

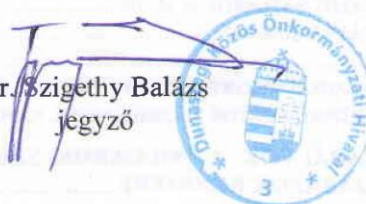
**ADATVÉDELMI, SZÁMÍTÁSTECHNIKAI VÉDELMI ÉS  
INFORMATIKAI BIZTONSÁGI SZABÁLYZAT**

**KÖZZÉTÉTELI REND**

**Érvényes: 2014. június 1-től**

Jóváhagyom:

dr. Szigethy Balázs  
jegyző



# TARTALOMJEGYZÉK

<b>I. SZABÁLYZAT CÉLJA, HATÁLYA</b> .....	<b>4</b>
<b>II. INFORMATIKAI STRATÉGIA</b> .....	<b>5</b>
1. A JELENLEGI INFORMATIKAI HELYZET BEMUTATÁSA .....	5
2. INFORMATIKAI INFRASTRUKTÚRA .....	6
<i>A szervezet informatikai ellátottsága</i> .....	6
<i>A település és a lakosság informatikai ellátottsága</i> .....	7
<i>Az információs gazdaság helyzete a településen</i> .....	7
<i>Informatikai alkalmazási készségek, ismeretek</i> .....	7
3. A SZERVEZET INFORMATIKAI FEJLESZTÉSEI .....	8
4. NAGYVONALÚ SWOT ANALÍZIS .....	8
5. ÁTFOGÓ STRATÉGIAI CÉLJAINK .....	9
6. FEJLESZTÉSI PRIORITÁSOK .....	9
6.1. E-HIVATAL .....	10
<i>e-Ügyintézés (elektronikus ügyintézési szolgáltatások)</i> .....	11
<i>e-Ügyfélkezelés</i> .....	11
<i>Közigazgatási alkalmazások (belső ügyintézés)</i> .....	11
<i>Adminisztratív (kötségvetési) alkalmazások</i> .....	11
<i>Irodaautomatizálás, kommunikáció</i> .....	12
6.2. E-ÖNKORMÁNYZAT .....	12
<i>e-Önkormányzás, döntés-támogatás</i> .....	12
<i>Gazdaságélénkítés</i> .....	12
<i>Település-marketing</i> .....	12
<i>e-Hirdetés</i> .....	13
6.3. KULTÚRA RÉSZPROJEKT .....	13
<i>e-Galéria</i> .....	13
<i>e-Klub</i> .....	13
<i>e-Hírmondó</i> .....	13
6.4. OKTATÁS .....	13
6.5. SZÉLESSÁVÚ ÁTVITELI CSATORNA AZ INTERNETHEZ CSATLAKOZÁSHOZ.....	14
6.6. ESZKÖZEINK KORSZERŰSÍTÉSE.....	14
6.7. HOZZÁFÉRÉS A SZOLGÁLTATÁSOKHOZ .....	14
6.8. INFORMATIKAI TUDÁS, ALKALMAZÁSI KÉSZSÉG .....	14
6.9. INFORMÁCIÓBIZTONSÁG, ADATVÉDELEM.....	15
7. A MEGVALÓSÍTÁS ELVEI, ESZKÖZEI.....	15
8. KÖLTSÉGVETÉSI VONZAT (ELŐZETES PÉNZÜGYI TÁBLA), FINANSZÍROZÁSI FORRÁSOK, ÜTEMEZÉS .....	16
9. PARTNERI EGYÜTTMŰKÖDÉS.....	16
10. NYOMONKÖVETÉS, KORREKCIÓ .....	16
<b>III. ÁLTALÁNOS ADATVÉDELMI SZABÁLYOK</b> .....	<b>17</b>
1. AZ ÁLTALÁNOS ADATVÉDELMI SZABÁLYOK .....	17
2. AZ ADATKEZELÉS SORÁN HASZNÁLT FONTOSABB FOGALMAK .....	17
3. A KELETKEZETT ADATOK BESOROLÁSI RENDJE .....	19
4. ADATKEZELŐK FELADATAI, JOGOSULTSÁGAI.....	20
<b>IV. KÖZÉRDEKŰ ADATOK KEZELÉSE</b> .....	<b>22</b>
1. KÖZÉRDEKŰ ADATOK NYILVÁNOSSÁGA.....	22
2. A KÖZADATTÁRHOZ VALÓ CSATLAKOZÁS MÓDJA .....	23
3. A KÖZZÉTÉTELI ELJÁRÁS SZABÁLYAI.....	23
4. KÖZZÉTÉTELI LISTA .....	24
5. A KÖZÉRDEKŰ ADATOK MEGISMERÉSÉRE IRÁNYULÓ IGÉNY ÉS TELJESÍTÉSE.....	27
6. JOGORVOSLAT A KÖZÉRDEKŰ ADATOK TELJESÍTÉSÉVEL KAPCSOLATBAN.....	29
<b>V. ADATVÉDELMI SZABÁLYOK A POLGÁROK SZEMÉLYES ADATAIVAL KAPCSOLATOS FELADATOKRA ÉS ELJÁRÁSOK RENDJÉRE</b> .....	<b>30</b>
1. ÁLTALÁNOS RENDELKEZÉSEK.....	30
2. ÉRTELMEZŐ RENDELKEZÉSEK .....	30
3. SZEMÉLYES ADATOK VÉDELME .....	30
4. ADATSZOLGÁLTATÁS.....	31
5. ELLENŐRZÉS .....	32

<b>VI. INFORMATIKAI BIZTONSÁGI SZABÁLYZAT .....</b>	<b>32</b>
1. ALAPVETŐ ELEKTRONIKUS INFORMÁCIÓBIZTONSÁGI KÖVETELMÉNYEK.....	35
2. AZ ELEKTRONIKUS INFORMÁCIÓS RENDSZER BIZTONSÁGI OSZTÁLYBA SOROLÁSA. ....	35
3. AZ ELEKTRONIKUS INFORMÁCIÓS RENDSZER BIZTONSÁGÁÉRT FELELŐS SZEMÉLY FELADATAI.....	35
4. ADATOK ÉS PROGRAMOK VÉDELME .....	36
5. SZÁMÍTÓGÉPEK, ESZKÖZÖK ÉS DOKUMENTÁCIÓK VÉDELME .....	38
6. MÁGNESES ADATHORDOZÓK VÉDELME.....	38
7. AZ ADATHORDOZÓK SELEJTEZÉSE.....	39
8. NEMZETI ELEKTRONIKUS INFORMÁCIÓBIZTONSÁGI HATÓSÁG .....	39
<b>VII. KATASZTRÓFA-ELHÁRÍTÁSI SZABÁLYOK .....</b>	<b>40</b>
1. VÉSZHELYZETEK.....	40
2. TOVÁBBI KÁROK MEGELŐZÉSE.....	40
3. HASONLÓ ESETEK MEGELŐZÉSE .....	41
4. NORMÁL ÜZEM VISSZAÁLLÍTÁSA .....	41
5. A HIBA OKAINAK FELDERÍTÉSE .....	41
<b>VIII. VÍRUSVÉDELMI ELJÁRÁSOK .....</b>	<b>41</b>
1. VÍRUSVÉDELMI ELJÁRÁSOK.....	41
2. A VÍRUSVÉDELEM SZABÁLYAI A FELHASZNÁLÓ RÉSZÉRŐL .....	42
3. AZ ELEKTRONIKUS LEVELEZÉS VÍRUSVÉDELME .....	42
<b>IX. ELEKTRONIKUS CSATORNÁK HASZNÁLATA .....</b>	<b>43</b>
1. INTERNET ÉTIKAI KÓDEX.....	43
2. INTERNET HASZNÁLATA .....	43
3. E-MAIL HASZNÁLATA .....	43
4. MOBIL ESZKÖZÖK HASZNÁLATA .....	43
<b>X. ZÁRÓ RENDELKEZÉS .....</b>	<b>44</b>

Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény alapján a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992. évi LXVI. tv. 30. § (1) bekezdésében kapott felhatalmazás szerint, valamint az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény alapján a szervezet adatvédelmével és informatikai biztonságával összefüggő feladatait és eljárási rendjét a következők szerint szabályozom:

## I.

### SZABÁLYZAT CÉLJA, HATÁLYA

Az Informatikai Biztonsági Szabályzat egy olyan belső szervezeti intézkedés, amely a szervezeten belül működtetett informatikai rendszerekre vonatkozóan szabályozza az informatikai rendszerrel kapcsolatos biztonsági intézkedéseket, szervesen illeszkedve a szervezet egyéb működési és ügyrendi előírásaihoz. Az adatvédelem oldaláról megközelítve viszont jelen esetben csak az adatokkal, mint informatikai elemekkel foglalkozó rendszerek biztonságát kell megteremteni, amelyek természetüknél fogva számítástechnikai eszközök felhasználását is igénylik. A számítástechnikai eszközök az informatikai rendszer részei és hozzátartozik a környezeti infrastruktúra, a hardver, az adathordozók, a dokumentumok, a szoftverek, az adatok, a kommunikáció és a személyek elemcsoport valamennyi eleme.

Az Informatikai Biztonsági Szabályzatban olyan intézkedéseket kell tenni, amelyek ezen rendszerelemekre korlátozódnak és az előírások lehetővé teszik az informatikai rendszerre irányuló veszélyek, fenyegető tényezők hatásainak elviselhető mértékűre való csökkentését.

A szabályzat személyi hatálya kiterjed **a Dunaszegi Közös Önkormányzati Hivatal és a tagönkormányzatok** (a továbbiakban: szervezet) közszolgálati, közalkalmazott jogviszonyban álló vezetőire, ügyintézőire, valamint a munkajogviszony keretében foglalkoztatott munkavállalókra. Kiterjed továbbá azokra a személyekre, akik az önkormányzattól kapott megbízásuk alapján az Informatikai Biztonsági Szabályzat előírt rendelkezéseivel kapcsolatba kerülnek.

A szabályzat **tárgyi hatálya** kiterjed a szervezet 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 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 szervezet által használt felhasználói programokra és rendszerprogramokra,
- az informatikai rendszerben megjelenő valamennyi dokumentációra (fejlesztési, szervezési, programozási, üzemeltetési).

A szabályzat az informatikai rendszerrel kapcsolatos, stratégiai, biztonságos adatkezelési és adatvédelmi eljárásokat, katasztrófa elhárítási, vírusvédelmi, IT üzemeltetési, Internet használati feladatokat rögzít. A számítástechnikai eszközök beszerzésének és használatának, a

saját készítésű és vásárolt szoftverek alkalmazásának a folyamatát, továbbá egyes személyek informatikai biztonságot érintő feladatait ismerteti.

## II. INFORMATIKAI STRATÉGIA

A szervezet megfelelő szakmai működéséhez szükséges az informatikai támogatás színvonalának folyamatos növelése és a kínálkozó pályázati lehetőségek biztosítása érdekében szükséges az informatikai stratégia kidolgozása.

Az IT alkalmazása a szolgáltatások területén magában foglalja a költségek racionalizálását (mint az emberi munkaerő helyettesítése), hatékonyabb minőségellenőrzést és közvetlenebb kapcsolatot jelent az ügyféllel. Ráadásul abban is szerepet játszhat, hogy a kívánatos emberi magatartásformát és/vagy közreműködést kialakítsa a helyi demokrácia kibővítésével egyidőben.

Az Európai Unió felismerve annak lehetőségét, hogy a világ legmeghatározóbb régiója legyen (versenyképesség, fejlődés, tudás tekintetében), több akciótervet dolgozott ki (eEurope 2002, eEurope+, eEurope 2005) melyek mind az információs társadalomban látják a megvalósulás mozgatórugóját.

Az információs társadalom alapját képezik az elektronikus közszolgáltatások, elektronikus ügyintézesek. Az Európai Unió négy fejlettségi szintet határozott meg a szolgáltatásokkal kapcsolatosan a „Common List of Basic Public Services” (CLBPS) ajánlásában.

A Magyar Információs Társadalom Stratégia (MITS) szintén négy fejlettségi szintet határoz meg az elektronikus szolgáltatás területén:

- 1. szint- információ:** on-line információk nyújtása a közigazgatási szolgáltatásokról
- 2. szint-egyirányú interaktivitás:** az ügyintézéshez szükséges űrlapok, nyomtatványok letölthetők, kinyomtathatók
- 3. szint- kétirányú interaktivitás:** az ügyintézéshez szükséges űrlapok nyomtatványok, on-line kitölthetők, elektronikus aláírás segítségével hitelesíthetők, on-line továbbíthatóak
- 4. szint-elektronikus ügyintézés:** a teljes ügyintézés, ügymenet elektronikus: űrlap, nyomtatványok on-line kitöltése, hitelesítés, továbbítás, döntés, kézbesítés, illeték lerovása (elektronikus aláírás felhasználásával)

### 1. A jelenlegi informatikai helyzet bemutatása

A fejezet célja az informatika jelenlegi helyzetének bemutatása és elemzése, amely kiterjed az informatikailag támogatott folyamatokra, a szervezetre, a szabályozásokra, az eszközökre és az alkalmazásokra. Kiindulási pontot képeznek a külső és belső környezet által támasztott követelmények.

A környezetelemzés stratégiaalkotáshoz szükséges összetevői pontokba foglaltan (SWOT). A Swot megállapítása alapján határoztuk meg a követendő stratégiát.

Jelenleg a hivatali munka több területén használunk informatikai eszközöket, módszereket. A szervezeti egységek és a munkatársak az alábbi 1. táblázatban összefoglaltak szerint alkalmazzák azokat:

**1. sz. táblázat**

<i>Ssz</i>	<i>Szervezeti egység megnevezése</i>	<i>Önkormányzati, igazgatási, közszolgáltatási funkciói</i>	<i>Informatikai eszközöket használnak-e?</i>	<i>Célszoftvert használnak-e?</i>	<i>Internet kapcsolatuk van-e?</i>
	1	2	3	4	5
1.	Jegyző	Testületi ülések előkészítése, jegyzőkönyvezése	Igen	Nem	Igen
2.	Adóügyi előadó	Helyi adók és gépjárműadó kivetése, nyilvántartása	Igen	Igen	Igen
3.	Igazgatási előadók	Általános- és szakigazgatási ügyek Népesség nyilvántartás	Igen	Igen	Igen
4.	Pénzügyi-gazdálkodási előadók	Vagyonkezelés és nyilvántartás, beruházások előkészítése, lebonyolítása	Igen	Igen	Igen
5.	Pénzügyi-gazdálkodási előadók	Költségvetési tervezés, beszámolás, gazdálkodás	Igen	Igen	Igen
6.	Ügyiratkezelés	Iktatás	Igen	Igen	Igen

Annak ellenére, hogy az új információk előállításához, kezeléséhez egyre több területen informatikai eszközöket és módszereket alkalmazunk, az információgyűjtés, az információnyújtás, a tájékoztatás és az elektronizált ügyintézés területein mégis van lemaradásunk.

