Csobánkai Polgármesteri Hivatal
2014 Csobánka, Fő út 1.

ADATVÉDELMI ÉS SZÁMÍTÁSTECHNIKAI VÉDELMI SZABÁLYZAT

Hatályos: 2017. január 1. napjától

Jóváhagyta:
dr. Filó-Szentes Kinga
jegyző

CSOBÁNKA KÖZSÉG JEGYZŐJE

TARTALOMJEGYZÉK

AZ ÁLTALÁNOS ÉS A POLGÁROK SZEMÉLYES ADATAIVAL KAPCSOLATOS ELJÁRÁSOK RENDJÉRE VONATKOZÓ ADATVÉDELMI, VALAMINT SZÁMÍTÁSTECHNIKAI VÉDELMI SZABÁLYZAT

Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény 24. § (3) bekezdésének felhatalmazása alapján a szervezet adatvédelemmel összefüggő feladatait és eljárási rendjét a következők szerint szabályozom.

I.
ÁLTALÁNOS ADATVÉDELMI SZABÁLYOK

1. A szabályzat célja, hatálya

A szabályzat célja, hogy a rendelkezéseink figyelembevételével meghatározza a szervezetnek a személyes adatok védelmével kapcsolatos általános feladatait és az eljárás rendjét, továbbá az adatbiztonság követelményeinek érvényesülését.

A szabályzat ***személyi hatálya*** kiterjed a Csobánkai Polgármesteri Hivatallal (a továbbiakban: Hivatal) közszolgálati jogviszonyban álló vezetőkre, ügyintézőkre, valamint a munkajogviszony keretében foglalkoztatott ügyviteli és fizikai alkalmazottakra, közszolgálati munkavállalókra. Kiterjed továbbá azokra a személyekre, akik az önkormányzattól kapott megbízásuk alapján az Adatvédelmi és Számítástechnikai Védelmi szabályzat előírt rendelkezéseivel kapcsolatba kerülnek.

A szabályzat ***tárgyi hatálya*** kiterjed Csobánka Község Önkormányzat tulajdonát képező, továbbá az épület(ek)ben lévő és használt:

- valamennyi használatban lévő, vagy tárolt informatikai berendezésre és azok műszaki dokumentációjára függetlenül attól, hogy az személyi használatra vagy szervezeti egység használatába került kiadásra;
- a Hivatalnál keletkezett minden elektronikus adatra, annak keletkezésének, felhasználásának és feldolgozásának helyétől és megjelenési formájától függetlenül;
- valamennyi adathordozóra, azok tárolására és felhasználására, illetve a beérkezés és a feldolgozás közötti időszakra;
- a Hivatal által használt felhasználói programokra és rendszerprogramokra;
- az informatikai rendszerben megjelenő valamennyi dokumentációra (fejlesztési, szervezési, programozási, üzemeltetési).

A szabályzat az informatikai rendszerrel kapcsolatos, biztonságos adatkezelési és adatvédelemi eljárásokat és feladatokat rögzít. A számítástechnikai eszközök beszerzésének és használatának, a saját készítésű és vásárolt szoftverek alkalmazásának a folyamatát, továbbá egyes személyek informatikai biztonságot érintő feladatait.

A személyes adatok védelméért, az adatkezelés jogszerűségéért a jegyző felelős.

A Hivatal köztisztviselőit érintő személyi nyilvántartások (Közszolgálati alapnyilvántartás, illetve Tartalékállomány és üres álláshely vezetése) adatvédelmére a Közszolgálati Adatvédelmi Szabályzat rendelkezése az irányadók.

A Hivatalnál nyilvántartott adatokat védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, nyilvánosságra hozatal, illetve a sérülés, törlés, vagy megsemmisülés ellen.

Iratot munkaköri feladat ellátásán kívül a munkahelyről kivinni, valamint munkahelyen kívül feldolgozni, tárolni csak a jegyző egyetértésével lehet, azzal a feltétellel, hogy az irat tartalmát illetéktelen személy ne ismerje meg.
Az iratok kezelése, tárolása során ki kell zárni annak a lehetőségét, hogy illetéktelen személy az iratok tartalmába betekintést nyerjen. Az iratokat a Hivatalnál zárható helységben, elkülönítetten kell tárolni. A munkavégzés céljára szolgáló irodákat a köztisztviselő, munkavállaló távozásakor kulcsra kell zárni.

