ADATVÉDELMI- ÉS INFORMÁCIÓBIZTONSÁGI SZABÁLYZAT

CLASSIC Oktatási és Szolgáltató Nonprofit Kft.

Forráskút

2018.

1. Összefoglaló

Az Adatvédelmi- és Információbiztonsági szabályzat a CLASSIC Oktatási és Szolgáltató Nonprofit Kft. (továbbiakban CLASSIC Kft.) minden dolgozójára vonatkozó információbiztonsággal kapcsolatos követelményeket és felelősségeket határoz meg, segítséget ad számukra a munkaköri leírásban rögzített feladataiknak az információbiztonsági szabályok szerinti végrehajtásában.

Az Adatvédelmi- és Információbiztonsági szabályzatot minden munkatárs rendelkezésére kell bocsájtani. A szabályzat ismerete és az abban foglaltak betartása a CLASSIC Kft. valamennyi alkalmazottjának és a CLASSIC Kft. informatikai rendszerével kapcsolatba kerülő, szerződéses viszonyban levő partnere számára kötelező.

2. Az Információbiztonsági szabályzat hatálya

Személyi hatály

Jelen Kézikönyv személyi hatálya kiterjed:

- a CLASSIC Kft.-nél foglalkoztatott munkavállalókra, az adatfeldolgozásban részt vevő külső cégekre, szerződéses jogviszonyban álló, jogi és természetes személyekre, jogi személyiséggel nem rendelkező szervezetekre,
- a CLASSIC Kft.-vel szerződéses kapcsolat keretében adatcserét (küldés és/vagy fogadás, tárolás/továbbítás) folytató szervezetekkel történő kommunikációra, függetlenül a szervezet betöltött szerepétől, szervezeti helyétől, elhelyezésétől és a CLASSIC Kft.-hez fűződő kapcsolatától.

Tárgyi hatály

A Szabályzat tárgyi hatálya kiterjed:

- A CLASSIC Kft. minden adatkezeléssel és feldolgozással kapcsolatos folyamatában résztvevő informatikai eszközre, illetve azok elhelyezésére szolgáló létesítményekre,
- az informatikai eszközök működtetésére szolgáló alap- és rendszerprogramokra, valamint alkalmazási programokra és azok dokumentációira (továbbiakban: program) a tulajdonviszonytól függetlenül,

- programrendszerek, berendezések beszerzési, fejlesztési, tervezési, kivitelezési munkálataira,
- a fentiek alapját képező szerződésekre, nyilvántartásokra, dokumentációkra, valamint,
- a feldolgozás alatt lévő, ott tárolt, illetve a feldolgozás eredményeképpen létrejött adatokra és adathordozókra, függetlenül azok keletkezési helyétől,
- a CLASSIC Kft. tulajdonában vagy használatában lévő informatikai eszközökre és az informatikai eszközök által kezelt, tárolt, továbbított adatokra.

3. Titoktartási megállapodások

Minden alkalmazottnak és a CLASSIC Kft.-vel kapcsolatba kerülő külső szervezetnek, személynek (cégnek, egyéni munkavállalónak, stb.) titoktartási nyilatkozatot kell aláírnia, melyben nyilatkoznak arról, hogy a munkájuk során a tudomásukra jutott, nem publikus adatokat sem a munkavégzésük, sem annak vége után nem hozzák harmadik fél tudomására.

4. Vagyontárgyak tulajdonlása

Valamennyi információ és az információfeldolgozással összefüggő vagyontárgy a CLASSIC Kft. tulajdona a felhasználók csak használatra kapják meg azokat.

A vagyontárgy használója felelős a következőkért:

- Gondoskodik az információ-feldolgozó eszközökkel kezelt adatok besorolásának megfelelő felhasználásáról,
- Gondoskodik az eszköz állagának megóvásáról, és rendeltetésszerű használatáról,
- Az eszközzel kapcsolatos hibás működést azonnal jelzi szakmai felettesének.

5. Emberi erőforrások

Fegyelmi eljárás

A szabályzat, illetve a biztonsági szabályok be nem tartása jogi következményeket vonhat maga után. A szabályzat ismeretének hiánya nem mentesít a felelősségre vonás alól.

Munkaviszony megszűntetése vagy módosítása

Az alkalmazási jogviszony megszüntetésekor, illetve a munkavállaló feladatkörét érintő megváltoztatásakor a szakmai vezető felelős azért, hogy a munkavállaló jogosultságai visszavonásra, illetve módosításra kerüljenek.

Minden munkavállaló, szerződéses partner, vagy külső fél köteles visszaszolgáltatni CLASSIC Kft. számára az összes birtokában lévő vagyontárgyat amennyiben az alkalmazás, szerződés vagy megegyezés megszüntetésre kerül.

6. Hordozható számítógépek fizikai védelme

A munkaállomásokra vonatkozó előírásokon kívül az alábbi fizikai védelmi szabályokat kell betartani:

- A mobilitás és a kis méret miatt a hordozható számítógépek fokozottan ki vannak téve a lopásveszélynek. Gondoljunk erre, és ezeket ne hagyjuk - még rövid időre sem - őrizetlenül autóban (még őrzött parkolóban sem), szállodai szobában, stb. (zárjuk el fizikailag, használjuk az értékmegőrzőt).
- A hordozható számítógép ellopása esetén a lopás tényét a lehető leggyorsabban jelenteni kell a felettes munkahelyi vezetőnek, továbbá:
    - értesíteni kell a rendőrséget,
    - értesíteni kell a szálloda vezetését, ha a számítógépet a szállodai szobából, vagy a szálloda ingatlanján álló kocsiból lopták el,
    - valamennyi rendőrségi és biztosítói jegyzőkönyvet, jelentést meg kell őrizni, és a CLASSIC Kft. részére át kell adni.

Adattároló, adatfeldolgozó eszköz elvesztése

Bármely adattároló, adatfeldolgozó eszköz elvesztését a lehető leggyorsabban jelenteni kell a munkahelyi vezetőnek, és tájékoztatni kell őket arról, hogy a berendezés tartalmaz-e bárminemű bizalmas adatot. /Előzetesen szóban, majd ahogyan lehetőség adódik erre, írásban (e-mailben) is megerősítve./

7. Logikai védelmi intézkedések

Hozzáférések védelme és ellenőrzése

A CLASSIC Kft. vezetése jogosult a tulajdonában lévő számítógépek és a hálózat használatát, a rajtuk végzett tevékenységeket (pl. céges levelezést, Internet használatot) ellenőrizni.

Felhasználó felelősségi köre

A CLASSIC Kft. felhasználói a munkaállomásokon azokat a jogtiszta szoftvereket használhatják, amelyek szükségesek a munkájukhoz, és a számítógépen az erre feljogosított személyek telepítették.