Településeink rendelkeznek honlappal, amelyeknek elérhetősége:

[www.dunaszeg.hu](http://www.dunaszeg.hu)

[www.dunaszentpal.hu](http://www.dunaszentpal.hu)

[www.kunsziget.hu](http://www.kunsziget.hu)

A szervezet munkatársainak informatikai eszközhasználati az irodai, illetve adminisztratív alkalmazások területén, valamint a kommunikáció és a közigazgatási alkalmazások területén jó.

## **2. Informatikai infrastruktúra**

### *A szervezet informatikai ellátottsága*

A hardverállományunk és eszközeink fejlettségi szintje jó. A számítógépes munkahelyek hálózatba vannak kapcsolva. Az Internethez való csatlakozást 5000 kbps sávszélességű ADSL átviteli csatornák biztosítják.

Szervezetünk a hivatali munka segítéséhez általános célú programokat (irodai programcsomagokat) és célszoftvereket használ. A célszoftverek egy részét térítésmentesen kaptuk a MÁK-tól. A rendszerprogramok és az irodai programcsomagok, a behatolás elleni és vírusvédelmi programok licencét megvásároltuk.

### *A település és a lakosság informatikai ellátottsága*

Mivel településünkön még nem végeztünk a lakosság informatikai eszközökkel ellátottságára, felhasználói, alkalmazói kultúrájára vonatkozó felmérést, ezért a fejlesztési célok meghatározásához az országos helyzetértékelést vesszük alapul.

Magyarországon 2010-ben a háztartások 65% rendelkezett számítógéppel és 40%-a internet-hozzáféréssel (a kistelepüléseken mindkét mutató jóval kisebb volt). Ezen belül további „digitális törésvonalak” rajzolódtak ki. A különbségeket létrehozó jellemzőbb mutatók a gazdasági aktivitás, az életkor, az iskolai végzettség, a jövedelem nagysága, a településtípus különbségei.

### *Az információs gazdaság helyzete a településen*

A településeken bejegyzett vállalkozások közül több nagyvállalat, valamint néhány vendéglátóhely és falusi szállásadó rendelkezik saját honlappal.

### *Informatikai alkalmazási készségek, ismeretek*

A szervezet munkatársainak informatikai eszközhasználatát az irodai, illetve adminisztratív alkalmazások és a kommunikációs és a közigazgatási alkalmazások tekintetében jó.

A 2. sz. táblázat a szervezet munkatársainak informatikai eszközhasználatát mutatja be.

**2. sz. táblázat**

Beosztás	Státusz	Létszám [fő]	Ebből informatikai eszközt használ		
			Kommunikációhoz	Irodai, adminisztratív munkához	Közigazgatási munkához
Jegyző	Köztisztviselő	1	Igen	Igen	Igen
Polgármester	Választott tisztviselő	3	Igen	Igen	Igen
Pénzügyi-gazdálkodási előadó	Köztisztviselő	4	Igen	Igen	Igen
Adóügyi előadó	Köztisztviselő	1	Igen	Igen	Igen
Igazgatás előadó	Köztisztviselő	3	Igen	Igen	Igen
Általános önkormányzati előadó	Köztisztviselő	1	Igen	Igen	Igen
Ügykezelő	Köztisztviselő	1	Igen	Igen	Igen

A Közös Önkormányzati Hivatal dolgozóinak informatikai végzettségét a 3. sz. táblázat mutatja.

**3. sz. táblázat**

	Döntéshozók, tisztségviselők	Ügykezelők, ügyintézők	Rendszergazda (üzemeltetők)
Nincs semmilyen informatikai előképzettsége	-	-	A szervezet jelenleg nem foglalkoztat informatikust. A rendszergazdai feladatokat külső
Tanfolyamot végzett (tanúsítvány)		-	
ECDL vizsgával rendelkezik		8 fő	

OKJ képe­si­tést szerzett (középfokú)		1 fő	szol­gáltató látja el.
Felsőfokú végzettséggel rendelkezik, amelynek részét képezte informatikai oktatás		2 fő	

A munkatársak informatikai felkészültsége jó, továbbképzésük új programok használatba vétele során szükséges.

### 3. A Szervezet informatikai fejlesztései

A szervezet évente a költségvetésben rendelkezésre álló pénzüsszeget fordít az informatikai eszközök fejlesztésére, üzemeltetésére. Az informatikai fejlesztések biztosítására pályázati támogatások bevonása is szükségessé válhat.

### 4. Nagyvonalú SWOT analízis

A SWOT analízis belső, „erősségeinket” és „gyengeségeinket”, azaz szervezetünk maga által befolyásolható informatikai jellemzőit, és a külső környezet állapotát foglalja összefoglaló keretbe. Az erősségek hatékony kihasználása és a gyengeségek kiküszöbölése, a stratégiában megfogalmazott intézkedések alapján biztosítható.

Belső tényezők – Erősségek	Belső tényezők - Gyengeségek
<u>Emberi erőforrások</u> <ul style="list-style-type: none"> <li>az alkalmazottak mindegyike munkája során számítógépet használ</li> <li>informatikai eszközök alkalmazása az irodai, adminisztratív munkára</li> <li>fokozott továbbképzési igény</li> <li>a testület elkötelezettsége az informatikai fejlesztések mellett</li> </ul>	<u>Emberi erőforrások</u> <ul style="list-style-type: none"> <li>a lakosság számítógép és internet-használatának alacsony aránya.</li> </ul>
<u>Infrastruktúra</u> <ul style="list-style-type: none"> <li>belső hálózattal rendelkezünk</li> <li>az internet-hozzáférés mindenki számára biztosított a szervezetnél</li> <li>rendelkezünk önkormányzati honlappal</li> <li>megfelelő adatbiztonság</li> </ul>	<u>Infrastruktúra</u> <ul style="list-style-type: none"> <li>az informatikai eszközök nagyrészt elfogadhatók, mintegy 20%-a azonban nem korszerű</li> </ul>
Külső tényezők – Lehetőségek	Külső tényezők - Veszélyek
<ul style="list-style-type: none"> <li>Európai Unió és hazai pályázatok.</li> <li>Alkalmazás Szolgáltató Központ (ASP) létrehozása</li> <li>a közigazgatási szervektől, illetve hivataloktól ingyenesen beszerezhető célszoftverek</li> <li>külső fejlesztő cégek bevonása, elkötelezettségük a fejlesztés mellett</li> <li>a térség szereplőiben tudatosultak az információk kor követelményei és az általa kínált lehetőségek</li> <li>hazai és nemzetközi települések és térségek közötti együttműködés</li> <li>az oktatás révén a felnövekvő generáció számára a digitális írástudás az írás-olvasáshoz hasonló készséggé válik</li> <li>a számítógép- és internet-használat társadalmításához korlátozottan ugyan, de rendelkezésre áll az eszközállomány.</li> <li>nyilvános internet-hozzáférési pontok a kistérség több településén kiépültek</li> <li>aktív civil élet</li> <li>az intézményi ellátottság térségi koordinációjának megvalósítása megkezdődött</li> <li>országos és nemzetközi szinten elismert</li> </ul>	<ul style="list-style-type: none"> <li>a lakosság számítógéppel való ellátottsága nem teljes körű</li> <li>az informatikai alkalmazások terén digitális szakadék</li> <li>az átviteli csatornák kiépítésének elhúzódása, drága igénybevétele</li> <li>alacsony szintű digitális írástudás</li> <li>alacsony a lakossági internet-használat aránya</li> <li>lakossági viszonylatban alacsony a szélessávú adatátviteli technológia térhódítása</li> <li>az ellátottsághoz viszonyítva az internet kínálta lehetőségek alulhasznosítottak</li> <li>az internetes tartalmak többsége nem használja ki az interaktivitási, kommunikációs lehetőségeket</li> <li>alacsony szintű a magasabb színvonalú internetes szolgáltatások igénybevétele</li> <li>a költségkímélő megoldások elterjedése csekély</li> <li>társadalmi és humán erőforrás problémák: előregedő korstruktúra</li> <li>gazdasági válság: munkanélküliség, alacsony vállalkozói aktivitás</li> <li>nem kellően rugalmas képzési rendszer</li> <li>az új technológia iránt érzéketlen csoportok</li> </ul>