Az irodahelységek nyitva tartása miatti iratokhoz történő illetéktelen hozzáférés esetén az érintett fegyelmi és kártérítési felelősséggel tartozik.

2. Az adatkezelés során használt fontosabb fogalmak

Adat: az adatok osztályozása szempontjából adatnak tekintjük azokat a dokumentumokat, jelentéseket, információkat, leveleket stb., amelyek az informatikai rendszerben elektronikusan tárolódnak.

Adatkezelő: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely önállóan vagy másokkal együtt az adatok kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az általa megbízott adatfeldolgozóval végrehajtatja.

Adatkezelés: az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (pl. ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítése.

Adatgazda: az a személy, akinél a rendszerben tárolásra kerülő elektronikus adat keletkezik.

Adattovábbítás: az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele.

Adathordozó: adathordozónak nevezzük az informatikai rendszertől elválasztható adattároló eszközöket.

Adatfelelős: az a közfeladatot ellátó szerv, amely az elektronikus úton kötelezően közzéteendő közérdekű adatot előállította, illetve amelynek a működése során ez az adat keletkezett.

Adatfeldolgozás: az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől, feltéve hogy a technikai feladatot az adatokon végzik.

Adatfeldolgozó: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely az adatkezelővel kötött szerződése alapján - beleértve a jogszabály rendelkezése alapján történő szerződéskötést is - adatok feldolgozását végzi.

Adatmegsemmisítés: az adatokat tartalmazó adathordozó teljes fizikai megsemmisítése.

Adattörlés: az adatok felismerhetetlenné tétele oly módon, hogy a helyreállításuk többé nem lehetséges.

Adatzárolás: az adat azonosító jelzéssel ellátása további kezelésének végleges vagy meghatározott időre történő korlátozása céljából.

Dokumentum: számítástechnikai eszközökkel készített irat vagy fájl (például Word szövegszerkesztővel vagy Excel táblázatkezelővel készített állomány, stb).

Felhasználó: minden dolgozó, aki az informatikai szolgáltatásokat használja.

Hozzáférés: olyan eljárás, amely lehetővé teszi valamely informatikai rendszer használója számára, hogy a rendszerben lévő adatokat elérje (írás, olvasás, módosítás, törlés, stb.).

Hozzájárulás: az érintett akaratának önkéntes és határozott kinyilvánítása, amely megfelelő tájékoztatáson alapul, és amellyel félreérthetetlen beleegyezését adja a rá vonatkozó személyes adatok - teljes körű vagy egyes műveletekre kiterjedő – kezeléséhez.

Közérdekből nyilvános adat: a közérdekű adat fogalma alá nem tartozó minden olyan adat, amelynek nyilvánosságra hozatalát, megismerhetőségét vagy hozzáférhetővé tételét törvény közérdekből elrendeli.

Közzététel: közérdekű és közérdekből nyilvános adatoknak internetes honlapon, digitális formában, bárki számára, személyazonosítás nélkül, korlátozástól mentesen, díjmentesen történő hozzáférhetővé tétele.

Különleges adat:

a) a faji eredetre, a nemzetiséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdek-képviseleti szervezeti tagságra, a szexuális életre vonatkozó személyes adat,

b) az egészségi állapotra, a kóros szenvedélyre vonatkozó személyes adat, valamint a bűnügyi személyes adat.

Közérdekű adat: az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő és tevékenységére vonatkozó vagy közfeladatának ellátásával összefüggésben keletkezett, a személyes adat fogalma alá nem eső, bármilyen módon vagy formában rögzített információ vagy ismeret, függetlenül kezelésének módjától, önálló vagy gyűjteményes jellegétől, így különösen a hatáskörre, illetékességre, szervezeti felépítésre, szakmai tevékenységre, annak eredményességére is kiterjedő értékelésére, a birtokolt adatfajtákra és a működést szabályozó jogszabályokra, valamint a gazdálkodásra, a megkötött szerződésekre vonatkozó adat.

Személyes adat: az érintettel kapcsolatba hozható adat - különösen az érintett neve, azonosító jele, valamint egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző ismeret -, valamint az adatból levonható, az érintettre vonatkozó következtetés.

3. Személyes adatok védelme

A jegyző a személyes adatkezelést végző személy munkaköri leírásában határozza meg az általa kezelhető és elérhető személyes nyilvántartások körét.