A felhasználó semmilyen IT eszközt nem telepíthet a CLASSIC Kft. informatikai hálózatába, azok elhelyezését, telepítési módját nem változtathatja meg. A felhasználó szoftvert csak külön engedéllyel és megfelelő jogosultság birtokában telepíthet, illetve módosíthatja a rendszerszintű beállításokat. Azok a felhasználók, akik adminisztrátori jogot gyakorolnak a gépükön, ők maguk felelnek a gépükre telepített programokért biztonsági és jogtisztasági szempontból egyaránt.

E rendelkezés megszegéséért a felhasználó ellen fegyelmi felelősségre vonás kezdeményezhető.

Az alkalmazottak a saját tulajdonukat képező számítógépeket, szoftvereket és egyéb informatikai eszközeiket csak eseti engedéllyel, bevizsgálás után használhatják a CLASSIC Kft.üzleti céljaira.

A CLASSIC Kft. tulajdonában lévő adatfeldolgozó eszközeinek hardver-, és szoftver integritásának megőrzése érdekében a felhasználónak tilos a számítógépet fizikailag megbontani, alkatrészeket cserélni, be- és kiszerelni.

A munkaállomás használatát nem szabad senkinek átengedni úgy, hogy a felhasználó saját felhasználói fiókjából nem jelentkezett ki előtte.

A fájlok, állományok elnevezéskor (mentésekor) egyedi, ékezeteket nem tartalmazó, a fájl tartalmára lehetőleg egyértelműen utaló nevet kell adni. A több lépcsőben készített anyagok esetében minden verziót külön verziószámmal kell ellátni.

Munkaállomásokon a fájl / könyvtár megosztás csak külön engedéllyel megengedett.

Hálózati védelem

A CLASSIC Kft. hálózatban lévő számítógép egyedi külső hálózati kapcsolattal (pl.: mobil internet, modem, ADSL) csak indokolt esetben, az adott szakterületi vezető engedélyével rendelkezhet. Az ilyen számítógépeken a CLASSIC Kft. számítógép-hálózatához való kapcsolódáskor nem engedélyezett a külső kapcsolat és a belső hálózat egyidejű használata.

Jelszókezelési szabályzat

A jelszavak használata az informatikai biztonság egyik meghatározó része. Az informatikai rendszer minden felhasználójának tisztában kell lennie a jelszavak fontosságával és a nem megfelelő jelszókezelés következményeivel, mert például egy rosszul megválasztott, könnyen kitalálható jelszó nemcsak a jelszó tulajdonosára, hanem a CLASSIC Kft. informatikai, telekommunikációs rendszerére is negatív következményekkel járhat.

A kezdeti jelszavak (pl. azok, melyek a felhasználói fiók létrehozásakor vagy jelszó reset esetén állítódnak be) csak az első bejelentkezésig maradhatnak érvényben, a rendszernek ki kell kényszerítenie a jelszó megváltoztatását, amennyiben a rendszer erre nem alkalmas a felhasználó feladata a jelszócsere elvégzése az első belépést követően. A kezdeti és új jelszavakat is a jelszószabályoknak megfelelően kell kialakítani és ezeknek egyedinek kell lennie.

Felhasználói jelszavak kezelése

A felhasználói jelszavak kezelése során az alábbiak betartása szükséges:

- A felhasználónak kötelessége a jelszó megváltoztatása a felhasználói fiók létrehozása utáni első belépéskor.
- A jelszavakat titokban kell tartani, ennek érdekében:
  - A jelszót tilos másoknak elmondani, a jelszóról mások előtt beszélni.
  - A jelszót se a feletteseknek, se a rendszergazdáknak, adminisztrátoroknak nem szabad elárulni, ha kifejezetten kérik ezt, akkor sem.
  - Tilos közös jelszavakat használni (még családtagokkal, barátokkal sem szabad).
  - A jelszót nem szabad leírni és elérhető helyen tárolni (irodában, táskában...).
  - Ne utaljunk a jelszó tartalmára (pl. „a kedvenc együttesem neve").
  - Ne használjuk a programok jelszó megjegyző funkcióját.
  - A jelszavunkat ne írjuk be kérdőívekbe, űrlapokba.

- Ha a belépési nevet és jelszót el kell küldeni, a felhasználó név/jelszó párost egy üzenetben (e-mailben, levélben vagy SMS-ben) nem szabad küldeni. Külön csatornán kell küldeni a nevet és a jelszót (pl. e-mail-ben és SMS-ben), hogy bármelyik lehallgatása, vagy illetéktelen kezekbe kerülése esetén se lehessen visszaélni a megszerzett adattal. A jelszót tartalmazó üzenetből ne lehessen kideríteni, hogy a kapott jelszót milyen felhasználónévvel, milyen rendszerhez lehet használni.

- Olyan jelszavakat kell használni, melyek nehezen visszafejthetőek, de könnyen megjegyezhetőek, nem személyes adatokon alapulnak (pl. nem tartalmaz telefonszámot, gyermek nevét, születési dátumot, kedvenc háziállat nevét, cégnevet, rendszámot, stb.) és nem szótári szó.
- Minél komplexebb a jelszó, annál kisebb a valószínűsége, hogy a nevünkben visszaélést követnek el, ezért a jelszóképzésnél az alábbi szempontokat kell betartani:
  - A jelszó nem tartalmazhatja az egész vagy egy felismerhető részét a felhasználónévnek; A jelszavaknak minimálisan 8 karakter hosszúnak kell lenniük és tartalmazniuk kell minimum 3 karaktertípust az alábbiakból: nagybetűk, kisbetűk, számok, speciális karakterek;
  - A jelszó az utolsó változtatás után maximum 90 napig maradhat érvényes;
  - Jelszóváltoztatáskor a felhasználó nem használhatja az utolsó 12 jelszavát;
  - Új jelszót csak két nap elteltével lehet megváltoztatni;
  - 5 hibásan megadott jelszó esetén a rendszer letiltja a fiókot.
- A felhasználó a jelszavát a legrövidebb időn belül köteles megváltoztatni, amennyiben felmerül a gyanú, hogy a jelszava más tudomására jutott. A jelszó kitudódását vagy annak gyanúját security incidensnek kell tekinteni és jelenteni szükséges.
- A felhasználónak tilos más felhasználó jelszavát megkérdeznie és tilos más felhasználó azonosítóját használnia annak belépése után. Hasonlóképpen, a felhasználó nem engedheti meg más felhasználónak az azonosítója használatát és nem engedheti át annak használatát a bejelentkezés után.
- A CLASSIC Kft. rendszereinek elérésére használt jelszavakat tilos külső rendszerek eléréséhez is használni (pl. gmail-hez, freemail-hez).
- Kezdeti jelszavak vagy a jelszó elfelejtése esetén, az ideiglenes jelszó kiadása előtt a felhasználót egyértelműen azonosítani kell.