<ul style="list-style-type: none"> <li>tájspecifikus mezőgazdasági termékek kedvező környezetállapot</li> </ul>	<ul style="list-style-type: none"> <li>munkavállalási esélyeinek romlása</li> <li>az e-gazdaság lassú fejlődésével késve jelennek meg a várt eredmények (foglalkoztatottság növekedése, távmunka stb.)</li> <li>a magas előfizetési díjak továbbra sem kedveznek az otthoni internet-használat növekedésének</li> </ul>
-----------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

## 5. Átfogó stratégiai céljaink

A Magyar Információs Társadalom Stratégiához kapcsolódó fő célunk:

- Az önkormányzati honlap tartalmának továbbfejlesztése
- A szervezet feladatához igazodva a kapcsolattartás és döntés előkészítési feladatok hatékonyságának növelése a belső informatikai rendszerek fejlesztésével
- A település és a helyi vállalkozások gazdasági versenyképességének növelése
- Segíteni a közigazgatás átalakulását e-közigazgatássá, amellyel hozzájárul a helyi és kistérségi politika és társadalmi e-demokrácia létrejöttéhez, ideértve a helyi e-népszavazás feltételeinek megteremtését.

A stratégiai célok elérését biztosító fejlesztési elvek

A döntés-előkészítési folyamatok korszerűsítése, hatékonyságának javítása információs és kommunikációs technológiák alkalmazásával.

A korszerűsítés elsősorban a belső folyamatok elemzését, szükség szerinti ésszerűsítését, újratervezését, újraszervezését jelenti, amelynek során minden olyan részfolyamatban, ahol az a hatékonyságot, illetve a gazdaságosságot növelni szükséges, infokommunikációs technológia eszközök alkalmazására törekszünk.

Szolgáltatásainkat modernizáljuk az info-kommunikációs technológiák alkalmazásával. Igyekszünk az elektronikus szolgáltatások minél magasabb fejlettségi szintjének elérésére (on-line információ elérés).

## 6. Fejlesztési prioritások

Fejlesztési tárgy- és témakörök	A fejlesztés célterülete
Elektronikus tartalmak és szolgáltatások	Döntés-előkészítés, helyi gazdaság, kultúra, oktatás, informálódás
Infrastruktúra	Szélessávú átviteli csatorna, internet-hozzáférés, új eszközök, meglévő eszközök műszaki korszerűsítése, biztonság
Informatikai tudás, alkalmazási készség	Képzés, továbbképzés, alkalmazói készségek fejlesztése
Befogadó környezet	Minőségfejlesztés, esélyegyenlőség biztosítás

A szervezet tárgy- és témakörök szerint csoportosított stratégiai célok megvalósítása érdekében a következő középtávú fejlesztési tervet (fejlesztési projekteket) határozza meg, amelyeket 2014. március 15. és 2017. december 31. között pályázati források bevonásával szeretne teljesíteni.

Prioritások	I. Elektronikus tartalmak és szolgáltatások	II. Infrastruktúra	III. Informatikai tudás, alkalmazási készség	IV. Befogadó környezet
Részstratégiák részprojektek	<b>e-Hivatal</b>	<b>Szélessávú internet kapcsolat</b>	<b>Szolgáltatói oldal</b>	<b>Információ biztonság, minőség</b>
	e-ügyintézés, e-ügyfélkezelés, közigazgatási alkalmazások, adminisztratív alkalmazások, odaautomatizálás, kommunikáció	szélessávú átviteli csatornák kiépítése, a csatlakozási pontos számának növelése	döntéshozók felkészítése, ügyintézők továbbképzése, informatikusok képzése	technológiai biztonság, eljárásrendek kidolgozása (adatvédelmi szabályzat), informatikai minőségirányítási rendszer
	<b>e-Önkormányzat</b>	<b>Eszközök korszerűsítése</b>	<b>Felhasználói oldal</b>	
	e-önkormányzás, vezetői döntéstámogatás, közhasznú információk	hardver-, szoftver környezet, jogtisztaság	közösségi oktatás, információs (PR) anyagok terjesztése	
	<b>Gazdaság</b>	<b>Hozzáférés</b>		
	településmarketing, turizmus,	helyi információs pontok, közösségi hozzáférés,		
	<b>Kultúra</b>	eszközbeszerzés segítése		
<b>Oktatás</b>				
	e-múzeum, e-könyvtár, e-galéria, klub, e-mondó			
	intézményi információk, adminisztratív tevékenységek			

## 6.1. e-Hivatal

Célkitűzésünk az elektronikus hivatal és szolgáltatási feltételek megteremtése, az ügyintézés korszerűsítése. A következő táblázat az e-Hivatal projektünk megvalósításához szükséges intézkedési területeket foglalja össze.

<b>e- Ügyintézés</b>	On-line információk a közigazgatási szolgáltatásokról (ügyleírások)	Nyomtatványok, űrlapok letöltése (az ügyintézéshez)	Nyomtatványok, űrlapok on-line kitöltése, hitelesítése, továbbítása	Teljes elektronizált ügyintézés, (döntés, kézbesítés, illeték stb.)	Függőben lévő ügyek elektronikus követése
<b>e- Ügyfélkezelés</b>	Egyirányú kommunikáció webes felületen				
<b>Közigazgatási alkalmazások</b>	Adók és egyéb bevételek	Vagyonkezelés, vagyongazdálkodás	Település-fejlesztés, beruházások	Településüzemeltetése	
	Ipari, kereskedelmi igazgatási feladatok	Művelődési, oktatási, sport feladatok	Szociális- és egészség- ügyek	Egyéb önkormányzati feladatok	
		Anyakönyvi hivatali feladatok		Egyéb területi igazgatási feladatok	
<b>Adminisztratív alkalmazások</b>	Számvitel, pénzügy, kontrolling	Humánpolitika, humánerőforrás-gazdálkodás,	Anyag-, tárgyeszköz-gazdálkodás,	Projektek és programok (beruházások, fejlesztések)	Elektronikus iktatás, ügyirat-dokumentum-, munkafolyamat – kezelés
<b>Iroda-automatizálás, kommunikáció</b>	Szövegszerkesztés, dokumentáció-készítés,	Táblázatos és grafikus kimutatás-készítés,	Elektronikus levelezés (belső, külső),	Prezentáció-készítés	Feladatkezelés, -ütemezés, stb.

### *e-Ügyintézés (elektronikus ügyintézési szolgáltatások)*

A („Common List of Basic Public Services”) Európai Unió ajánlás alapján önkormányzatunk következő szolgáltatásait kívánja az interneten elérhetővé tenni:

- a helyi polgárok és más jogosultak számára: a hatósági igazolásokkal (születési, házassági, halálozási anyakönyvi kivonatok), a lakcímváltozás bejelentésével, a gépjármű-regisztrációval, a súlyadó-fizetéssel, a szociális juttatásokkal, támogatás fizetésével, helyi adózással kapcsolatos ügyintézés;
- az üzleti szféra szereplőinek: a gépjárműadó, engedélyek (pl. telepengedély, működési engedély) kiadás ügyintézését.

A szolgáltatásokat az alábbiak szinteknek megfelelően kívánjuk biztosítani:

1. szint: on-line információk a közigazgatási szolgáltatásokról (ügyleírások, ügyfélfogadási idő, elérhetőségek)
2. szint: nyomtatványok, űrlapok letöltése (az ügyintézéshez)
3. szint: nyomtatványok, űrlapok on-line kitöltése, hagyományos hitelesítése, továbbítása
4. szint: teljes elektronizált ügyintézés (digitális hitelesítés, továbbítás, döntés)

Közigazgatási szolgáltatásaink további támogatására létrehozunk egy, a függőben lévő ügyek elektronikus követésére szolgáló rendszert.