A személyes adatkezelést végző személy felelősséggel tartozik azért, hogy tevékenységét az adatkezelésre és az adatok védelmére vonatkozó jogszabályoknak, az adatkezelést elrendelő jogszabály hiányában pedig az érintett hozzájárulásának megfelelően végezze. Az adatgazda a nyilvánvalóan jogsértő adatkezelési utasítását köteles megtagadni és erről a szervezet vezetőjét (jegyzőt) haladéktalanul írásban tájékoztatni.

Az adatkezelési tevékenységet végző személyek kötelesek az adatvédelmi és az adatbiztonsági szabályokat betartani.

Az adatgazda azokat a személyes adatokat veheti fel, illetve veheti át harmadik személytől, amelyek kezelésére törvény vagy az érintett felhatalmazza.

Az érintett hozzájárulásán alapuló adatkezelésnél az adat felvételekor az érintettet előzetesen tájékoztatni kell az adatszolgáltatás önkéntességéről és kérésére a hozzájárulás megadásának vagy megtagadásának az adatkezelő tevékenységi körébe eső következményeiről.

Az adatok tárolási módját úgy kell megválasztani, hogy törlésük az adattörlési határidő lejártakor, illetve ha az más okból szükséges, elvégezhető legyen.

Az adatok a jogszabályban és a besorolási kategóriában elfoglalt helyük szerint a meghatározott célra használhatók fel.

A Hivatal számítógépes hálózatán lévő nyilvántartásokba történő belépés a jegyző döntése alapján – a személyes jelszón kívül – a hálózati szoftverben egyedileg beállított hozzáféréssel engedélyezhető. A belépés csak a legszükségesebb körben, az ügyintéző munkaköri feladatai ellátásához kapcsolódóan engedélyezhető a következők szerint:

Megnevezés	Hozzáférési jogosultság
Ügyirat nyilvántartás	*ügyiratkezelők*
Közszolgálati alapnyilvántartás KÖZIGTAD	*Pénzügyi Csoport*
Illetmény átutalás	
Hatósági statisztika	*ügyiratkezelők, hatósági ügyintéző*
Gyámügyi statisztika	*gyámügyi ügyintéző*
Vagyonnyilvántartás	*műszaki ügyintéző*

A Hivatal által elérhető nem saját személyes adatokat tartalmazó nyilvántartásokból történő adatkezelés esetén az alábbiak szerint kell eljárni:

- Az adatkezelésre jogosultak jóváhagyása a jegyző feladatkörébe tartozik. A belépésre vonatkozó személyi javaslat csak a munkavégzéshez feltétlenül szükséges, lehető legszűkebb körre vonatkozhat. (***2. sz. melléklet***)

II.
ADATVÉDELMI SZABÁLYOK A POLGÁROK SZEMÉLYES ADATAIVAL KAPCSOLATOS FELADATOKRA ÉS ELJÁRÁSOK RENDJÉRE

1. Általános rendelkezések

E szabályok célja, hogy a vonatkozó jogszabályok rendelkezéseinek figyelembevételével meghatározza a polgárok személyes adatai védelmével kapcsolatos feladatait, az eljárások rendjét.

2. Értelmező rendelkezések

A polgár természetes személyazonosító adatai: családi és utóneve(i), születési családi és utóneve(i) (a továbbiakban együtt: név); neme; születési helye és ideje; anyja leánykori családi és utóneve(i) (a továbbiakban : anyja neve).

A polgár lakcím adata: bejelentett lakóhelyének, illetve tartózkodási helyének címe (a továbbiakban együtt: lakcím).

Adatszolgáltatás: a nyilvántartásban szereplő polgárok adatainak a törvényben meghatározott tartalmú és terjedelmű közlése. Ezen belül:

- egyedi adatszolgáltatás: egy polgár adatainak közlése;
- csoportos adatszolgáltatás: az adatigénylő által vagy jogszabályban meghatározott szempontok szerint képzett csoportba tartozó polgárok adatainak rendszeres vagy eseti közlése.

3. Személyes adatok védelme

Az adatkezelés törvényességének ellenőrzése az adatvédelmi felelős feladata, aki a munkaköri leírása alapján a jegyző által megbízott ügyintéző.

4. Adatszolgáltatás

Az adatszolgáltatás iránti kérelem elbírálása a jegyző hatáskörébe tartozik.