- A felhasználók csak akkor tudják megváltoztatni a jelszavukat, miután a rendszer hitelesíti őket például a jelenlegi jelszót beírva.
- Kezdeti vagy ideiglenes jelszavakat a felhasználónak biztonságos csatornán kell eljuttatni.
- Kezdeti vagy ideiglenes jelszónak egyedinek kell lennie.
- A felhasználónak tilos a jelszavak megfejtésére alkalmas alkalmazást futtatnia.

A jelszószabályok betartása minden felhasználónak jól felfogott érdeke.

A felhasználó felelőssége, ha neki felróható mulasztása miatt a jelszava megismerése révén valaki visszaélést követ el.

Adathordozók megsemmisítése

Adathordozók megsemmisítésére vonatkozó igényt a szakmai felettesnek szükséges jelezni, aki intézkedik a helyes megsemmisítési eljárás lefolytatása kapcsán.

8. Biztonsági mentések, archiválás

Az adatokat nem a lokális gépen, hanem a szerverek megfelelő könyvtáraiban kell tárolni, ahol biztosítható azok rendszeres adatmentése és biztonságos tárolása. A megfelelő könyvtárba való mentés a felhasználó felelőssége.

9. Információbiztonsági hiányosságok és incidensek kezelése

Minden dolgozónak, szerződéses partnernek vagy külső félnek kötelessége a tudomására jutott információbiztonsági hiányosságokról, sérülékenységről, valamint az információbiztonsági szabályok megszegésről azonnal jelentést tenni az információbiztonsági incidensek megakadályozás céljából.

A dolgozók, szerződéses partnernek vagy külső felek a felfedezett biztonsági hiányosságokat semmilyen körülmények között sem jogosultak kihasználni vagy megpróbálni kihasználni azokat, illetve nem jogosultak a felfedezett incidenssel kapcsolatosan intézkedni!

Az információbiztonságot érintő eseményekről, a felfedezésük után, haladéktalanul tájékoztatni kell a felfedező közvetlen munkahelyi vezetőjét.

Az információbiztonságot veszélyeztető események kivizsgálására irányuló vizsgálatokban a dolgozók kötelesek együttműködni a kivizsgálókkal.

Az információbiztonsági hiányosságok megelőzése céljából a munkatársak kötelesek rámutatni az információbiztonsági szint romlására, illetve annak lehetőségére.

Szoftverműködési zavarok

A felhasználó a tárolt adataiban bekövetkező bármely megmagyarázhatatlan változást, az informatikai rendszer szokatlan működését azonnal köteles jelenteni a közvetlen felettesének. Hiba esetén a felhasználónak rögzíteni kell:

- a hibajelenséget és
- a képernyőn megjelenő hibaüzenetet.

Szükség esetén a munkavégzést azonnal fel kell függeszteni és a számítógépet le kell választani a hálózatról. Amíg nem derítették ki a hiba okát, a számítógépben lévő adathordozókat nem szabad másik számítógépre áttenni.

Forráskút, 2018. május 24.

CLASSIC NONPROFIT KFT. * Forráskút *

.....
Kocsis Mária
ügyvezető

ELEKTRONIKUS ÁLLOMÁNYTÁROLÁS SZABÁLYZATA

CLASSIC Oktatási és Szolgáltató Nonprofit Kft.

Forráskút

2018.

1. Általános irányelvek

A munkavégzéssel kapcsolatos adatok tárolására a CLASSIC Oktatási és Szolgáltató Nonprofit Kft. (továbbiakban CLASSIC Kft.) szerverei szolgálnak.

Amennyiben elengedhetetlen laptopokon, felhasználói PC-ken tárolni és módosítani munkavégzéssel kapcsolatos állományokat, azokat minél hamarabb a fájlszerverre kell másolni, mert a helyi gépen történő adattárolás esetén az adatok rendelkezésre állása nem garantált. A fájlszerveren tárolt adatokról rendszeresen biztonsági mentést kell készíteni, így lehetőség van azok visszaállítására. A notebookon, desktop gépen tárolt adatokról központi mentés nem készül, az így tárolt adatokért az adott munkavállaló a felelős!

A fenti könyvtárban kizárólag a munkavégzéshez szükséges adatok tárolhatók.

2. Elektronikus állománytárolással kapcsolatos rendelkezések

Elektronikus adattárolás csak az erre kinevezett fájl szervereken engedélyezett, melyekről mentések készülnek. Egyéb helyeken (pl. a felhasználók desktop PC-jén vagy laptopján, USB kulcsokon, külső merevlemezeken, stb.) tárolt adatokért a CLASSIC Kft. semmilyen felelősséget nem vállal, ezek elveszéséért és az ezzel kapcsolatos költségekért (pl. sérült merevlemezről az adatok visszaállítása) minden esetben a munkavállalót terheli a felelősség.

Nem kifejezetten fájl tárolásra kijelölt szerveren hálózati megosztások kialakítása kifejezetten tilos. Így tilos fájl megosztások létrehozása munkaállomásokon, alkalmazás-szervereken (amennyiben a megosztás nem képezi az adott alkalmazás részét), teszt és fejlesztői szervereken. Ennek a szabálynak a betartását a CLASSIC Kft. folyamatosan felügyelheti, és a nem engedélyezett megosztások azonnal törlésre kerülnek.

A fájl szervereken (beleértve a felhasználók saját könyvtárát, illetve bármilyen közösen használható könyvtárat is) csak a munkavégzéshez szükséges elektronikus adatok tárolása engedélyezett, melynek betartását a CLASSIC Kft. folyamatosan felügyelheti. Az egyértelműen nem munkavégzéshez kötődő adatok felsorolása az 1. mellékletben található.

Az egyértelműen nem a munkavégzéshez köthető elektronikus adatok előzetes értesítés nélkül eltávolításra kerülhetnek, és az adatok elhelyezéséért felelős személy ellen munkaügyi felelősségre vonás indulhat.

A CLASSIC Kft. végfelhasználói hálózati megosztást nem hozhatnak létre. E szabály megszegése munkaügyi felelősségre vonást vonhat maga után.

A fájlmegosztási célokat szolgáló szervereken hálózati megosztás létrehozására csak az informatikai területen a szerverek üzemeltetéséért felelős, rendszergazdai jogosultsággal rendelkező kollégái jogosultak.

A CLASSIC Kft. felhasználóinak saját könyvtárt biztosít.

A saját használatú könyvtárak méretét a CLASSIC Kft. egy előre meghatározott méretben korlátozza.

A saját használatú könyvtárakban csak a CLASSIC Kft. üzleti feladatait támogató, a munkavégzéshez szükséges dokumentumok tárolása engedélyezett.

A CLASSIC Kft. a saját felhasználású könyvtárak tartalmát rendszeresen ellenőrizheti. A nem engedélyezett tartalmak előzetes értesítés nélkül törlésre kerülnek.

A nem engedélyezett tartalmat tároló felhasználók ellen munkaügyi felelősségre vonás kezdeményezhető.

F o r r á s k ú t, 2018. május 24.

CLASSIC NONPROFIT KFT. * Forráskút

.....

