha nem szabad ismeretlen vagy gyanús helyről fájlokat letölteni.
- Az Office csomag programjainál, ahol lehet, be kell állítani a makrók jelenlétének kijelzése funkciót. Idegen állományokat csak makrók futtatása nélkül opcióval szabad megnyitni.
- Ismeretlen, megbízhatatlan forrásból származó furcsa, gyakran vicces e-mail-ek csatolt fájljait nem szabad megnyitni, azonnal törölni kell őket (az e-mail-ben küldött vírusok, férgek rendszeresen operálnak valamilyen különös megjegyzéssel a levelek tárgy bejegyzésében).
- A fontos adatokról és a rendszerkonfigurációról készüljön archiválás.

4.) Teendők vírusfertőzés esetén:

- Tájékoztatni kell a vírusvédelemért felelős rendszergazdát a fertőzésről vagy annak gyanújáról.
- 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 (lehetőleg hálózati kapcsolat nélkül).
- A vírusvédelmi szoftver segítségével megszüntetjük a vírusfertőzést. Ez történhet elsődlegesen a fertőzött állomány javításával (a vírus eltávolítása), ha erre lehetőség van, egyébként a fertőzött állomány törlésével. Ez utóbbi esetben ügyelni kell arra, hogy nem rendszerállományról van-e szó.
- A víruskeresést addig kell végezni, amíg el nem éri a rendszerfelelős, hogy a víruskereső program úgy fusson végig az összes állományon, hogy fertőzött állományt már nem talál.

VI. fejezet A távoli elérés szabályai

1.) A fejezet célja, hogy meghatározza a Hivatal belső hálózatához távoli gépről történő csatlakozás szabályait. A cél a Hivatal hálózatának, informatikai rendszerének védelme a nem jogosult felhasználásból eredő károktól. A károk magukban foglalják az érzékeny adatok elvesztését, a Hivatal anyagi károsodását, illetve a Hivatal belső rendszerének sérülését.

2.) A Hivatal hálózatának távoli elérésére az egyes külső szerverek, munkaállomások távoli elérésének keretében van lehetőség (VPN, titkosított terminál kapcsolat, SQL).

3.) A távoli elérések szabályai:

- A bejelentkezés időtartamára a felhasználóra kötelezőek a jelen szabályzatban foglaltak.
- A távoli elérésnek biztonságos VPN kapcsolaton keresztül kell megvalósulnia.
- A rendszerbe való belépéshez szükséges a belépő személy azonosítása (felhasználói azonosító / jelszó megadása).
- A belépési azonosítókat másra átruházni, illetve más azonosítóját használni tilos.
- 5 egymás utáni sikertelen bejelentkezési kísérlet után a hozzáférést le kell tiltani.
- A bejelentkezéseket naplózni kell a tűzfalon. A naplózás beállításáért a hálózatért felelős rendszergazda felel.

VII. fejezet A szerverek biztonsági szabályai

A fejezet célja, hogy a Hivatal szervereire olyan követelményeket és alapbeállításokat határozzon meg, amik a biztonságos használatot elősegítik.

1.) A fejezet hatálya kiterjed minden a Hivatal tulajdonában, illetve felügyelete alatt levő szerverre, valamint a csakvar.hu tartomány alatt található önkormányzati tulajdonú szerverre.

2.) Alapelvek:

- A szervereket számítógépközpontban, zárt helyiségben kell elhelyezni. A szerverekhez való hozzáférést fizikailag is korlátozni kell.
- A szervereknek illetéktelen behatolástól jól védettnek kell lennie (megfelelő alapbeállítások használata, majd upgrade-k, biztonsági javítások mielőbbi telepítése).

~ A szerverek konzoljairól az adminisztrációs tevékenység befejeztével ki kell lépni, nem szabad felügyelet nélkül bejelentkezve hagyni.

- Indokolatlanul nem szabad adminisztrátori jogosultságokkal használni a szervert.
- A szervereken le kell tiltani minden nem használt szolgáltatást.
- A biztonsági mentéseket minden esetben a szervertől elkülönített helyiségben elzárva kell őrizni.
- A szerverhez, illetve szolgáltatásaihoz történő hozzáférési kísérleteket naplózni, és ezeket a naplókat rendszeresen ellenőrizni kell. A naplózás beállításáért és heti rendszerességű ellenőrzéséért a szerverekért felelős rendszergazda felel.
- A biztonsági eseménynaplókat - amennyiben a rendelkezésre álló tárhely lehetővé teszi - 90 napra, a mentéseit pedig 180 napra visszamenőleg meg kell őrizni. Amennyiben nem áll rendelkezésre megfelelő méretű tárhely az eseménynaplók 90 napig történő megőrzéséhez, úgy a megőrzési időt a biztonságos működést nem veszélyeztető lehető maximumban kell megállapítani a rendszergazdának.
- A jelentős biztonsági eseményeket be kell jelenteni az informatikáért felelős szervezeti egység vezetőjének.