Az adatszolgáltatás iránti kérelmet jogszabályban meghatározott tartalommal kell benyújtani.

Az adatszolgáltatás iránti kérelmet 30 napon belül kell elbírálni.

Az adatszolgáltatásért – a 16/2007. (III. 13.) IRM-MeHVM együttes rendelet előírásai alapján – fizetendő igazgatási szolgáltatási díj összegének mértékéről az engedélyező határozatban rendelkezni kell.

Az érintett polgár adatai szolgáltatását korlátozó, vagy tiltó nyilatkozatát, illetőleg annak visszavonását személyesen, vagy meghatalmazott képviselője útján, továbbá ajánlott levélben teheti meg a Hivatalnál. (***1. számú melléklet***)

Az érintett polgár tájékoztatást kérhet személyes adatai kezeléséről, kérheti személyes adatainak helyesbítését, törlését.

Az érintett kérelmére a Hivatal – a kérelem benyújtásától számított legrövidebb idő alatt, legfeljebb azonban 30 napon belül – tájékoztatást ad az általa kezelt adatairól, továbbá arról, hogy kik és milyen célból kapják, vagy kapták meg az adatokat.

III.
SZÁMÍTÁSTECHNIKAI VÉDELMI SZABÁLYOK

1. Adatok és programok védelme

A szervezet számítógépes adat-feldolgozási folyamatába kerülő információkat és programokat fokozott biztonsági szabályok szerint kell kezelni. Ennek oka, hogy a számítógépen titoknak minősített adatokat nem tárolnak, illetve a feldolgozás során keletkező adatok sem minősülnek titkosnak. Ezen fokozatba sorolás független az adatok megjelenési formájától.
Ettől eltérő esetben a titkos ügykezelés szabályai szerint kell eljárni.

A Hivatalnál működő számítógépeken csak előzetesen ellenőrzött programot szabad futtatni. Az ellenőrzésnek ki kell terjednie a vásárolt vagy átvett program tesztelésére, esetleges működést akadályozó hibák felderítésére. A feltárt hiányosságokról jegyzőkönyvet kell felvenni, melyet a programot szállító szervhez haladéktalanul el kell juttatni. Hibás programot üzembe helyezni tilos.

Tilos vírusellenőrzés nélkül adathordozót a számítógépbe helyezni, arról programot vagy adatot a rendszerbe tölteni!

A tesztelést a felhasználóval közösen az informatikai feladatot ellátó ***megbízott vállalkozó végzi.***

Vásárolt, vagy átvett adathordozón tárolt program esetén minden esetben biztonsági másolatot kell készíteni, majd az eredeti lemezt írásvédetté kell tenni.
A programok felhasználói dokumentációját a felhasználás helyén kell elhelyezni.

Feldolgozásra kerülő adatok előkészítése

a) Számítástechnikai feldolgozásra csak tartalmilag és formailag ellenőrzött adatok kerülhetnek.

b) Az ellenőrzésért az adatfelelősség elve szerint adatlapos rögzítés esetén az adatlapot kiállító, adatlap nélküli rögzítés esetén feldolgozást végző kijelölt köztisztviselő felelős. Lehetőség szerint biztosítani kell, hogy az adatok a keletkezés helyén kerüljenek rögzítésre.

Feldolgozás folyamata

a) Az adatállományok módosítását kizárólag csak a feldolgozásra készült programmal lehet elvégezni.

b) Az adatfeldolgozás során a számítógép- vagy programhibából adódó adatvesztés fordulhat elő. Ilyenkor az adatrögzítést azonnal be kell fejezni és a további adatvesztés elkerülésére az informatikai felelőst haladéktalanul értesíteni kell.

Mentés

a) A számítógépeken tárolt információk biztonságos megőrzése céljából az adatokat szükséges rendszerességgel legalább két egyező példányban menteni kell.

b) Naponta szükséges menteni az iktatási adatállományokat adathordozóra és a hálózati rendszerbe is.

c) Hetente mentést kell végezni a hálózati működést biztosító központi gépen történt adatváltozásokról.

d) Az egyedi gépekről a mentést az egyedi gép használója, a szervezet központi szervergépéről a mentést a kijelölt számítástechnikai megbízott végzi el.

Másolás

A számítógépes programok a szerzői jog szerint védelmet élveznek, ezért másolásuk, harmadik fél számára történő továbbadásuk tilos.

