INFORMATIKAI ÉS ADATBIZTONSÁGI SZABÁLYZAT

A Polgármesteri Hivatalban a számítógépes informatikai rendszer működtetési és adatvédelmi feladatainak ellátása az alábbiak szerint kerül szabályozásra:

I.
Általános rendelkezések

1.1. Az Informatikai szabályzat (továbbiakban: ISZ) betartása a Polgármesteri Hivatal minden dolgozójára nézve kötelező. E feladatok megszervezése és folyamatos ellenőrzése az informatikai feladatok ellátásával megbízott vállalkozás (továbbiakban: informatikus) feladata.

1.2. Az ISZ hatálya a kiterjed minden, a számítástechnikai rendszer alkalmazásával összefüggő tevékenységre és az azt végző hivatali munkatársra.

1.3. Az ISZ alkalmazásának, a számítástechnikai eszközök és szoftverek használatának irányítását és felügyeletét az informatikus látja el.

1.4. Az informatikus kötelezettségei az alábbiak:

- gondoskodik a rá bízott alkalmazások optimális működéséről,
- havonta elvégzi az egyes alkalmazások adatainak biztonsági mentését,
- installálja a rá bízott alkalmazások szoftvereit, elvégzi a megfelelő paraméterek beállításait,
- a felhasználóknak kiadja a munkájuk elvégzéséhez szükséges és elégséges hozzáférési jogosultságokat,
- gondoskodik a hozzáférési és jogosultsági rendszer folyamatos aktualizálásáról,
- a távozó munkatársak hozzáférési jogosultságait késedelem nélkül visszavonja és a hálózati tárhelyen levő adataikat tömöríti.

1.5. A Hivatalban dolgozó felhasználók kötelesek a hálózati szolgáltatások során tapasztalt bármilyen szokatlan, a normális működéstől eltérő jelenséget az informatikusoknak azonnal jelezni.

1.6. Tilos:

- a hivatalba használat céljából számítógépet illetve bármilyen informatikai eszközt (monitor, nyomtató, winchester, floppy, CD, DVD, pen-drive, digitális fényképezőgép) behozni,
- illetéktelen jogosultságok és adatok megszerzése,
- mások felhasználói nevével, jelszavával, fénymásoló-és telefonkódjával visszaélni,

- szoftver és hardver elemek megrongálása, működőképességük veszélyeztetése,
- informatikai eszközök jogosulatlan átkonfigurálása,
- szerzői joggal védett szoftverek másolása.

II.
Fizikai védelem

2.1. A számítógépek, valamint az informatikai rendszer telepítésénél gondoskodni kell arról, hogy az mindenféle előrelátható természeti csapással és emberi gondatlanságból származó, vagy szándékosan okozott kártétellel és üzemzavarral szemben az anyagi és technikai lehetőségek korlátait figyelembe véve biztonságban legyen.

2.2. A 2.1. pontban foglaltak biztosítása érdekében a számítástechnikai eszközök elhelyezésénél biztosítani kell az alábbiakat:

- a számítógép környezetében egyenletes hőmérséklet legyen biztosítva: a meghibásodások elkerülése érdekében mindent el kell követni annak érdekében, hogy a helyiség hőmérséklete semmilyen körülmények között ne emelkedhessen + 25 fok fölé, és ne csökkenjen + 10 fok alá. Azon helyiségben ahol a szerver találhatók, melyek napi 24 órán át működnek és a hivatal működését biztosítják a klimatizáció elengedhetetlen.
- az eszközöket ne érje közvetlen napsugárzás,
- a gép szellőzése jól megoldott legyen.

III.
Tűzvédelem

3.1. A nagy értékű berendezések és anyagok, valamint a Polgármesteri Hivatal számára alapvető fontosságú adatok biztonsága megfelelő tűzvédelmet követel (tűzjelző, poroltó).

3.2.A számítógép mellett csak a legszükségesebb, a konkrét feldolgozáshoz szükséges dokumentumok lehetnek. Feldolgozás után a dokumentumokat rendszerezni kell, majd további feldolgozásra vagy irattározásra át kell adni. Dokumentumot a számítógép mellett tárolni, raktározni tilos! Egyéb éghető anyag, pl. leporelló is csak a szükséges mértékben lehet a gép mellett.