Kocsis Mária
ügyvezető

3. Mellékletek

1. számú melléklet

Az egyértelműen nem munkavégzéshez tartozó elektronikus adatok a következők (lista nem teljes körű):

- bármilyen fájl, amely implicite vagy explicite szexuális vagy pornográf tartalmú;
- bármilyen fájl, melynek tartalma implicite vagy explicite bármi nemű hátrányos megkülönböztetésre vagy gyűlöletkeltésre ösztönöz;
- bármilyen fájl, ami kártékony kódot tartalmaz (pl. bármilyen számítástechnikai vírussal fertőzött fájl) vagy a biztonsági előírások megkerülését, megszegését segíti (pl. keylogger, speciális az Acrobat eszközök biztonsági réseit kihasználni képes PDF állomány, stb.);
- bármilyen, nem jogtiszta tartalom (pl. feltört szoftverek, fájl cserélőről letöltött filmek, stb.)

Nem egyértelmű, de nagy valószínűséggel nem munkavégzéshez kötődő elektronikus adatok a következők (lista nem teljes körű):

- filmek (pl. Youtube-ról saját célra letöltött videók);
- zenei anyagok (pl. a korlatlanzene.hu-ról saját célra letöltött zenék)
- fényképalbumok (pl. családi képek), de a munkatársakkal tartott pl. csapatépítő összejövetelek képei már nem tartoznak ide.

2. számú melléklet: Fogalomtár

Fontosabb kifejezések értelmezése az informatikai biztonság szemszögéből, amelyek néha eltérnek a köznyelvi vagy más szakma értelmezésétől.

Fájl Szerver: Nagykapacitású tárolóval rendelkező számítógép, mely hálózati kapcsolata révén a központi adattároló egységét a felhasználók számára megosztani képes.

Hálózati megosztás: Meghatározott felhasználói kör számára a hálózaton keresztül elérhetővé tett tárterület.

Közös megosztás: Minden felhasználó számára a hálózaton keresztül elérhetővé tett tárterület.

Felhasználó, végfelhasználó: Az a személy, aki egy vagy több informatikai rendszert használ feladatai megoldásához.

Nem engedélyezett tartalom: Bármilyen nem üzleti célú vagy nem jogtisztán birtokolt dokumentum vagy egyéb elektronikus állomány.

SZABÁLYZAT AZ IRATOK MEGŐRZÉSÉRŐL ÉS MEGSEMMISÍTÉSÉRŐL

CLASSIC Oktatási és Szolgáltató Nonprofit Kft.

Forráskút

2018.

1. A szabályzat tárgya

Jelen Szabályzat (a „Szabályzat") tárgya a CLASSIC Oktatási és Szolgáltató Nonprofit Kft.-nél (továbbiakban CLASSIC Kft.) keletkezett iratok megőrzése és megsemmisítése általános követelményeinek meghatározása.

2. A szabályzat hatálya

2.1. Személyi hatály

A Szabályzat kiterjed a CLASSIC Kft.-vel munkaviszonyban, munkavégzésre irányuló egyéb jogviszonyban álló természetes személyekre, valamint minden olyan személyre, aki CLASSIC Kft.-vel szerződéses jogviszonyban áll.

2.2. Tárgyi hatály

A Szabályzat kiterjed a CLASSIC Kft. tulajdonát képező iratokra, függetlenül az iratok megjelenési formájától (hard copy, soft copy vagy e-mail), továbbá attól, hogy az iratok tervezetek vagy végleges állapotúak-e.

2.3. Időbeli hatály

A Szabályzat 2018. május 24. napjával lép hatályba, rendelkezéseit ezen időponttól kezdődően kell alkalmazni.

3. Elsőbbségi esetek

A körülményektől függően jelen 3. Fejezetben foglalt rendelkezések (az "Elsőbbségi Követelmények") elsőbbséget élveznek az alábbi 4. Fejezet követelményeivel szemben (az „Általános Követelmények"):

3.1. Minden olyan dokumentum, amely

a CLASSIC Kft.-t érintő tényleges vagy potenciális peres eljárásra; vagy bármilyen, a CLASSIC Kft.-t érintő tényleges vagy potenciális vizsgálatra vonatkozik, amelyet közigazgatási szerv (különösen, de nem kizárólag a szabályozó, adóhatóság vagy versenyhatóság) folytat, megőrzendő, függetlenül minden egyéb követelménytől. Ez a kötelezettség akkor keletkezik, és addig marad érvényben, amikor, illetve amíg az a személy a CLASSIC Kft.-nél, aki a legfelsőbb szinten felel a kérdéses perért vagy vizsgálatért ilyen értelmű közleményt ad ki.

3.2. Minden olyan dokumentum, amely:

a CLASSIC Kft.-t érintő tényleges vagy potenciális peres eljárásra; vagy bármilyen, a CLASSIC Kft.-t érintő tényleges vagy potenciális vizsgálatra vonatkozik; megőrzendő, függetlenül minden egyéb követelménytől. Ez a kötelezettség akkor keletkezik, és addig marad érvényben, amikor, illetve amíg a CLASSIC Kft. részéről a per vagy vizsgálat ügyében intézkedési felelősséggel bíró személy ilyen értelmű közleményt ad ki.

4. Általános követelmények

4.1. A jelen 4. Fejezetben szereplő Általános Követelmények a 3. Fejezetben meghatározott Elsőbbségi Követelmények alá vannak rendelve.

4.2. A CLASSIC Kft. irat megőrzési irányelvei megadják a hatáskörükbe tartozó dokumentumok főbb kategóriáit, azzal, hogy ezen túlmenően is az iratként kell kezelni a CLASSIC Kft. működésével, illetőleg az alkalmazottak, szerződéses partnerek tevékenységével kapcsolatosan bármilyen anyagon, alakban és bármilyen eszköz felhasználásával keletkezett írott szöveget, adatot és ehhez hasonló anyagokat.

Ezek a kategóriák a következők:

4.2.1. Adózással kapcsolatos iratok.

Idetartoznak mindazok a jogszabályban előírt bizonylatok, könyvek, nyilvántartások - ideértve a mágneses adathordozón rögzített adatokat is – amelyek az adó alapjának, az adó összegének, a mentességnek, a kedvezménynek, a költségvetési támogatás alapjának és összegének, továbbá ezek megfizetésének, illetve igénybevételének megállapítására, ellenőrzésére alkalmasak, illetve ehhez szükségesek. Értelemszerűen az adó és az ezzel kapcsolatos kifejezések alatt érteni kell mind az adóval, a járulékokkal, az illetékkel, a központi költségvetés, az elkülönített állami pénzalap, a Nyugdíjbiztosítási Alap, az Egészségbiztosítási Alap vagy az önkormányzat javára teljesítendő, törvényen alapuló kötelező befizetéssel, a központi költségvetés, az elkülönített állami pénzalap terhére törvényben, kormányrendeletben vagy miniszteri rendeletben meghatározott feltételek alapján juttatott támogatással összefüggésben keletkező iratokat.