Törlés

Mágneses adathordozókon tárolt adatok és programok törlését csak a jegyző írásbeli engedélye alapján lehet elvégezni. Külön figyelmet kell fordítani az irattárazási és selejtezési szabályok betartására.

Archiválás

Az informatikai eszközein tárolt adatok archiválását az adatok biztonságos kezelése érdekében a szervezetnél évente egyszer (december 31-ig) kell elvégezni. Az archív adatok tárolásánál figyelembe kell venni a biztonsági előírásokat (zárható, tűzbiztos tárolóeszköz), és biztosítani kell a tárolási körülményeket (hőmérséklet, páratartalom).

Visszatöltés

Az adathordozókon tárolt adatok visszatöltését, visszaállítását a jegyző engedélyezheti. Ez alól kivételt képeznek az egyedi felhasználók, akik a mentésekből saját munkakönyvtáruk adatait engedély nélkül is visszatöltetik.

2. Számítógépek, eszközök és dokumentációk védelme

A számítógépek és eszközök rendeltetésszerű használatáért a személyi leltár szerint a használatra kijelölt köztisztviselő felelős.

A hálózati működő számítógépeken kizárólag az erre kiképzett szakemberek dolgozhatnak.

Meghibásodás megelőzéséről folyamatos karbantartással kell gondoskodni, üzemzavar esetén a javítást csak arra kiképzett szakember végezheti.

Fizikai sérülések megelőzésére (pl.: hálózati vezetékszakadás) a számítógépet telepítési helyéről elmozdítani, vagy áthelyezni nem szabad.
Vagyonvédelmi megfontolásból azokat a szobákat, ahol számítógép üzemel, biztonsági felszereléssel kell ellátni. A köztisztviselő köteles a munkaidő végzetével a számítógépet kikapcsolni, az azok elhelyezésére szolgáló irodahelységet bezárni és a kulcsot az időpont dokumentálásával elzárt helyen letenni. A Hivataltól javításra, vagy más célból elszállítani eszközöket csak bizonylatolás után lehet.

Elektromos érintésvédelmi szempontból a számítástechnikai eszközöket csak védőföldeléses, minden számítógéphez leltár szerint tartozó biztonsági kapcsolóval ellátott dugaszoló aljzatba lehet csatlakoztatni. Annak sérülését minden esetben jelezni kell. ***A berendezéseket vízzel oltani vagy tisztítani tilos!***

3. Mágneses adathordozók védelme

A mágneses adathordozók védelmére és azonosítására az adathordozókat azonosítóval (címkével) kell ellátni és azokról nyilvántartást kell vezetni.

A mentést tartalmazó adathordozók megőrzési idejét úgy kell meghatározni, hogy azokról az aktuális adatállomány sérülés esetén visszaállítható legyen.

Vírust tartalmazó, nem mentesíthető adathordozót használatban tartani nem lehet.
Az adathordozót óvni kell a szennyeződésektől és a fizikai sérüléstől, ezért használat közben óvakodni kell a mágnesezhető réteg megérintésétől, használat után pedig zárható dobozban, vagy a gyári csomagolásban elektromos erőterektől távol (monitor, televízió, hangszóró, ventilátor, telefon, rádió, stb.) kell tartani.

Külső szervnek átadott adathordozókról bizonylatot (az átadás, átvétel időpontját, az átadás célját, az átadott adathordozó számát, tartalmát az átvevő szerv megnevezését és címét, az átadás idejét, (ideiglenesen vagy véglegesen) az átvevő szerv őrzéssel megbízott felelősének megnevezését, valamint az átadó és átvevő szerv erre feljogosított képviselőjének aláírását tartalmazó jegyzéket) kell készíteni.

4. Az adathordozók selejtezése

A szervezet által vásárolt és a dolgozó(k) részére kiadott adathordozót abban az esetben kell selejtezni, ha:

- fizikailag megsérült,
- gyári, gyártási hibából következően felhasználásra alkalmatlan,
- a tároló kapacitás a megengedhető érték alá csökken,
- véglegesen elhasználódott.

A felhasználók felelőssége, hogy a használhatatlanná vált adathordozókat (floppy, CD, DVD, stb.) a jegyző felé jelezze, aki gondoskodik azok közös helyen történő összegyűjtéséről. A selejtezés előtt biztosítani kell az adathordozón tárolt adatok biztonságos törlését (fizikai törléssel, formattálással). Ha a tárolt adatok biztonságosan nem törölhetők, akkor az adathordozót úgy kell megsemmisíteni, hogy további felhasználásra már alkalmatlan legyen, azaz fizikai roncsolással kell használhatatlanná tenni.