3.3. Tűz keletkezése esetén az oltás haladéktalan megkezdése mellett azonnal értesíteni kell a tűzoltóságot és a tűzriadó terv szerint kell eljárni.

3.4. A helyiségben egyéb elektromos és tűzveszélyes készüléket csak a számítógéptől és a gyúlékony anyagoktól elkülönítve lehet használni.

3.5. A számítógépeket és perifériáit a napi munka befejezésével ki kell kapcsolni.

3.6. A tűzvédelmi előírások betartását a Titkársági csoport vezetője (aljegyző) és a Polgármesteri Hivatal tűzvédelemmel megbízott munkatársa köteles évente ellenőrizni.

3.7.A tűzvédelemmel összefüggő feladatokkal kapcsolatban a Polgármesteri Hivatal tűzvédelemmel megbízott munkatársa jogosult eljárni, intézkedni, illetve intézkedésre javaslatot tenni.

IV.

Érintésvédelem, eszközbeszerzés

4.1. A számítógépet, mint villamos fogyasztó-berendezést érintésvédelemmel kell ellátni.

4.2.Az adatfeldolgozás biztonsága érdekében a szükséges helyeken gondoskodni kell megfelelő kapacitású szünetmentes áramforrások telepítéséről.

4.3. Meghibásodáskor az egyes csoportok az informatikust haladéktalanul kötelesek értesíteni.

4.4. A számítástechnikai eszközbeszerzésekről a csoportok vezetői és az informatikus javaslata alapján a jegyző a Pénzügyi csoport vezetőjével egyetértésben dönt.

V.
Szoftverhez és hardverhez kapcsolódó védelmi intézkedések

5.1. A Hivatalnál rendszerszoftvert, operációs rendszert, informatikai alkalmazást kizárólag az informatikus installálhat.

5.2. Minden aktuális szoftverről egy példányban biztonsági másolatot kell készíteni. A Hivatalban használt szoftverek listáját az 1. sz. melléklet tartalmazza.

5.3. A rendszerszoftverek és operációs rendszerek minden paraméterének beállítását kizárólag az informatikus végezheti és felelős a zavartalan működésért.

5.4. Az alkalmazói szoftvereket kizárólag az informatikus installálhatja, törölheti, módosíthatja.

5.5. A hardver eszközök javítását, karbantartását csak szakember végezheti.

5.6. A Polgármesteri Hivatal számítógépei, valamint a hozzájuk tartozó eszközök és szoftverek nyilvántartását, leltározását a Polgármesteri Hivatal Pénzügyi csoport vezetője végzi az informatikus közreműködésével.

5.7.A leltározás segítése érdekében a Pénzügyi csoport technikai nyilvántartást vezet a számítástechnikai eszközökről az alábbiak szerint:

A) A dolgozóknak kiadott konfigurációkról készített nyilvántartás tartalmazza a
- dolgozó nevét,
- konfiguráció nevét,
- beszerzés dátumát,
- szállító megnevezését,
- kiadás dátumát,
- vonalkód számát.

B) Az elektronikai berendezésekről vezetett nyilvántartás tartalmazza a:
- dolgozó nevét,
- hardver megnevezését és típusát,
- kiadás dátumát,

- vonalkód számát.

C) A nyomtatókról vezetett nyilvántartás tartalmazza a:
- dolgozó nevét/ hivatali szoba számát,
- nyomtató megnevezését, típusát, márkáját,
- kiadás dátumát,
- vonalkód számát,
- gyári számot.

D) A konfigurációkra telepített szoftverekről készített nyilvántartás tartalmazza a:
- konfiguráció megnevezését,
- dolgozó megnevezését,
- kiadás dátumát,
- konfiguráció vonalkódjának számát,
- szoftver megnevezését,
- szoftver vonalkód számát,
- szoftver sorozatszámát.

5.8. A Pénzügyi csoport köteles a gépekhez és a programokhoz tartozó bizonylatok, használati utasítások, jótállási jegyek másolatát, valamint a kezelési leírások megőrzését biztosítani.

5.9. Az informatikus köteles az eszközök felhasználóit tájékoztatni a számítástechnikai eszközök és programok rendeltetésszerű használatáról, alkalmazási lehetőségeiről.