4.2.2. Számvitellel kapcsolatos iratok.

4.2.2.1. Ide tartozik a CLASSIC Kft. által kiállított, készített, illetve a vele üzleti vagy egyéb kapcsolatban álló természetes személy vagy más gazdálkodó által kiállított, készített okmány (számla, számlát helyettesítő okmány, szerződés, megállapodás, kimutatás, hitelintézeti bizonylat, bankkivonat, jogszabályi rendelkezés, egyéb ilyennek minősíthető irat) - függetlenül annak nyomdai vagy egyéb előállítási módjától -, amelyet a gazdasági esemény számviteli nyilvántartása céljára készítettek, és amely rendelkezik az e törvényben meghatározott általános alaki és tartalmi kellékekkel.

4.2.2.2. Bizonylatnak minősül többek között, de nem kizárólag a CLASSIC Kft. jegyzett tőkéjére és tőketartalékára kihatással bíró alapító okirata és annak módosításai, az ezzel kapcsolatos közgyűlési és igazgatósági határozatok.

4.2.2.3. Számviteli iratnak minősül az üzleti évről készített beszámoló, valamint az azt alátámasztó leltár, értékelés, főkönyvi kivonat, továbbá a naplófőkönyv vagy más, a Szt. követelményeinek megfelelő nyilvántartás.

4.2.3. Személyes adatokat tartalmazó iratok.

Ide tartoznak mindazok az iratok, amelyek meghatározott természetes személlyel kapcsolatba hozható adatokat, az adatokból levonható, az érintettre vonatkozó következtetéseket tartalmaznak. A személyes adat az adatkezelés során mindaddig megőrzi e minőségét, amíg kapcsolata az érintettel helyreállítható.

4.2.4. Szerződések (általános).

Ide tartoznak azok az iratok, amelyek a kölcsönösen mellérendelten tevékenykedő felek jogviszonyait tartalmazzák, amelyben őket kölcsönös kötelezettség terheli valamely – többnyire vagyoni tartalmú - szolgáltatás teljesítésére, amely során a kötelezettség teljesítése a másik fél számára alanyi jogosultságot képez, ideértve ezen jogviszonyok módosítását is, függetlenül attól, hogy ezek a jogviszonyok egy vagy több iratba kerülnek belefoglalásra.

4.2.5. Vállalati dokumentumok.

Ide tartoznak mindazon, más körbe nem sorolható dokumentumok, amelyek a döntés előkészítéssel, tevékenységével, működésével kapcsolatos információkat tartalmaznak.

4.2.6. Ügyfelek reklamációi.

Ide tartoznak a CLASSIC Kft. tevékenységével, működésével kapcsolatos panaszai és bejelentései, vonatkozzon az akár egy egyedi esetre, akár pedig általános észrevételekre.

4.2.7. Szabályozási ügyek.

Ide tartoznak a CLASSIC Kft. jogalkotási folyamatban való részvétele során keletkezett iratok, csakúgy, mint az Általános Szerződési Feltételei és egyéb belső szabályzatai.

4.2.9. Egyéb iratok.

Minden más iratok, levelezést és egyéb dokumentumot addig kell megőrizni, amíg ez esetleg jelentőséggel bírhat a vállalat folyamatos üzletvitele szempontjából.

5. A dokumentumokra vonatkozó megőrzési kötelezettség

A 4.2. pontban felsorolt iratokat legalább a következőkben meghatározott időtartam alatt meg kell őrizni. A dokumentumokat, amennyiben az irányadó jogszabály más előírást nem tartalmaz, a keletkezésüktől számított 5 (öt) évig, az általános polgári jogi általános elévülési időn belül kell megőrizni, amennyiben abból jogok vagy kötelezettségek keletkeznek, illetve hatósági eljárás vagy vizsgálat alapját képezhetik, feltéve, hogy a 3. Elsőbbségi követelmények pont eltérő rendelkezést nem tartalmaz.

Amennyiben egy irat a meghatározások vagy jogi jellege alapján több kategóriába is sorolható, akkor az iratra azt a megőrzési határidőt kell figyelembe venni, amelyik a lehetséges besorolások közül a leghosszabb.

A nevelési-oktatási intézményekre vonatkozó iratmegőrzési időket az 1. sz. melléklet tartalmazza.

6. Az iratok nyilvántartása

A fizikai formában létező iratokat zárt tároló szekrényben, az elektronikus formában létező iratokat pedig a tárolásukat és megőrzésüket biztosító adathordozón keletkezésük helyén kell elhelyezni. Az iratokhoz illetéktelenek általi hozzáférést a megfelelő módon meg kell akadályozni. A jogszabály vagy a külön ügyvezetői utasítás szerint minősített iratoknak számító dokumentumokat a minősítésüknek megfelelő biztonsági intézkedések megtétele mellett (pl. tűzbiztos lemezszekrény, páncélszekrény, stb.) kell őrizni.

7. Az iratok megsemmisítése

Az iratok a megőrzési idő eltelte után kerülhetnek megsemmisítésre. Hacsak nincs jogi, kereskedelmi vagy jogszabályi indoka a megőrzésüknek, a dokumentumok tervezeteit azonnal meg lehet és meg is kell semmisíteni feltéve, hogy a végleges verzió a követelmény szerint megőrzésre kerül. Az adott szervezeti egység vezetője felelős az irat megsemmisítéséért, azonban, amennyiben a vállalat érdekei ezt indokolják, dönthet az iratok további őrzéséről. A megsemmisítésnek ki kell terjednie az iratok másolati példányainak lehetőség szerinti felkutatására és megsemmisítésére. A megsemmisítésnek olyan formában kell megtörténnie, amely a dokumentum helyreállítását és tartalmának mások általi megismerhetőségét lehetetlené teszi. A megsemmisítésről jegyzőkönyvet kell felvenni, amely tartalmazza a megsemmisítés helyét és idejét, a megsemmisítés módját, az eljárás során jelenlevők felsorolását, valamint a megsemmisített iratok felsorolását. A jegyzőkönyvet a megsemmisítés lefolytatásáért felelős személy írja alá és őrzi. Ez az irat megsemmisítésre nem kerülhet. Az Általános követelményeken kívül a dokumentumokat rutinszerűen és rendszeresen meg kell vizsgálni megsemmisítési célból.

8. A CLASSIC Kft.-n belüli szervezeti felelősség az iratok kezeléséért

A Szabályzat személyi hatálya alá tartozók mindannyian felelősek a Szabályzatban foglalt előírások megismeréséért, azok betartásáért és nyilvántartás szervezeti egységen belül történő megszervezéséért és annak Szabályzatban foglaltak szerinti teljesülésének figyelemmel kíséréséért. Az egyes kategóriákért (lásd fent) általános felelősséggel bíró személyek számára létre kell hozni egy rendszert, amelynek alapján ezen követelmények szerinti megfelelőséget jelentik a jogi vezetőnek.