A megsemmisítés során a felesleges vagyontárgyak hasznosításának és selejtezésének szabályzatában előírtak szerint kell eljárni, annak tényét megsemmisítési jegyzőkönyvben kell rögzíteni.

5. Vírusvédelmi eljárások

A Hivatalnál alkalmazott vírusvédelmi rendszernek meg kell felelnie a következő elvárásnak:

- a vírus védelmi szoftvernek jó minőségűnek és kellő gyakorisággal aktualizáltnak (frissítettnek) kell lennie, hogy felismerési hatékonysága maximális legyen;
- a vírus védelmi szoftvernek minden támadási ponton aktívan üzemelnie kell.

A Hivatal egészére kiterjedően a vírusfertőzések megelőzése, kiszűrése és megszüntetése céljából a Kaspersky Anti-Virus elnevezésű vírusvédelemi szoftvert alkalmazza. A szoftver teljes számítástechnikai gépparkot lefedő (beleértve a mobil eszközöket is) telepítéséért, naprakész és folyamatos üzemeltetéséért, frissítéséért, a vírustámadások elleni védekezés megszervezéséért a megbízott felelős. Az újonnan vásárolt számítógépekre azok rendszerbe állítása során telepíteni kell a víruskereső programot.

A számítógépes munkaállomásokon a víruskereső programot úgy kell beállítani, hogy naponta egyszer (az első bejelentkezéskor) megtörténjen az automatikus vírusteszt futtatása. A rendszerbe kívülről bekerülő adatokat (floppylemez, USB portról csatlakoztatható eszközök, CD-ROM, Internet stb.) felhasználás előtt vírusellenőrzésnek kell alávetni. A víruskereső program munkaállomásokon történő lefuttatása a külső megbízott feladata és felelőssége.

A víruskereső szoftvernek minden lehetséges bejutási pontot (floppylemez, USB portról csatlakoztatható eszközök, CD-ROM, hálózat, e-mail, stb.) ellenőriznie kell, így az elsődleges támadási felületnek minősülő munkaállomásokat, és a másodlagos támadási felületnek minősülő tűzfalakat, alkalmazás és levelező szervereket.

A vírusadatbázisok frissítése a rendszer hatékony működésének szempontjából fontos, mivel az új vírusok megjelenése és elterjedése között rövid idő (esetenként néhány óra) telik el.

6. A vírusvédelem szabályai a felhasználó részéről

A Hivatalnál alkalmazott Kaspersky Anti-Virus elnevezésű vírusvédelmi rendszer a számítógépek működése közben folyamatosan dolgozik, így a felhasználói munka során igénybe vett állományok (programok, adatok, dokumentumok) közvetlenül már a használat előtt vírusellenőrzése kerülnek.

A számítástechnikai eszközökön beállított aktív védelemi rendszer kikapcsolása tilos. A rendszer kikapcsolásából adódó károkért (adatvesztés, illetéktelen hozzáférés stb.) a szabályt megszegő teljes körű felelősséggel tartozik.
Amennyiben a felhasználó a víruskereső program *„futtatása"* során vírust észlel, azonnal jelentenie kell a külső megbízott felé, aki feljegyezi a vírus és a fertőzött file nevét, továbbá a munkaállomás számát (helyét). A külső megbízott gondoskodik a vírus további terjedésének megakadályozásáról, és – amennyiben a felhasználói gépen futó program automatikusan nem törölte – a vírus szakszerű kiirtásáról.

7. Az elektronikus levelezés vírusvédelme

Ha a szervezet elektronikus levelezési rendszerén keresztül fertőzött levél, vagy csatolt állomány érkezik, arról a Kaspersky Anti-Virus víruskereső szoftver értesíti a felhasználót (és amennyiben van a rendszergazdát). Ha az aktív védelem a fertőzött állományt eltávolítja, akkor a munka megkezdhető vagy tovább folytatható, amennyiben nem képes a fertőzés eltávolítására, akkor a víruskereső rendszer a fertőzött állományt törli.
Ha a felhasználó levelezési rendszerébe indokolatlan vagy váratlan e-mail érkezik annak tartalmát személyesen (pl. telefonon, e-mailben) ellenőrizni szükséges. Ha a küldő nem szándékosan mellékelt az e-mailhez állományt, akkor nem szabad megnyitni.