VIII. fejezet A felhasználók regisztrálásának szabályai

Az informatikai rendszer használatával való visszaélés kizárása érdekében minden felhasználónak egyedi felhasználói azonosítóval és az ahhoz tartozó jelszóval kell azonosítania magát. Felhasználó a Hivatal dolgozója lehet, egyedi jegyzői engedély alapján külső személy is kaphat felhasználó azonosítót.

Alapelvek:

- A felhasználó azonosítók kiadása központilag a felelős rendszergazda által történik minden rendszer esetében.
- Felhasználó azonosítót az érintett szervezeti egység vezetőjének írásban kell igényelni, a 4. sz. melléklet szerinti informatikai megrendelő kitöltésével, és a szakrendszer rendszergazdájának történő megküldésével.
- Azonosító igénylésekor egyértelműen meg kell határozni a jogosultságot birtokló, azért felelősséggel tartozó személyt és az azonosítóhoz kapcsolódó hozzáférési jogosultságokat.
- A felhasználót az azonosító átadását megelőzően tájékoztatni kell a használat feltételeiről és szabályairól. A tájékoztatást követően a felhasználó aláírásával igazolja, hogy azokat megismerte és magára nézve kötelezőnek tekinti.

- Szakrendszerhez kapcsolódó felhasználói azonosító átadását megelőzően a felhasználót oktatásban kell részesíteni annak használatáról. Az oktatás az ügyiratkezelő rendszer esetében az azért felelős rendszergazda, míg más szakrendszer esetében az érintett szervezeti egység vezetője által kijelölt személy feladata.
- Adminisztrátori feladatokat ellátó személyek részére a normál felhasználói feladatok ellátására és adminisztrációs célokra külön azonosítót kell létrehozni.
- A különböző hozzáférési jogosultságok a felhasználó azonosítóhoz kapcsolódnak.
- Az azonosításnak (és ha szükséges a hitelesítésnek) meg kell előznie az informatikai rendszernek a felhasználóval kapcsolatos valamennyi más kölcsönhatását.
- A felhasználó azonosítót le kell tiltani, ha azzal visszaélés történt, és az esetet ki kell vizsgálni.
- A felhasználó azonosítókat a rendszerből törölni kell, ha a felhasználó már nem a Hivatal dolgozója, illetve már nincs az adott rendszer használatához joga. A törlést az érintett szervezeti egység vezetője a 4. sz. melléklet szerinti informatikai megrendelőn kezdeményezi a rendszergazdáknál.
- Az iratkezelési rendszer jogosultságai tekintetében az Iratkezelési Szabályzat rendelkezései az irányadóak.
- A rendszergazdák a felhasználói azonosítókról és kapcsolódó hozzáférési jogosultságokról teljes körű és naprakész nyilvántartással kell, hogy rendelkezzenek. A nyilvántartásnak tartalmaznia kell azon felhasználói azonosítókat és a kapcsolódó jelszavakat, hozzáférési jogosultságokat is, amelyek más, nem a Hivatal rendszereihez tartoznak, de valamely feladat kapcsán a Hivatal vagy a Hivatal dolgozója hozzáférést igényelt, kapott ahhoz (pl.: pályázati rendszerhez tartozó hozzáférés, Hivatali kapuhoz tartozó hozzáférés, stb.). A nyilvántartásba vételt az érintett szervezeti egység vezetője írásban kezdeményezi.

IX. fejezet A mentés és archiválás szabályai

1.) Az elektronikusan tárolt adatok folyamatosan ki vannak téve a hardver meghibásodási lehetőségének, ezért a biztonság növelése és a károk csökkentése érdekében szükség van rendszeres mentésekre. Míg a mentések fő feladata a biztonsághoz kapcsolódik, addig az archiválás egy korábbi állapot eltárolását szolgálja. Ez utóbbinak biztonsági incidensek bekövetkezése esetén lehet fontos szerepe, a napló és log fájlokban, valamint egyéb adatok között értékes információkat, nyomokat lehet találni a biztonsági esemény bekövetkezésével kapcsolatban.

