

Tiszajenői Közös Önkormányzati Hivatal
5094 Tiszajenő, Vasút utca 11.

**ADATVÉDELMI ÉS SZÁMÍTÁSTECHNIKAI
VÉDELMI SZABÁLYZAT**

Érvényes: 2017. február 1-től

ADATVÉDELMI ÉS 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 Tiszajenői Közös Önkormányzati Hivatal, Tiszajenő Községi Önkormányzat, Vezseny Községi Önkormányzat, Tiszajenő-Tiszavárkony Víziközmű Beruházási Társulás szervezettel 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 a 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 szervezetnél 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 szervezet 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 adatvédelmi 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 szervezet vezetője (jegyző) felelős.

A szervezet által vezetett személyes adatokat tartalmazó, illetve a személyes adatokat nem tartalmazó nyilvántartásokat, valamint az azokból történt adattovábbításokat, továbbá a

szervezet által elérhető személyes adatokat tartalmazó, nem saját nyilvántartásokat jelen szabályzat **1-6. számú melléklete** tartalmazza.

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

A szervezetnél 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 szervezet vezetője (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 szervezetnél 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 feygelmi 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 tenyérynnyomat, 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.

Adatvédelmi incidens: személyes adat jogellenes kezelése vagy feldolgozása, így különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés.

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 szervezet vezetője (jegyző) a személyes adatkezelést végző személy munkaköri leírásában határozza meg az általa kezelhető és elérhető személyes nyilvántartások körét.

A személyes adatkezelést végző személy felelőséggel 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 szervezet számítógépes hálózatán lévő nyilvántartásokba történő belépés a szervezet vezetőjének (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
<i>Ügyirat nyilvántartás</i>	<i>ügyiratkezelők</i>
<i>Közzolgálati alapnyilvántartás KÖZIGTAD</i>	<i>személyzeti ügyintéző</i>
<i>Illetmény átutalás</i>	<i>pénzügyi ügyintéző</i>
<i>Hatósági statisztika</i>	<i>hatósági ügyintéző</i>
<i>Szabálysértési statisztika</i>	<i>hatósági ügyintéző</i>
<i>Gyámügyi statisztika</i>	<i>gyámügyi ügyintéző</i>
<i>Vagyonynyilvántartás</i>	<i>pénzügyi ügyintéző</i>

(A hozzáférési jogosultság általánosságban a hálózaton levő adatok feldolgozását jelenti, melyet az adott munkakör ellátására feljogosított ügyintéző végez. A hozzáférés jogosultság

lekérdezés formájában történő megvalósítása csak egyes nyilvántartásoknál lehet mindenkire kiterjedő. Ilyen pl.: a szervezet ügyirat nyilvántartása.)

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

- Az adatkezelésre jogosultak névsorának jóváhagyása a szervezet vezetője (jegyző) feladatkörébe tartozik. A belépésre vonatkozó személyi javaslat csak a munkavégzéshez feltétlenül szükséges, lehető legszűkebb körre vonatkozhat.
- Hozzáférési jogosultsággal rendelkező adatkezelő az adatlekérdezésekről e szabályzat mellékletét képező „Adatszolgáltatási nyilvántartást” köteles vezetni.

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), nők esetében leánykori 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 szervezet vezetője (jegyző) által megbízott ügyintéző. Az adatvédelmi felelős ellátja az Info. tv. 24. § (2) bekezdésében meghatározott feladatokat, továbbá ellenőrzi az

adatvédelmi incidenssel kapcsolatos intézkedéseket és vezeti az adatvédelmi incidenssel kapcsolatos nyilvántartást az Info. tv. 15. § (1a) bekezdés meghatározott tartalommal.¹

(Az adatvédelmi felelős alkalmazása /kinevezése/ a jelenleg hatályos jogszabály szerint csak egyes államigazgatási szerveknél kötelező /az országos hatósági, munkaiügyi vagy büntügyi adatállományt kezelő, illetve feldolgozó adatkezelőnél és adatfeldolgozónál, a pénzügyi szervezetnél, az elektronikus hírközlési és közüzemi szolgáltatónál /, a jogszabály azonban nem tiltja meg azt, hogy ezen szerveken kívül is kinevezhető legyen adatvédelmi felelős, alkalmazása nagyobb szervezeteknél célszerű.