Az egyes kategóriákkal összefüggésben a CLASSIC Kft. felelős vezetői meghatározzák az alábbiakat:

- részleteiben azokat a dokumentum típusokat, amelyek valamely fenti kategóriába tartoznak;
- a jogszabály által előírt (vagy más jogilag kötelező) időtartamot a kérdéses dokumentum kategória megőrzésére;

- ha nincs jogszabály által előírt vagy más megőrzési időszak, akkor a felelős vezető által a kérdéses dokumentum kategória megőrzésére előírt időtartamot, amely 1 (egy) évnél kevesebb nem lehet;
- eljárásokat a megőrzendő vagy megsemmisítendő dokumentumok azonosítására, és azt, hogy milyen gyakorisággal kell ezt a kiválasztási eljárást lefolytatni;
- a dokumentumok megőrzésének pontos módját:
- ha a dokumentumok elektronikusak, akkor a formátumot és a helyet, amelyben és ahol azokat tárolni kell;
- ha a dokumentumok fizikai formátumúak, akkor a dokumentum kategóriákra alkalmazandók különböző biztonsági intézkedéseket (pl. tűzbiztos széfek);
- a tényt, hogy a fenti pontokban megállapított megőrzési időszak végén a dokumentumokat meg kell-e semmisíteni;
- azt a módszert, amellyel a dokumentumokat meg kell semmisíteni, amikor a vonatkozó megőrzési időszak letelt.

F o r r á s k ú t, 2018. május 24.

.....
Kocsis Mária
ügyvezető

1. sz. melléklet

A nevelési-oktatási intézmény irattári terve

a 20/2012. (VIII. 31.) EMMI rendelet 1. melléklet alapján

Irattári tételszám	Ügykör megnevezése	Őrzési idő (év)
Vezetési, igazgatási és személyi ügyek		
1.	Intézménylétesítés, -átszervezés, -fejlesztés	nem selejtezhető
2.	Iktatókönyvek, iratselejtezési jegyzőkönyvek	nem selejtezhető
3.	Személyzeti, bér- és munkaügy	50
4.	Munkavédelem, tűzvédelem, balesetvédelem,	10
5.	Fenntartói irányítás	10
6. *	Szakmai ellenőrzés	20
7.	Megállapodások, bírósági, államigazgatási ügyek	10
8.	Belső szabályzatok	10
9.	Polgári védelem	10
10.	Munkatervek, jelentések, statisztikák	5
11.	Panaszügyek	5
Nevelési-oktatási ügyek		
12.	Nevelési-oktatási kísérletek, újítások	10
13.	Törzslapok, póttörzslapok, beírási naplók	nem selejtezhető
14.	Felvétel, átvétel	20
15.	Tanulói fegyelmi és kártérítési ügyek	5
16.	Naplók	5
17.	Diákönkormányzat szervezése, működése	5
18.	Pedagógiai szakszolgálat	5

19.	Szülői munkaközösség, iskolaszék szervezése, működése	5
20.	Szaktanácsadói, szakértői vélemények, javaslatok és ajánlások	5
21.	Gyakorlati képzés szervezése	5
22.	Vizsgajegyzőkönyvek	5
23.	Tantárgyfelosztás	5
24.	Gyermek- és ifjúságvédelem	3
25.	Tanulók dolgozatai, témazárói, vizsgadolgozatai	1
26.	Az érettségi vizsga, szakmai vizsga	1
27.	Közösségi szolgálat teljesítéséről szóló dokumentum	5
Gazdasági ügyek		
27.	Ingatlan-nyilvántartás, -kezelés, -fenntartás, határidő nélküli épülettervrajzok, helyszínrajzok, használatbavételi engedélyek	
28.	Társadalombiztosítás	50
29.	Leltár, állóeszköz-nyilvántartás, vagyonnyilvántartás, selejtezés	10
30.	Éves költségvetés, költségvetési beszámolók, könyvelési bizonylatok	5
31.	A tanműhely üzemeltetése	5
32.	A gyermekek, tanulók ellátása, juttatásai, térítési díjak	5
33.	Szakértői bizottság szakértői véleménye	20
34. *	Költségvetési támogatási dokumentumok	5

VÍRUSVÉDELMI ELJÁRÁSREND

CLASSIC Oktatási és Szolgáltató Nonprofit Kft.

Forráskút

2018.

1. Összefoglaló

A CLASSIC Oktatási és Szolgáltató Nonprofit Kft. (továbbiakban CLASSIC Kft.) egészére kiterjedő, folyamatos vírusvédelem és rendszeres vírusellenőrzés biztosítása érdekében automatikus frissítésű, központilag menedzselhető, többszintű (eltérő gyártótól származó adatbázis alapján történő víruskeresés) vírusvédelmi rendszert kell kiépíteni. Minden lehetséges lépést meg kell tenni, a veszélyes programok által okozott incidensek kiküszöbölésére. Ennek érdekében hatékony vírusellenőrző alkalmazásokat kell telepíteni mind a munkaállomásokra, mind pedig a szerverekre és informatikai határvédelmi eszközökre.

Amennyiben egy munkaállomás működési környezete nem teszi lehetővé a vírusellenőrző alkalmazás telepítését, úgy alternatív vírusvédelmi megoldást kell alkalmazni. Ilyen alternatív megoldás a megfelelő hardening alkalmazása mellett, hogy elszeparált hálózati szegmensek kerülnek kialakításra, amennyiben ezen hálózati szegmensekbe mégis kell adattároló eszközt csatlakoztatni, úgy a használatot megelőzően az eszköz vírusmentességéről meg kell győződni.

Az elektronikus levelezés során az elsődleges szűrést a „SMTP gateway" funkcióval rendelkező rendszernek kell megvalósítania, a levelezés biztonságának megteremtését pedig kéretlen levél (spam) szűrő rendszer alkalmazásával, valamint vírusvédelmi rendszer használatával kell biztosítani. Az egyéb lehetséges vírus bejutási irányok védelmét az alkalmazott munkaállomás(ok) és szerver számítógép(ek) állandó vírusvédelmének kell biztosítania.

2. Általános rendelkezések

Kártékony programok okozta kockázat miatt, vírusvédelem nélkül sem hálózati, sem önálló munkaállomás, sem hordozható számítógép nem üzemeltethető.

Olyan számítógépek esetén, melyekre anti-vírus program (valamilyen okból) nem telepíthető (pl. speciális feladatú, Unix alapú szerverek), vagy a közvetlen vírustámadás esélye minimális, kompenzációs védelmi intézkedéseket kell kialakítani, pl. tűzfal, router beállításaival.

A vírusvédelmi rendszerhez kapcsolódóan olyan jogosultsági rendszert kell kialakítani, hogy csak az arra feljogosított személyek állíthassák le teljes a rendszer, vagy moduljainak

működését, végezhessenek módosítást a beállításokon, telepíthessenek programot a számítógépekre.