2.) A fejezet hatálya kiterjed minden, a Hivatal tulajdonában, illetve felügyelete alatt levő szerverre, valamint a csakvar.hu tartomány alatt található összes szerverre.

3.) Feladatok:

- Az adatmentésekért felelős rendszergazda köteles minden szerveren szoftvert telepíteni és minden szakalkalmazás esetében az automatizált biztonsági mentéseket és azok naplózását konfigurálni.
- Az adatmentésekért felelős rendszergazda köteles a biztonsági mentések napló állományait naponta ellenőrizni, a mentések sikeres lefutását ellenőrizni.
- A mentések időzítését a hivatali munkaidőn kívülre kell beállítani.
- A mentések elsődlegesen disk alapú adathordozóra egy kizárólagosan erre a célra rendszeresített tárterületre, másodlagosan hordozható adathordozóra készülnek.
- Hetente teljes biztonsági mentést kell végezni minden rendszerről, a köztes időben pedig naponta inkrementális mentés készítése szükséges.
- A mentésekhez szükséges szalagos adathordozókat rotálni lehet.
- Havonta, évente teljes rendszerarchiválást kell készíteni, és ezeket megőrizni. Ehhez biztosítani kell a megfelelő számú szalagos adathordozó egységet.
- A havi és éves biztonsági mentéseket és archiválásokat tartalmazó adathordozókat minden esetben a szervertől elkülönített helyiségben elzárva kell őrizni, őrzésükre tűzbiztos, zárható szekrényt kell biztosítani és rajtuk jól láthatóan fel kell tüntetni a mentés típusát, idejét és az adathordozó sorszámát.
- A teljes mentéseket egy évig meg kell őrizni.

- Legalább évente visszatöltési kísérletet kell végezni a technika megfelelőségének ellenőrzése érdekében.

X. fejezet Katasztrófakezelési terv

1.) Informatikában a katasztrófa fogalom az informatikai rendszer - meghibásodás, áramkimaradás okozta - helyrehozhatatlan károsodását jelenti. Az ilyen veszélyeket, úgynevezett katasztrófa okokat nem lehet teljesen kivédeni, de hatásukat csökkenteni lehet. Az ilyen megelőző és elhárító tevékenységeket nevezzük katasztrófakezelésnek.

2.) A fejezet szabályait alkalmazni kell a Hivatal minden kritikus fontosságú rendszere esetén.

3.) Alapelvek:

Jegyző hatáskörébe tartozó:

- A katasztrófák megelőzése érdekében megfelelő hibatűrő rendszereket kell alkalmazni (szünetmentes tápegységek, hardveres RAID rendszerek alkalmazása), és rendelkezni kell tartalék eszközökkel.
- Katasztrófa helyzet fennállását a jegyző állapíthatja meg.
- A visszaállításra intézkedési ütemtervet kell készíteni, amely pontosan és részletesen tartalmazza az elvégzendő feladatokat, a hozzájuk kapcsolódó hardver és szoftver eszközök elérhetőségével együtt.
- Listát kell készíteni a legszükségesebb funkciókról és szolgáltatásokról, és elsődlegesen ezeket kell visszaállítani.
- Az intézkedési ütemtervet legalább évente, és minden jelentősebb változás bekövetkezésekor felül kell vizsgálni, és az abban foglaltakat a megváltozott körülményekhez igazítani.

Rendszergazda hatáskörébe tartozó:

- Rendszeresen biztonsági mentéseket kell készíteni.
- A rendszergazdák feladata egy értesítési lista összeállítása, ami tartalmazza a katasztrófa helyzet esetén értesítendő személyeket és elérhetőségeiket. A listát naprakészen kell tartani, és negyedévente ellenőrizni szükséges.
- Az intézkedési ütemtervben foglaltakat oktatni, és évente tesztelni kell katasztrófa helyzet szimulálásával.

XI. fejezet Záró rendelkezések

A felhasználók számára elérhető módon közzé kell tenni a felhasználókra vonatkozó szabályok érvényes változatát.

Jelen szabályzat 2014. április 15. napján lép hatályba.

Csákvár, 2014.április 8.

Tóth Jánosné
címzetes főjegyző

A jelen szabályzatot Csákvár Város Önkormányzat Képviselő-testülete a …/2014(IV.08.) számú határozatával elfogadta.