Az adatvédelmi felelős feladata, a szervezeti adatkezelés törvényességének ellenőrzése. E feladatkörrel megbízni a szervnél az adatvédelemért, valamint a számítástechnikai berendezések üzemeltetéséért felelős szervezeti egység valamely köztisztviselőjét célszerű, akinek munkaköri leírásában ezt fel kell tüntetni.)

4. Adatszolgáltatás

Az adatszolgáltatás iránti kérelem elbírálása a szervezet vezetője (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 adatszolgáltatások engedélyezéséről az igazgatási ügyintéző nyilvántartást köteles vezetni, melynek adattartalmát a **8. sz. melléklet** tartalmazza.

Adatszolgáltatásnak minősül, így a nyilvántartásnak tartalmaznia kell a szervezet munkatársai által, feladatkörük ellátása érdekében, egyedi ügyeik elintézése céljából igényelt adatok közlését is.

Az érintett polgár adatai szolgáltatását korlátozó, vagy tiltó nyilatkozatát, illetőleg annak visszavonását személyesen, vagy meghatalmazott képviselője útján, továbbá ajánlott levélben teheti meg a szervezetnél. (**10. számú melléklet.**) az adatszolgáltatást korlátozó, vagy megtiltó, vagy ezek visszavonásáról rendelkező nyilatkozatokról nyilvántartást vezet, melynek adattartalmát a **9. sz. melléklet** tartalmazza.

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

Az érintett kérelmére az igazgatási ügyintéző – 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.

¹ Beiktatta: 2015. évi CXXIX. törvény 3. §. Hatályos: 2015. X. 1-től.

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 titkosnak 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 szervezetnél 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 felárt 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 köztisztviselő 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 adatfelelőség 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) Egyedi gépek vagy programok esetén a mentés gyakoriságát az adott adatfeldolgozási tevékenységet felügyelő illetékes vezető határozza meg.
- e) Az egyedi gépekről a mentést az egyedi gép használója, a szervezet központi szervergépéről a mentést a kijelölt számítástechnikai munkatárs 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 tevékenységet felügyelő illetékes vezető írásbeli engedélye alapján lehet elvégezni. Külön figyelmet kell fordítani az irattározási 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 szervezetnél annak vezetője (jegyző) engedélyezheti. Ez alól kivételt képeznek az egyedi felhasználók, akik a mentésekből saját munkakönyvtáruk adatait engedély nélkül is visszatöltetik.

Hálózati alkalmazások esetében az adatvesztés elkerülésére és az adatbiztonság fokozására személyre lebontott hozzáférési jogosultságot kell meghatározni. (**11. számú melléklet**).

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 végétével a számítógépet kikapcsolni, az azok elhelyezésére szolgáló irodahelységet bezárni és a kulcsot az időpont dokumentálásával elzárt helyen letenni. A szervezettől javításra, vagy más célból elszállítani eszközöket csak bizonylatolás után lehet.

(A vagyonsvédelemmel összefüggésben meg kell említeni, hogy a technikai, adminisztratív védelem /az informatikai rendszerben az adatkezelésre vonatkozó adatvédelmi és adatbiztonsági követelmények meghatározása/ a helyi sajátosságoktól, de elsősorban a szerv által kezelt biztonsági okmányoktól függően különböző lehet. A 86/1996. (VI. 14.) Korm. rendelet szerint az úgynevezett okmányvédelmi kategóriák /„A”, „B”, „C”/ követelményei alapján kell meghatározni a védelmi módszereket és az adminisztratív eljárásokat.)

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!**

A tűz elleni védekezés rendjét és elhárítása érdekében szükséges intézkedéseket a szervezet Tűzvédelmi Szabályzata tartalmazza.