Vírusgyanú esetén a felhasználó köteles azonnal leválasztani a számítógépet a hálózatról, és értesíteni a szakmai felettesét, aki ellátja utasítással.

Aki az adatait és adathordozóit a vírus-ellenőrzés vagy vírusvédelmi intézkedés (pl. vírusmentesítés) alól bármilyen indokkal kivonja, felelősségre vonható, illetve az abból eredő kár is őt terheli.

A CLASSIC Kft. vírusvédelmi rendszere korszerű vírusvédelmi technológiák, összehangolt folyamatok és szabályok összessége, melyek alkalmazásának irányelvei az alábbiak:

- ***Megelőzés:*** A rosszindulatú programkódok elleni védekezésben a megelőző folyamatokra kell koncentrálni. A vírusvédelmi rendszeren túl, az informatikai rendszer egyéb hardver és szoftver eszközeinek lehetőségeit is kihasználva, biztosítani kell (fokozni kell) a többszintű védelmet.
- ***Folyamatosság***: A fertőzések megelőzése, valamint vírustámadás kockázatának csökkentése érdekében, a vírusvédelmi rendszert folyamatosan kell üzemeltetni. Gondoskodni kell a vírusvédelmi rendszer adatbázisának és szoftverének folyamatos frissítéséről.
- ***Reagálás:*** A világban folyamatosan változó, vírusvédelemmel kapcsolatos kihívásokra a CLASSIC Kft. igyekszik rugalmasan, gyorsan, és hatékonyan reagálni. Ennek érdekében biztosítani kell az új vírusokról és szoftver-sérülékenységekről szóló információk rendelkezésre állását, feldolgozását. Az információk alapján folyamatosan hangolni kell a vírusvédelmi eszközök beállítását, esetleg új eszközöket kell bevonni, alkalmazni. A felmerülő hibákat a lehető leggyorsabban ki kell javítani.
- ***Tudatosság:*** A vírusvédelmi rendszer hatékonyága jelentős mértékben növelhető, ha a vírusvédelemben résztvevő személyek (rendszergazdák, felhasználók), felkészültsége, motivációja, illetve tudatos felelősségvállalása biztosított. Ennek érdekében, a dolgozók részére, rendszeresen, a munkakörüknek megfelelő szintű információt kell biztosítani, időszakosan oktatásban kell őket részesíteni, a megszerzett tudásukat pedig mérni kell.

3. A vírusvédelmi rendszer

A hatékony védelem érdekében valósidejű, több szintű vírusvédelmet kell kialakítani, mely a végpontokon (munkaállomásokon) és az adatáramlás központjain (fájl- és levelezés kiszolgálókon) működik.

A szervereken és munkaállomásokon a valósidejű védelemnek folyamatosan bekapcsolva kell lennie, hogy biztosítsa a felhasználói munka során igénybevett állományok (adatok, programok) használat előtti vírusellenőrzését.

Amennyiben a valósidejű védelem a detektált vírus eltávolítására nem képes, a vírusvédelmi rendszernek automatikus értesítést kell küldeni a felhasználó számára, továbbá a fertőzésgyanús állományt a rendszernek automatikusan karanténba kell helyezni.

4. A vírusvédelmi rendszer konfigurációja

- A vírusvédelmi rendszer alapbeállításainak elvégzésére létre kell hozni a vírusvédelmi rendszer konfigurációs telepítő file-ját, amely lehetővé teszi az egységes beállításokkal történő telepítést.
- A CLASSIC Kft. által kiválasztott és alkalmazott vírusvédelmi szoftvert alkalmazni kell a szervereken, a munkaállomásokon, mobil eszközökön (okos telefonok esetében a fenti feltételeknek megfelelő vírusvédelmi szoftver annak megfelelő verzióját), azaz a teljes informatikai hálózaton, valamint a hálózatba nem kötött számítógépeken is.
- A fenti szabály alól a külső személyek (pl. fejlesztést,- diagnosztikát végző,- projekt tevékenységeket végrehajtó személyek) információ-feldolgozó eszközei kivételt képezhetnek (tehát nem kötelező ugyanazt a márkájú, típusú vírusvédelmi szoftver alkalmazniuk), azonban ezen rendszerek esetében is, a jelen eljárásrendben foglalt kritériumoknak megfelelő vírusvédelmi rendszerrel kell, hogy rendelkezzenek. Távoli hozzáférés esetén a külső személyek a szerződésben vállalt anyagi és erkölcsi felelősséggel tartoznak egy esetlegesen miattuk bekövetkező vírusfertőzéskor.
- A vírusvédelmi program telepítése során alapértelmezésben be kell kapcsolni a víruskereső azon rezidens részét, amelyik állandóan figyeli a lemezműveleteket és a memóriában tartózkodó adatokat.
- Az automatikus frissítést kell választani a vírusvédelmi szoftver konfigurációja során.

5. Vírusvédelmi programok kiválasztási, tesztelési szempontjai, általános követelmények

A vírusvédelmi programok kiválasztásánál az alábbi szempontok pontos meghatározása és értékelése szükséges:

- A vírusvédelmi programnak támogatnia kell a CLASSIC Kft. alkalmazott operációs rendszereket, meg kell felelnie a központilag menedzselt vírusvédelmi feladatok ellátására,
- A kártékony szoftverek elleni védelmet a hardver-eszközök három különböző szinten kell kialakítani – meg kell valósítani
- a kliens-oldal védelmét,
- a szerver-oldal védelmét, és
- az átjárókon (gateway-eken) áthaladó forgalom védelmét.
- Támogatnia kell mindazokat a platformokat, illetve mindazokat az alkalmazásokat, melyeket a rendszer a felhasználók számára szolgáltatásként nyújt,
- Támogatnia kell az okos telefonok vírusvédelmi megoldásait,
- Támogatnia kell a munkaállomások vírusellenőrzését, a hálózati rendszerben központilag tegye menedzselhetővé a vírusvédelmet,
- Legyen aktív, memória rezidens, azaz folyamatos felügyeletet biztosító rendszer,
- A vírusvédelmi szoftver gyártójának folyamatosan biztosítani kell a frissítéseket (mind vírusadatbázis, mind vírusvédelmi szoftver tekintetében),
- A rendszernek támogatnia kell az Internetes böngészőkbe való integrációt, link és letöltés figyelést, blokkolást,
- A rendszernek alkalmasnak kell lennie a mobil kódok ellenőrzésére, futtatásuk tiltására (pl.: Word makrók, Java scriptek),
- A rendszernek ismernie kell a népszerűbb archívum (tömörített fájl) formátumokat: ZIP, 7-Zip, ARJ, RAR, CAB, LZH, ACE, JAR, GZip, TAR, BZ2, Z.
- A fent említett tömörített fájlokban mélységi átvizsgálást is végre kell, hogy tudjon hajtani a keresőmotor,
- Vírusvédelmi programnak támogatnia kell a heurisztikus vírusfelismerést,
- A programnak alkalmasnak kell lennie olyan bejegyzések létrehozására a napló állományban, amelyből automatikus riasztási megoldás generálható,