VI.
Vírusvédelem, mentesítés

6.1. A számítógép vírusok elleni védekezés érdekében e szabályzat alapján a következő rendelkezések szigorú és következetes betartása szükséges:

a) Mind a saját fejlesztésű, mind a vásárolt szoftvereket rendszerbe állításuk előtt a számítógépes hálózathoz nem kapcsolódó egyedi gépeken kell tesztelni.

b) A hivatal számítógépes rendszerét víruskereső és irtó programmal kell ellátni. A számítógép hálózathoz nem kapcsolódó egyedi gépeket külön-külön víruskereső programmal kell felszerelni.

c) Rendszeres időközönként teljes körű vírusellenőrzést kell végezni.

d) A hivatalon kívülről származó CD-ROM-okat a számítógépekben lévő CD-ROM egységekbe helyezni csak és kizárólag vírusvizsgálat után lehet.

c.) Az Internetről és külső hálózatokból letöltött fájlokat és elektronikus leveleket vírusvizsgálatnak kell alávetni. További feldolgozásra csak vírusmentes fájlokat lehet felhasználni.

d.) Számítógép vírus észlelése esetén azonnal értesíteni kell az informatikust, aki a vírusmentesítést elvégzi.

e.) Vírusfertőzöttségre utalnak az alábbi jelek:
- szokatlan rendszerviselkedés,
- lassan induló és hosszú ideig futó programok,
- az egyes állományok méretének megváltozása,
- memória csökkenése, hibás lemezterületek szaporodása,
- állományok hirtelen eltűnése,
- rendszer automatikus újraindulása,
- szokatlan jelenségek a képernyőn,
- hálózati rendellenességek,
- előzőleg hibátlanul működő programok lemerevedése és hibaüzenetek küldése.

f.) Észlelés és megsemmisítés után a vizsgálatot még egyszer újból el kell végezni.

VII.
A számítógép hálózat üzembe helyezése és lekapcsolása

7.1. A rendszer üzembe helyezésére vagy leállítására az informatikus jogosult.

7.2. Az aktív hálózati elemek lekapcsolása előtt az informatikus vagy az általa megbízott személy köteles meggyőződni arról, hogy a hálózaton, vagy az érintett hálózati szegmensen senki nem dolgozik és nincs bejelentkezve. Ennek megtörténte után a szerverek és az aktív hálózati elemek lekapcsolása a hálózati operációs rendszer kezelői leírásának megfelelően történik.

7.3.A szünetmentes tápegységet csak a saját kapcsolójával szabad az elektromos hálózatról leválasztani, azt a fali csatlakozóból kihúzni nem kell.

VIII.
Teendők áramkimaradás és egyéb, a számítógépes hálózatot érintő, veszély esetén

8.1. Áramkimaradás esetén a számítógépeket a szünetmentes tápegység néhány percig tovább üzemelteti. Amennyiben az áramkimaradás nem néhány másodpercre terjed csak ki akkor a számítógép hálózat leállítását meg kell kezdeni. Ha az lehetséges figyelmeztető üzenetet kell küldeni az összes üzemelő számítógéphez, amely szerint mindenki lépjen ki az általa használt programokból, és kapcsolódjon le a hálózatról is, ezek után a számítógépek szabályos leállítását meg kell kezdeni.

8.2. Az áramszünet, vagy a számítógépes hálózat épségét veszélyeztető helyzet elmúltával, amennyiben az biztonságos, a számítógépes hálózatot üzembe kell helyezni.

IX.
A felhasználók (munkaállomások) be- és kilépése

9.1 A számítógépes hálózatba a bejelentkezés a munkaállomás elindulása után az ügyintéző felhasználói nevével és jelszavával történik.

9.2.Minden ügyintéző hálózati jelszava egyedi. Jelszavát mindenki köteles titokban tartani, azt más dolgozó nem ismerheti. Amennyiben szükséges az informatikus köteles az ügyintézőt felszólítani, hogy változtassa meg a jelszavát.

9.3. A számítógépet használó dolgozó a munka befejezését követően köteles az általa használt programból kilépni, majd a hálózatból kijelentkezni. A gép kikapcsolása csak ezt követően történhet!
E két tevékenység elmaradása adatvesztéssel járhat!