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 szervezet vezetője (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 szervezetnél 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 szervezet egészére kiterjedően a vírusfertőzések megelőzése, kiszűrése és megszüntetése céljából a elnevezésű vírusvédelmi szoftvert alkalmazza. A szoftver teljes számítástechnikai gépparkot lefedő (beleértve a mobil eszközöket is) telepítéséért, naprakész és folyamatos üzemeltetéséért, frissítéséért, a vírustámadások elleni védekezés megszervezéséért az informatikus 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 vírusesztt 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 felhasználó 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 szervezetnél alkalmazott 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 felé, aki feljegyezi a vírus és a fertőzött file nevét, továbbá a munkaállomás számát (helyét). A 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 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 mellékelte az e-mailhez állományt, akkor nem szabad megnyitni.

IV. ZÁRÓ RENDELKEZÉS

Ez a szabályzat 2017. január 1. napján lép hatályba.

Tiszajenő, 2017. január 1.

Gyapjasné Sepsi Erzsébet
jegyző

I. SZEMÉLYES ADATOKAT TARTALMAZÓ NYILVÁNTARTÁS

Saját nyilvántartások

Sor-szám	Megnevezés	Típus	Jog-szabály	Érintettek köre	Adatok forrása	Adatkezelés		Archiválás	Adat-továbbítás	Adat-védelmi szabályzat	Hozzáférési jogosultság	
						helye	módja				Adat-feldolgozás	csak lekérdezés
1.												
2.												
3.												
4.												
5.												
6.												
7.												
8.												
9.												
10.												
11.												
12.												
13.												
14.												
15.												
16.												

HOZZÁFÉRÉSI JOGOSULTSÁG

Sor-szám	Adatfeldolgozás megnevezése	Ügyiratszám	Név	Munkahely
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				
16.				
17.				
18.				

A SZÁMÍTÓGÉPES RENDSZERBE BELÉPÉSRE JOGOSULTAKRÓL

Sor- szám	Név	Beosztás
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		
11.		
12.		
13.		
14.		
15.		
16.		
17.		
18.		
19.		
20.		
21.		
22.		
23.		
24.		
25.		
26.		
27.		
28.		
29.		
30.		

8. sz. melléklet

Lapszám:

ADATSZOLGÁLTATÁSI NYILVÁNTARTÁS

Ügyintéző neve:

.....adatbázisból

Sor-szám	Dátum	Ügyirat szám	Érintett személy neve, szül. ideje	Igénylő megnevezése	Lekérdezés célja, jogalapja	Lekérdező neve	Megjegyzés
1.							
2.							
3.							
4.							
5.							
6.							

**AZ ADATSZOLGÁLTATÁSI KORLÁTOZÁSRÓL TETT NYILATKOZAT NYILVÁNTARTÁSI
ADATTARTALMÁRÓL**

Hozzáférési jogosultság

Sor- szám	Nyilatkozó neve	Személyi azonosítója	Lakóhelye	Tartózkodási helye	Nyilatkozattétel ideje
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					
11.					
12.					
13.					
14.					

10. 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

HOZZÁFÉRÉSI JOGOSULTSÁG

Sor-szám	Adatfeldolgozás megnevezése	Név	Beosztás
1.	Ügyirat nyilvántartás		<i>jegyző / szervezetvezető érintett szervezeti egység vezetője ügyiratkezelő</i>
2.	Közzolgálati alapnyilvántartás KÖZIGTAD		<i>jegyző / szervezetvezető érintett szervezeti egység vezetője személyzeti ügyintéző</i>
3.	Illetmény átutalás		<i>jegyző / szervezetvezető érintett szervezeti egység vezetője pénzügyi ügyintéző</i>
4.	Hatósági statisztika		<i>jegyző / szervezetvezető érintett szervezeti egység vezetője hatósági ügyintéző</i>
5.	Szabálysértési statisztika		<i>jegyző / szervezetvezető érintett szervezeti egység vezetője hatósági ügyintéző</i>
6.	Gyámügyi statisztika		<i>jegyző / szervezetvezető érintett szervezeti egység vezetője gyámügyi ügyintéző</i>
7.	Vagyonnyilvántartás		<i>jegyző / szervezetvezető érintett szervezeti egység vezetője pénzügyi ügyintéző</i>

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