IV.
ZÁRÓ RENDELKEZÉS

A jelen szabályzat 2017. január 1. napján lép hatályba, mellyel egyidőben a tárgyban kiadott valamennyi szabályzat hatályát veszíti.

A költségvetési szerv vezetőjének kell gondoskodni, hogy a Szabályzatban foglalt előírásokat az érintett munkatársak megismerjék, annak tényét a szabályzat *mellékletében* szereplő megismerési nyilatkozaton aláírásukkal igazolják a hatálybalépés napjával egyidejűleg.

Csobánka, 2017. január 1.

dr. Filó-Szentes Kinga
jegyző

CSOBÁNKA KÖZSÉG JEGYZŐJE

1. sz. melléklet

Tárgy: Adatszolgáltatás letiltása a … nyilvántartásból

Címzett

Települési Önkormányzat
jegyzőjének

Település

Tisztelt Jegyző Asszony/Úr!

Alulírott ……..– a további jognyilatkozatom megtételéig – a … személyes adataim kiadását, az erre vonatkozó adatszolgáltatás végzését a mai nappal kezdődően letiltom.

A tilalommal érintett valamennyi az Önök által vezetett nyilvántartásokban levő személyes adatom külön-külön is csak külön írásbeli eseti engedélyem alapján szolgáltatható ki.

Kérem, hogy a kérelmem alapján a megtett intézkedéséről írásban értesítsen.

Kelt,……., 201…év……..hó…….nap

……
aláírás

2. sz. melléklet

HOZZÁFÉRÉSI JOGOSULTSÁG

Sor-szám	Adatfeldolgozás megnevezése	Név	Beosztás
1.	Ügyirat nyilvántartás	dr. Filó-Szentes Kinga Törökériné Varga Erzsébet	*jegyző / érintett köztisztviselő*
2.	Közszolgálati alapnyilvántartás KÖZIGTAD	dr. Filó-Szentes Kinga Katona-Berényiné Ferencz Krisztina	*jegyző / pénzügyi csoportvezető*
3.	Illetmény átutalás	dr. Filó-Szentes Kinga Katona-Berényiné Ferencz Krisztina	*jegyző / pénzügyi csoportvezető*
4.	Hatósági statisztika	dr. Filó-Szentes Kinga Törökériné Varga Erzsébet	*jegyző / érintett köztisztviselő*
5.	Gyámügyi statisztika	dr. Filó-Szentes Kinga Karányi Krisztina	*jegyző / érintett köztisztviselő*
6.	Vagyonnyilvántartás	dr. Filó-Szentes Kinga Katona-Berényiné Ferencz Krisztina Viza Zsuzsanna	*jegyző / pénzügyi csoportvezető / műszaki ügyintéző*

Megismerési nyilatkozat

Az adatvédelmi és számítástechnikai védelmi szabályzatában foglaltakat megismertem. Tudomásul veszem, hogy az abban foglaltakat a munkavégzésem során köteles vagyok betartani.

Név	Beosztás	Kelt	Aláírás
KATONA - BERÉNYINÉ FERENCZI KRISZTINA	PÉNZÜGYI CSOPORTVEZETŐ	2017.01.02.	
[illegible]	Műszaki ü.	2017.01.02	
[illegible]	Adóhatósági ü.	2017.01.02.	
KARÁCSONY KRISZTINA	szociális ü.	2017.01.02.	
IMRE ZSUZSANNA	Igazgatási ü.	2017.01.02.	
DR. FILÓ-SZENTES KINGA	jegyző	2017.01.02.	
MÉSZÁROS ILONA	családsegítő	2017.01.02.	
BALOGÁNÉ ERDEI KATALIN	CSALÁDSEGÍTŐ	2017.01.02.	
TÖRÖLÉKINÉ VARGA [illegible]	NÉPESSÉG ÜGYINTÉZŐ	2017.01.02.	
MILLER-TÓTH CECÍLIA	ADÓHATÓSÁGI ü.	2017.01.02.	
WINKLER SÁNDOR JÓZSEFNÉ	polgármester	2017.01.02.	
UJHÁRI MÓNIKA	pénzügyi ü.	2017.05.15.	