### *e-Ügyfélkezelés*

Célunk, egy olyan, az ügyfélszolgálati tevékenységet támogató rendszer kialakítása, amely hatékonyabbá, kényelmesebbé és egyszerűbbé teszi az ügyintézését, mind a lakosság, mind pedig ügyintéző munkatársaink részére. Ezt három szinten kívánjuk megvalósítani:

1. szint: elektronikus levélben történő kérdésfeltevés, segítségkérés
2. szint: bejelentkezett, illetve auditált ügyfelek számára (azonosító és jelszó használatával) kétirányú kommunikációt lehetővé tevő, web alapú ügyfélszolgálat (Customer Relationship Management – CRM)
3. szint: az ügyfelek az információs portálon keresztül érdeklődhetnek az éppen folyamatban lévő ügyeikről

### *Közigazgatási alkalmazások (belső ügyintézés)*

Folyamatosan beszerezzük, alkalmazzuk és ha kell, frissítjük a szükséges célszoftvereket. Adók és egyéb bevételek; Vagyongazdálkodás, vagyongazdálkodás; Település-fejlesztés, beruházások; Településüzemeltetés; Ipari, kereskedelmi igazgatási feladatok; Művelődési, oktatási, sport feladatok; Szociális- és egészségügy; Gyámügyi feladatok; Anyakönyvi hivatali feladatok; népesség nyilvántartás, munkaügy.

### *Adminisztratív (költésgvetési) alkalmazások*

Meg kívánjuk oldani az adminisztratív tevékenységek elektronizálását és az adatok digitalizálását. Számvitel, pénzügy, kontrolling; Humánpolitika, humán erőforrás-gazdálkodás; Anyag-, tárgyszerkezet-gazdálkodás; Projektek és programok (beruházások, fejlesztések) szervezése; Elektronikus iktatás, ügyirat-, dokumentum-, munkafolyamat – kezelés; Jogszabályi információk szolgáltatása (jogtárak).

### *Iroda-automatizálás, kommunikáció*

Alapvető elvárásként fogalmazzuk meg, hogy a hivatalnál keletkező adatok, dokumentumok, táblázatok, kimutatások, prezentációk elektronikus formában keletkezzenek. Ezen cél elérésének érdekében munkatársaink számára kötelezően előírjuk a szövegszerkesztésre, kiadványszerkesztésre, táblázatkezelésre, grafikus kimutatások és prezentációk készítésére alkalmas programok használatát.

Munkatársaink egymás közötti és az ügyfelekkel kapcsolatos kommunikációjának megkönnyítésére elektronikus levelező rendszert hozunk létre.

Önkormányzatunk telekommunikációs költségeinek csökkentése érdekében folyamatosan áttérünk a beszédet és a faxot az internet csatornáján továbbító VoIP technológia alkalmazására.

## **6.2. e-önkormányzat**

### *Közérdekű, közhasznú információk*

A lakosság tájékoztatására információs portált hozunk létre, amelyen megjeleníthetők a közérdekű információk. Hozzáférhető lesz a képviselő testület elérhetősége, fogadóóráik, a testületi ülések időpontja, napirendje, a testület felépítése, a polgármester, a tisztségviselők, a képviselők bemutatkozása, tevékenységeik ismertetése, a bizottságok munkájának leírása. Közzé tesszük az előterjesztéseket, határozatokat, rendeleteket, pályázati lehetőségeket. Szerepeltetjük a közszolgáltatókról és a közintézményekről a legfontosabb információkat. Virtuális lakossági – fórumokat rendezünk, és elektronikus önkormányzati hírlevelet teszünk közzé, illetve terjesztünk.

### *e-Önkormányzás, döntés-támogatás*

A képviselő-testület hatékonyságának növelését első lépésben a képviselők online kapcsolathoz jutásának segítségével, az önkormányzati levelezőrendszer használatával, illetve csoportmunka-szoftverek alkalmazásával kívánjuk elérni.

Második lépésben létre kívánunk hozni egy, az önkormányzat rendeletalkotási és határozathozatali feladatainak követésére és támogatására szolgáló adatbázist, amelynek segítségével követhetik a közgyűlési folyamatokat (az elsődlegesen megfogalmazott előterjesztésektől, a szakmai és jogi értékelésen, a bizottsági tárgyalásokon és véleményalkotáson át, egészen a döntéshozatalig).

A települést érintő fontos kérdésekkel kapcsolatos lakossági vélemények megismerésére elektronikus közvélemény-kutató rendszert alakítunk ki.

### *Gazdaságélénkítés*

Célkitűzés: a helyi vállalkozások gazdasági versenyképességének és piaci lehetőségeinek növelése.

### *Település-marketing*

A fenti cél elérése érdekében településünk portálrendszerén gazdasági modult kívánunk kialakítani településfejlesztés, turizmus és helyi vállalkozások témákkal.

Itt is ismertetjük településünk fejlesztési koncepcióját, ipari-, mezőgazdasági létesítményeit, közzé tesszük a település gazdasági statisztikáit és mutatóit, a közbeszerzési és pályázati kiírásokat, az új vállalkozásoknak nyújtandó kedvezményeket, a befektetési lehetőségeket.

A turizmus témakörben bemutatjuk településünket és környékét, megközelítési lehetőségeket, a főbb természeti és kulturális látnivalókat és érdekességeket, valamint szerepeltetjük a település által ajánlott szálláshelyeket, éttermeket, szabadidős- és sporttevékenységeket.

#### *e-Hirdetés*

A modul létrehozásával az állampolgárok közötti kommunikációt, illetve gazdasági tevékenységet kívánjuk elősegíteni.

### **6.3 Kultúra részprojekt**

Célkitűzés: a település kultúrájának megőrzése, a társadalom minél szélesebb körében terjesztése, valamint a kulturális élet minőségének javítása.

<b><i>e-Galéria</i></b>	helyi lakosok művészi alkotásainak közzététele (kézimunka, fafaragás, népművészet)	virtuális kiállítások amatőr művészek munkáiból
<b><i>e-Klub</i></b>	helyi kulturális csoportok bemutatása	internetes klubrendszer
<b><i>e-Hírmondó</i></b>	hasznos információk közzététele	kulturális vitafórumok, szavazások helyi újság elektronikus változata

Kulturális értékeink megőrzése érdekében digitalizáljuk, majd katalogizáljuk a helyi írott, nyomtatott, rajzolt, festett, fotózott dokumentumokat. Az így számba vett értékeket összehangoljuk az országos adatbázisokkal.

#### *e-Galéria*

A településen élők napi alkotásait mutatjuk be virtuális kiállítás keretében. Helyi népművészek, művészek és más alkotók munkáit, a kortárs képző- és iparművészet, zeneművészet, irodalom darabjait és gyermekműveket teszünk közzé. Biztosítanánk, hogy bizonyos feltételek vállalása mellett bármely lakos létrehozza saját elektronikus galériáját.

#### *e-Klub*

A helyi kulturális közösségek (egyesületek, szakkörök, klubok, csoportok) életét és tevékenységét mutatjuk be (pl.: bélyeggyűjtő szakkör, fotószakkör, helyi zenekar, színészcsoport, táncklub, nyugdíjas klub, irodalmi kör). Helyi internetes klubrendszert alakítunk ki.