- A rendszernek alkalmasnak kell lennie a számítógépen található, közvetlenül futtatható fájlok (pl.: .exe) változását figyelemmel kísérnie – és ha azt nem hitelesített folyamat változtatja meg (pl.: a szoftver frissítést végző komponense) akkor a megváltozott szoftver futtatásáról jóváhagyást kell, hogy kérjen a vírusvédelmi szoftver a felhasználótól,
- A vírusvédelmi rendszernek paraméterezhetőnek kell lennie úgy, hogy a felhasználó ne változtathassa a beállításokat,
- Ne igényeljen állandó felhasználói és rendszergazdai beavatkozást,
- A vírusvédelmi programhoz kapcsolódóan a support támogatást biztosítani szükséges,
- A programnak lehetővé kell tennie az aktuális vírusadatbázis és szoftververzió státuszának lekérdezhetőségét a felhasználók által is,
- A működési státuszt lekérdezhetővé kell tennie a felhasználóknak is (rezidens védelem státusza, frissítési rendszer működőképessége, vizsgálat folyamatban van vagy sem),
- A programnak lehetővé kell tennie a vizsgálat alatt lévő file jelzését,
- A programnak lehetővé kell tennie a karantén alkalmazási lehetőségét,
- A szoftver támogassa a frissítési megoldások (időzíthető-e, külső - Internet és/vagy belső szerverről) egyénileg beállítható típusait,
- támogassa a távoli installálás, konfigurálás lehetőségét,
- A szoftver legyen képes a vírusvédelmi feladatok automatizálására.

6. A fertőzések elkerülése érdekében:

Vírusvédelem nélkül sem hálózati, sem önálló munkaállomás, sem hordozható számítógép nem üzemeltethető.

A felhasználók nem rendelkezhetnek jogosultsággal a gépükön futó vírusvédelmi szoftver leállításához, és a beállítások megváltoztatásához.

A CLASSIC Kft. hálózatához nem, vagy régen csatlakozott számítógépen a vírusvédelmi program frissítése a felhasználó feladata és felelőssége, ennek elmaradásából keletkező kár is őt terheli. A belső hálózathoz vagy Internethez nem csatlakoztatott munkaállomások esetén a vírusdefiníciós állományok frissítését legalább hetente el kell végeznie a felhasználónak manuálisan, vagy csatlakoztatnia kell a munkaállomást a belső hálózathoz vagy az Internethez a frissítés idejére.

7. Számítógépes vírusfertőzésre utaló jelek:

- A számítógép nem indul el, vagy bekapcsolás után lefagy
- A szabad memória látványosan kevesebb, mint amennyinek lennie kéne
- A korábban megszokottnál érezhetően lassabb rendszerműködés tartósan jelentkezik
- Szokatlan hang vagy dallam szól a számítógép hangszórójából
- Más jelenik meg a monitoron, mint amit beírunk, vagy a gép nem reagál a leütött billentyűkre
- Képernyőn vagy nyomtatott papíron megjelenő szokatlan felirat, ábra
- Program vagy fájl hirtelen eltűnik
- Ismeretlen program vagy fájl titokzatos megjelenése
- Bizonyos állományokat nem lehet betölteni vagy végrehajtani
- A vírusvédelmi program nem indul el
- A vírusvédelemi cégek (angol) honlapját nem lehet megnyitni
- Új menüpont jelenik meg a Word, Excel programban, illetve egy menüpont indokolatlanul nem érhető el
- A TEMPLATE könyvtárat kivéve, semmilyen könyvtárba nem lehet elmenteni egy Word dokumentumot
- Az állomány utolsó módosításának időpontja érthető indok nélkül megváltozik
- Hirtelen változás a programok, fájlok méretében, ok nélkül lecsökkenő merevlemez kapacitás
- A szokásostól eltérő, rendellenes "Write protection error" - írásvédelem hiba üzenet jelenik meg
- A merevlemez leformattálódik

Természetesen, a fentiek más hibára is utalhatnak.

8. Levelezés biztonsága

Tilos megnyitni ismeretlen forrásból származó elektronikus levelet és annak mellékletét. A fertőzöttség gyanújának elbírálásához az alábbiakat kell figyelembe venni:

- A levél nyelvezete: fertőzött lehet a levél, ha idegen nyelven, rossz magyarsággal, vagy nem a szokásos kommunikációs nyelven íródott.
- Várható volt a levél a feladótól? Fertőzött levél ismert személytől, vagy ismerősnek tűnő forrásból is származhat!

- Gyanús a levél, ha a levél tárgya szokatlan, elgépelést tartalmaz, illetve nem munkaköri feladattal kapcsolatos.
- A levél címzettje: fertőzött lehet a levél, ha szokatlanul sok a címzettje.
- Gyanús lehet a levél, ha az alábbi kiterjesztésű csatolt állományt tartalmaz: .bat, .com, .exe, .dll, .pif, vagy beágyazott hivatkozást (linket) tartalmaz.

A fertőzöttnek ítélt elektronikus levelet megnyitás nélkül törölni kell. Levelet az előnéző ablakban sem szabad megnézni!
Gyanús levélben levő hivatkozásokat nem szabad megnyitni (rákattintani), még akkor sem, ha az látszólag ismert weboldalra mutat.

9. Internetezés biztonsága

Az ügyvitellel össze nem függő Internetes oldalak látogatása megengedett, kellő óvatosság és önmérséklet mellett.
Tilos a fájlletöltő oldalak, Internetes játékoldalak, ún. csevegő oldalak, valamint szexuális szolgáltatásokat kínáló oldalak látogatása.
Tilos az ügyvitellel össze nem függő fájlok megnyitása, letöltése az Internetről.

10. Adathordozók kezelése

A CLASSIC Kft. szervezetén kívülről származó és vírusvédelmi szempontból nem ellenőrzött adathordozót a számítógép adatmeghajtó eszközeibe helyezni, illetve bármi módon a számítógéphez csatlakoztatni (USB, FireWire, Bluetooth, stb.) tilos. Partner céggel történő folyamatos munkakapcsolat esetén, az ellenőrzés történhet a partner cégnél.
Munkaállomásokon a fájl / könyvtár megosztás csak külön engedéllyel megengedett.
Ha idegen számítógéphez kell csatlakoztatni USB pendrive-ot vagy külső winchestert, és nem kell az adathordozóra írni (arra adatot másolni), akkor - ha lehetséges - azt írásvédetté kell tenni, így a vírus nem tudja azt megfertőzni.

F o r r á s k ú t, 2018. május 24.

CLASSIC NONPROFIT KFT. Forráskút

Kocsis Mária
ügyvezető