X.
Ügyintézői jogosultságok

10.1. Minden ügyintéző jogosult használni a számítógépeken elhelyezett alábbi erőforrásokat:

1./ Saját „NÉV" könyvtárát teljes jogosultsággal.
2./„MINDENKI" könyvtár írásra és olvasásra.
3./ Opten Jogtárat csak olvasásra.
4./ Internet hozzáférés azon dolgozóknak akiknek ehhez külön hozzáférésük van.

10.2. Az egyes ügyintézők jogosultságait mindenkor az informatikus adja meg és erről jegyzéket vezet.

XI.
Adatmentéssel kapcsolatos feladatok

11.1. A számítógépes rendszer biztonságos működtetése érdekében szükséges az adatok és a programrendszerek e szabályzat szerinti mentése és tárolása.

11.2. Ha a programok, vagy az adatok mentése vagy tárolása során az adathordozó épségével és tökéletes használhatóságával kapcsolatban kétség merül fel, akkor azt az adathordozót a feldolgozásban nem szabad használni.

11.3. Az informatikus feladata a hivatal számítógép rendszerében használatos programok biztonsági tárolása. A tárolás a tárolt adatok mennyiségének megfelelő adathordozón történik.
A programrendszerekben történt változásokat úgy kell tárolni, hogy a módosítás, valamint az azt megelőző állapot is megőrzésre kerüljön.

11.4. Központi adatmentés havi rendszerességgel történik. A mentést az informatikus végzi.

11.5.A mentett adatok tárolása az adat mennyiségének megfelelő adathordozón történik. Ezen adathordozók megőrzésének határideje a tárolt adatok jellegétől függ, de legalább 1 év.

11.6.Az egyedi felhasználói programok mentését a mentéssel megbízott ügyintéző végzi. A mentés gyakorisága és megőrzésének ideje a program által támasztott követelmények szerint, valamint az informatikussal való előzetes egyeztetés alapján negyedévente történik. A mentés történhet az informatikus által kijelölt winchesterre, CD ill. DVD lemezre.

11.7. Mind a programrendszerek, mind az adatok mentése esetén meg kell győződni a mentés sikerességéről.

XII.

Adathordozókhoz kapcsolódó védelmi intézkedések

12.1. Az elöregedett, hibás működést mutató, javíthatatlan fizikai károsodást szenvedett adathordozó tovább nem használható. A rajta található menthető adatokat át kell helyezni letesztelt, sérülésmentes adathordozóra, a régit meg kell semmisíteni vagy selejtezni kell.

12.2. A véglegesen elhasználódott, valamint a megőrzési kötelezettséggel nem terhelt adathordozót selejtezni kell.

12.3. Használatra alkalmatlan CD-ket fizikailag meg kell semmisíteni.

12.4. Bizalmas adatokat, felhasználói és rendszerprogramokat tartalmazó adathordozókról az adatokat jegyző írásbeli engedélye alapján törölni kell úgy, hogy azok tartalmát vissza ne lehessen állítani vagy ha az adathordozó a törlés után tovább nem használható, az adathordózót fizikailag meg kell semmisíteni, erről nyilvántartást kell vezetni.

XIII.
Záró rendelkezések

13.1 Ezen szabályzat 2013. február 15. napján lép hatályba.

13.2 E szabályzatot valamennyi belső szervezeti egység (csoport), illetve az informatikus részére 1-1 példányban ki kell adni.

13.3 A Hivatal vezetője köteles a szabályzatot annak hatálya alá tartozó személyekkel megismertetni, és annak tényét igazoltatni.

Visegrád, 2013. február 15.

Dr. Szabó Attila
aljegyző

1.sz. melléklet

Visegrád Város Polgármesteri Hivatal
Szoftver listája

Az Informatikai és Adatbiztonsági Szabályzatban foglaltakat megismertem:

Köztisztviselő neve	Saját kezű aláírása
……..	…….
……..	…….
……..	…….
……..	…….
……..	…….
……..	…….
……..	…….
……..	…….
……..	…….
……..	…….
……..	…….
……..	…….
……..	…….
……..	…….
……..	…….
……..	…….