#### *e-Hírmondó*

Közzétesszük a településünk kulturális életével kapcsolatos hasznos információkat és az aktuális programajánlatokat, tudósítunk környezetünk főbb kulturális eseményeiről, valamint vitafórumokat és közvélemény-kutatásokat szervezünk. Mindenki számára elérhetővé tesszük a helyi újság aktuális és archív számait.

### **6.4 Oktatás**

Célkitűzés: az oktatási-, nevelési intézmények bekapcsolása a helyi információs társadalom vérkeringésébe. Az oktatással kapcsolatos adminisztratív tevékenységek támogatása.

<b><i>Intézményi információk</i></b>	Szülői tájékoztatás	Alapvető dokumentumok közzététele	Oktatási segédanyagok
--------------------------------------	---------------------	-----------------------------------	-----------------------

Lehetőséget adunk a helyi oktatási-, nevelési intézmények bemutatására. Tájékozódhatnak a szülők gyermekeik programjairól (e-Faliújság). Az alapító okirat, a pedagógiai program, az intézményi minőségirányítási program, statisztikák közzététele, a nevelőtestület bemutatása.

### **6.5 Szélessávú átviteli csatorna az internethez csatlakozáshoz**

Célkitűzés: A települést lefedő, nagy sebességű internet-hozzáférés minél szélesebb körben elérhető legyen a község területén működő civil szervezetek és a lakosság számára.

### **6.6 Eszközeink korszerűsítése**

Célkitűzés: az informatikai koncepcióban felsorolt részprojektek megvalósításához szükséges hardver- és szoftverkörnyezet korszerűsítése.

Célkitűzéseink megvalósításához olyan nyílt szabványú adatcsere-technológiát biztosító számítógépes hálózat, illetve információtechnológia kialakítására van szükség, amelyet a szerverrendszer kialakításán túl hardver- és szoftverfejlesztéssel, illetve a meglévő eszközök teljesítményének növelésével alkalmassá tehetünk az új kliensoldali technológiák befogadására.

Olyan rendszer bevezetését tervezzük, mely képes ellátni a következő feladatokat: számítógépes hálózatvezérlés, címtárszolgáltatás, különböző információs, levelező és védelmi szerverfeladatok ellátása, kétirányú kapcsolat biztosítása az internettel, internetes portál működtetése, irodai-információtechnológiák működtetése, dinamikus űrlapok kialakítása, közzététele, adatainak összegyűjtése egy portálra, csoportmunka koordinálása, megjelenítése a weboldalon (illetve a portálokon), kommunikációs szolgáltatások.

E részprojekt keretében kívánjuk megoldani az adatok biztonságos kezelésének technológiai kérdéseit is. Ide értve egyfelől az adatbázis sérülés elleni védelmét (vírusvédelem, fizikai megsemmisüléssel szembeni védekezés), a rendszer állapotaiban illetve az adatbázisban végrehajtott módosítások mindenkor nyomon követhetőségét, a jogosulatlan hozzáférések kiküszöbölését (tűzfalvédelem).

### **6.7 Hozzáférés a szolgáltatásokhoz**

Célkitűzés: A számítástechnikai rendszerek és szolgáltatások széleskörű elérésének elősegítése az egyéni hozzáférés megvalósulását akadályozó tényezők lebontása valamint a közösségi hozzáférés formáinak fejlesztése útján.

Felhívjuk a lakosság figyelmét a számítástechnikai eszközök beszerzésénél igénybe vehető kedvezményekre, pályázati lehetőségekre.

### **6.8 Informatikai tudás, alkalmazási készség**

Célkitűzés: A döntéshozók és az ügykezelők felkészítése az elektronikus önkormányzat szolgáltatásrendszerének kialakítására és működtetésére, illetve az információk megszerzéséhez és a szolgáltatások igénybevételéhez szükséges ismeretek elterjesztése a lakosság minél szélesebb körében.

Elkötelezettek vagyunk az informatikai tudás és ismeret megszerzésében, fejlesztésében, terjesztésében. Meg kívánjuk oldani a döntéshozók informatikai felkészítését oly módon,

hogy megfelelő ismeretekkel rendelkezzenek az informatikai fejlesztésekkel kapcsolatos kérdésekben, globális rálátásuk legyen a településen végbenő fejlesztési folyamatokra.

A lakosság ismereteinek bővítését nyíltnapok és közösségi oktatás szervezésével kívánjuk támogatni. Az elsősorban az önkormányzati tartalmak és szolgáltatások gyakorlati felhasználásának bemutatására koncentrált közösségi oktatást, a lakossághoz eljuttatott, az új lehetőségeket bemutató információs-, illetve PR anyagokkal is ki kívánjuk egészíteni.

## **6.9 Információbiztonság, adatvédelem**

**Célkitűzés:** Fogyasztói bizalom növelése, beleértve annak biztosítását, hogy a felhasználók biztonságban érezzék magukat, mind a saját és idegen információk kezelését, mind a szolgáltatások megbízható működésének garanciáit illetően.

E cél teljesülése érdekében önkormányzatunk fokozatosan bevezeti a technológiai eszközök és megoldások által nyújtott lehetőségeket (vírusvédelem, tűzfal, digitális aláírás, intelligens kártya), másrészt informatikai minőségirányítási és biztonsági (adatvédelmi) szabályzatot dolgoz ki az elektronikus szolgáltatásokkal kapcsolatos folyamatok és eljárások rendszerére vonatkozóan.

## **7. A megvalósítás elvei, eszközei**

A stratégiai cél elérését szolgáló fejlesztési projektek tervezésekor és megvalósításakor a következő alapelveket tartjuk szem előtt.

Programozás, melyen a stratégiai alapokról induló konkrét tervezést és az intézkedések projektszemléletű kidolgozását értjük. A programok együttesen fedjék le a stratégiát, együttes megvalósulásuk biztosítsa a stratégiai célok elérését. Az ilyen fejlesztési programok rendelkezésre állása az Európa Unió és a nemzeti források sikeres megpályázásának általános feltétele. A stratégiai tervben kifejtett intézkedések így a hazai és uniós támogatások elnyerésének eszközei lesznek.

Közös érdekek: Alapvetően olyan intézkedésekre van szükség, amelyek a kívánt célok elérését piaci alapon teszik lehetővé (pl. információs gazdaság). Az önkormányzati szerepvállalás viszont indokolt annak érdekében, hogy a folyamatok olyan területeken is lejátszódjanak, ahol ezt a tisztán piaci működés nem biztosítaná, s ahol az önkormányzati példamutatás olyan intenzitású folyamatot indít el, amely jelentősen erősíti a piac kialakulását, illetve a működését.

Fenntarthatóság: A programok működési modelljével szembeni követelményünk, hogy az a folyamatos, hosszú távú működést támogassa az egyszeri megoldások helyett (mind a technológiai, mind a gazdasági, mind a humán erőforrás tekintetében). Az informatikai koncepciónk - az információs technológiák gyors fejlődéséből és a társadalmi igények állandó változásából adódó - elavulását pedig a stratégiánk folyamatos korszerűsítésével kívánjuk elkerülni. Ez egyrészt gazdasági, technológiai és statisztikai helyzetelemzések segítségével érjük el, másrészt a rövid távú programokat a gördülő tervezés módszerével aktualizáljuk.

Esélyegyenlőség elősegítése: Szervezetünk az infokommunikációs eszközökhöz és szolgáltatásokhoz való hozzáférést, illetve a lakosság ismereteinek bővítését célzó programok kidolgozása során különösen nagy figyelmet kíván fordítani társadalmi különbségekből és a területi egyenlőtlenségekből adódó problémák csökkentésére. Különös tekintettel a hátrányos helyzetű társadalmi csoportokat (fogyatékkal élők, szociális problémákkal küzdő

kisebbségek, idősek) érintő kirekesztettségre, korlátozottságra és diszkriminációra, ezáltal is segítve a társadalomba való integrálódásukat.

## 8. Költségvetési vonzat (előzetes pénzügyi tábla), finanszírozási források, ütemezés

Miután forrásaink nem elegendőek fejlesztési célkitűzéseink megvalósításához, e stratégia csak a fejlesztési irányok meghatározását vázolja. A megvalósítás függ az időközben megszerzett pályázati támogatásoktól, illetve döntően azokra alapoz.

Az egyes projekteket a pályázati önrész mértékéig támogatjuk. Az alábbi táblázatban X jelöli a projektek ütemezését:

Projektek megnevezése	2014	2015	2016	2017
	A projektek tervezett időpontjai			
<b>I. Elektronikus tartalmak és szolgáltatások fejlesztése</b>				
e-Hivatal fejlesztése				X
e-Önkormányzat fejlesztése				X
Gazdasági szolgáltatások fejlesztése			X	X
Kulturális tartalmak fejlesztése				X
<b>II. Infrastruktúra fejlesztése</b>				
Szélessávú infrastruktúra fejlesztése	X	X		
Informatikai eszközök modernizációja	X		X	X
Közösségi hozzáférés biztosítása, támogatása		X	X	
<b>III. Informatikai tudás, ismeret fejlesztése</b>				
Szolgáltatói oldal (döntéshozók felkészítése, ügyintézők, informatikusok továbbképzése)	X	X		
Felhasználói oldal (lakossági felkészítés)		X	X	X
<b>IV. Társadalmi környezet</b>				
Információ biztonság és minőség fejlesztése		X	X	
<i>Támogatott fejlesztési területek (összesen)[db]</i>	3	5	5	6

## 9. Partneri együttműködés

A jelen fejlesztési stratégia megvalósítása csak a koncepcióban érintettek partnerek együttműködésén alapulhat.

Az együttműködés kialakítását már a tervezés és előkészítés korai fázisában megkezdjük. A folyamatos egyeztetés és érdekarmonizáció mellett a megvalósítási valamint az ellenőrzési és értékelési folyamatokba is bevonjuk partnereinket.

Kezdeményezzük egy, az informatikai stratégiánk megvalósítását támogató civil csoport létrehozását, amelyben képviselteti magát az önkormányzatunk, intézményeink vezetése, a településhez kötődő valamennyi civil szervezet, a helyi gazdasági társaságok tulajdonosai, vezetői, valamint a csoport munkáját segítő informatikus szakemberek.

Célunk továbbá szoros partneri együttműködést folytatni kistérségünk más településeivel, így biztosítva kialakítandó informatikai rendszereink kompatibilitását.

## 10. Nyomon követés, korrekció

Középtávú informatikai fejlesztési koncepciónk megvalósulását évenként értékeljük, a tervet szükség szerint módosítjuk, korrigáljuk.



### III.

## ÁLTALÁNOS ADATVÉDELMI SZABÁLYOK

### 1. Az általános adatvédelmi szabályok

A személyes adatok védelméért, az adatkezelés jogszerűségéért a jegyző a 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 (közszolgálati alapnyilvántartás, illetve tartalékállomány és üres álláshely vezetése) adatvédelmére a Közszolgálati 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 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 munkavállalók 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.

**Adatállomány:** az egy nyilvántartásban kezelt adatok összessége.

**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 tenyérynymat, DNS-minta, íriszkép) rögzítése.

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

**Adattovábbítás:** ha az adatot meghatározott harmadik személy számára hozzáférhetővé teszik.

**Adathordozó:** adathordozónak nevezzük az informatikai rendszertől elválasztható adattároló eszközöket.

**Adatfelelős:** az a közfeladatot ellátó szerv, amely az elektronikus úton kötelezően közzeendő 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.

**Adatmegjelölés:** az adat azonosító jelzéssel ellátása annak megkülönböztetése céljából.

**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.

**Adatközlő:** az a közfeladatot ellátó szerv, amely - ha az adatfelelős nem maga teszi közzé az adatot - az adatfelelős által hozzá eljuttatott adatait honlapon közzéteszi.

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

**Érintett:** bármely meghatározott, személyes adat alapján azonosított vagy - közvetlenül vagy közvetve - azonosítható természetes személy.

**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-képviselési szervezeti tagságra, a szexuális életre vonatkozó személyes adat.

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

**Bűnügyi személyes adat:** a büntetőeljárás során vagy azt megelőzően a bűncselekménnyel vagy a büntetőeljárással összefüggésben, a büntetőeljárás lefolytatására, illetve a bűncselekmények felderítésére jogosult szerveknél, továbbá a büntetés-végrehajtás

szervezeténél keletkezett, az érintettel kapcsolatba hozható, valamint a büntetett előéletre vonatkozó 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.

**Tiltakozás:** az érintett nyilatkozata, amellyel személyes adatainak kezelését kifogásolja, és az adatkezelés megszüntetését, illetve a kezelt adatok törlését kéri.

**Nyilvánosságra hozatal:** az adat bárki számára történő hozzáférhetővé tétele.

### 3. A keletkezett adatok besorolási rendje

A szervezetnél az informatikai biztonsággal összefüggésben az adatok besorolási rendje a következő képen kerül meghatározásra:

- **Bizalmasság:** az információt csak az legyen képes elolvasni, aki arra jogosult.
- **Sértetlenség:** az információt csak az módosíthassa vagy törölhesse, aki arra jogosult, továbbá az adat hiteles forrása bizonyítható legyen.
- **Rendelkezésre állás:** az arra jogosult felhasználó a szükséges információhoz a megfelelő helyen és időben hozzáférhessen.

A keletkezett információk besorolási kategóriái a következők:

- **Nyilvános:** Minden olyan személyes és közérdekű adat, amelynek nyilvánosságra kerülése az érintett személyek, illetve szervezetek számára erkölcsi, anyagi és jogi következményekkel nem jár.
- **Belső információ:** Minden olyan adat, amely a szervezeten belül minden alkalmazottnak és szerződéses munkatársnak korlátozás nélkül rendelkezésére áll, ugyan-akkor szervezeten kívül nem kerül kihirdetésre.
- **Bizalmas:** Olyan nem minősített adat, amelynek nyilvánosságra kerülése az érintett személyek vagy szervezetek számára hátrányos erkölcsi, jogi és anyagi következményeket von maga után.
- **Szigorúan bizalmas:** az információszabadságról szóló törvényben meghatározott adatok, különös tekintettel a személyes és azon belül a különleges adatokra.

Ha a rögzíteni vagy létrehozni kívánt adat egyértelműen egyik adatcsoportba sem sorolható be, abban az esetben az adatgazda köteles az adat besorolási eljárását írásban kérni a jegyzőtől.

A szervezet informatikai rendszerének minden felhasználója köteles az általa tárolt, kezelt vagy létrehozott adatot annak besorolása szerint a szabályzatban meghatározott módon kezelni és tárolni. Az egyes adatokra vonatkozó előírások betartatásáért az adatgazda felelős. A szervezet informatikai rendszerében tárolt és kezelt adatok adatgazdája az a felhasználó, aki azt a rendszerben rögzítette, illetve létrehozta.

#### 4. Adatkezelők feladatai, jogosultságai

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 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 számítógépein lévő nyilvántartásokba történő belépés a jegyző döntése alapján az alábbi:

A jegyző jogosult a szervezetenél keletkező bármely adatba betekinteni.

Az ügyintézők részére a belépés csak a legszükségesebb körben, az ügyintéző munkaköri feladatai ellátásához kapcsolódóan engedélyezhető a következők szerint:

Megnevezés	Hozzáférési jogosultság
Ügyirat nyilvántartás	Minden dolgozó hozzáférhet
Közzszolgálati alapnyilvántartás	Személyzeti ügyintéző
Illetmény	Pénzügyi ügyintéző, adóügyi ügyintéző
Helyi népesség nyilvántartás	Igazgatási ügyintéző
Hatósági statisztika	Igazgatási ügyintéző
Szabálysértési statisztika	Igazgatási ügyintéző
Gyámügyi statisztika	Gyámügyi ügyintéző
Vagyonynyilvántartás	Pénzügyi ügyintézők
Helyi adó nyilvántartás	Adóügyi ügyintézők

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

- Az adatkezelő köteles az adatkezelési műveleteket úgy megtervezni és végrehajtani, hogy biztosítsa az érintettek magánszférájának védelmét.
- Az adatkezelő, illetve tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek e törvény, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.
- Az adatokat megfelelő intézkedésekkel védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetlenné válás ellen.
- A különböző nyilvántartásokban elektronikusan kezelt adatállományok védelme érdekében megfelelő technikai megoldással biztosítani kell, hogy a nyilvántartásokban tárolt adatok - kivéve ha azt törvény lehetővé teszi - közvetlenül ne legyenek összekapcsolhatók és az érintetthez rendelhetők.
- A személyes adatok automatizált feldolgozása során az adatkezelő és az adatfeldolgozó további intézkedésekkel biztosítja
  - a jogosulatlan adatbevitel megakadályozását;
  - az automatikus adatfeldolgozó rendszerek jogosulatlan személyek általi, adatátviteli berendezés segítségével történő használatának megakadályozását;
  - annak ellenőrizhetőségét és megállapíthatóságát, hogy a személyes adatokat adatátviteli berendezés alkalmazásával mely szerveknek továbbították vagy továbbíthatják;
  - annak ellenőrizhetőségét és megállapíthatóságát, hogy mely személyes adatokat, mikor és ki vitte be az automatikus adatfeldolgozó rendszerekbe;
  - a telepített rendszerek üzemzavar esetén történő helyreállíthatóságát és
  - azt, hogy az automatizált feldolgozás során fellépő hibákról jelentés készüljön.
- Az adatkezelőnek és az adatfeldolgozónak az adatok biztonságát szolgáló intézkedések meghatározásakor és alkalmazásakor tekintettel kell lenni a technika mindenkori fejlettségére.
- Több lehetséges adatkezelési megoldás közül azt kell választani, amely a személyes adatok magasabb szintű védelmét biztosítja, kivéve, ha az aránytalan nehézséget jelentene az adatkezelőnek.
- Az adatkezelésre jogosultak névsorának jóváhagyása a jegyző feladatkörébe tartozik. A belépésre vonatkozó személyi javaslat csak a munkavégzéshez feltétlenül szükséges, lehető legszűkebb körre vonatkozhat.
- A nyilvántartási rendszerekhez hozzáférési jogosultsággal rendelkezők névsorát a jegyző köteles naprakészen vezetni.
- Hozzáférési jogosultsággal rendelkező adatkezelő az adatlekérdezésekről e szabályzat mellékletét képező „Adatszolgáltatási nyilvántartást” köteles vezetni.
- A jegyző folyamatosan köteles ellenőrizni azt, hogy a nyilvántartási rendszerekhez hozzáférési jogosultsággal rendelkező személyek az adatkezelési szabályokat betartják-e.
- A jegyző havonta köteles ellenőrizni az adatkezelők által vezetett „Adatszolgáltatási nyilvántartás” naprakész vezetését.

## IV. KÖZÉRDEKŰ ADATOK KEZELÉSE

### 1. Közérdekű adatok nyilvánossága

A szervezet, mint jogszabályban meghatározott közfeladatot ellátó szerv a feladatkörébe tartozó ügyekben köteles elősegíteni és biztosítani a közvélemény pontos és gyors tájékoztatását.

A tájékoztatási kötelezettsége kiterjed különösen:

- a szervezet költségvetésére és annak végrehajtására,
- az önkormányzati rendeletekre,
- az önkormányzati vagyon kezelésére,
- a közpénzek felhasználására és az erre kötött szerződésekre,
- a piaci szereplők, a magánszervezetek és -személyek részére különleges vagy kizárólagos jogok biztosítására

vonatkozóan.

A szervezet rendszeresen, elektronikus úton, vagy más módon közzéteszi, továbbá erre irányuló igény esetén hozzáférhetővé teszi a tevékenységével kapcsolatos legfontosabb adatokat. így:

- hatáskör,
- illetékesség,
- szervezeti felépítés,
- szakmai tevékenység, annak eredményességére is kiterjedő értékelés,
- a birtokában lévő adatfajták, és működéséről szóló jogszabályok,
- gazdálkodás,
- önkormányzati rendeletek.

**Dunaszeg, Dunaszentpál és Kunsziget Községek Önkormányzata** saját honlappal rendelkezik.

A közérdekből nyilvános adatainkat a honlapon, ill. faliújságon tesszük közzé.

**A honlap működtetésével, frissítésével megbízottak neve, beosztása, elérhetősége:**

- **Dunaszeg esetében Nagyné Sztítás Judit, a Dunaszegi Közös Önkormányzati Hivatal ügykezelője**  
**szitas.judit@gmail.com; (96) 352-012**
- **Dunaszentpál esetében Csontos Attila, Dunaszentpál község polgármestere**  
**polgarmester@dunaszentpal.hu; (96) 352-026**
- **Kunsziget esetében Bábics Norbert, teleházvezető**  
**kunszigetitele haz@yahoo.com; (96) 552-010**

A szervezet kezelésében lévő közérdekből nyilvános adatokat bárki megismerheti kivéve:

- ha az adatot törvény alapján az arra jogosult szerv állam- vagy szolgálati titokká nyilvánította,
- ha az nemzetközi szerződésből eredő kötelezettség alapján minősített adat,

- ha a közérdekű adatok nyilvánosságához való jogot az adatfajta meghatározásával – főként bírósági vagy közigazgatási hatósági eljárásra tekintettel – törvény korlátozza.
- ha az adat a Ptk. 81. § (2) bekezdése alapján üzleti titoknak minősül.

A közérdekből nyilvános adatok megismerésére a közérdekű adatok megismerésére vonatkozó rendelkezéseket kell alkalmazni.

Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény előírja, hogy a közigazgatási informatika infrastrukturális megvalósíthatóságának biztosításáért felelős miniszter **közadatkeresőt** működtet.

A közadatkereső használatával bárki hozzáférhet a közzétételre kötelezett szervek közzétett adataihoz, pontosabban az arra utaló hivatkozásokhoz.

A közérdekű adatokat a saját honlapon túl a Közadattárban is közzéteszük.

A közérdekű adatok összegyűjtése a jegyző feladata.

A honlap működtetési feltételeinek a biztosítása, a megfelelő internetszolgáltató kiválasztása, a szolgáltatóval való szerződéskötés a polgármester feladata. A polgármester felelőssége, hogy a honlap a közérdekű adatok közzétételére alkalmas legyen, adatstruktúrája, formájának kialakítása, folyamatos üzemeltetése, az esetleges üzemzavar elhárítása biztosított legyen.

Az adatállomány megsemmisítés, adatvesztés, illetéktelen hozzáférés, törlés, módosítás elleni védelme az internetszolgáltató feladata.

A Kormányzati Informatikai Egyeztető Tárcaközi Bizottság (a továbbiakban: KIETB) 19. számú ajánlásában meghatározott formai és tartalmi követelmények érvényre juttatását a szervezet honlapján a költségvetési lehetőségek függvényében biztosítjuk.

## 2. A közadattárhoz való csatlakozás módja

A közadatkeresőhöz való csatlakozás miatt **regisztrálni kell** az [admin.kozadat.hu](http://admin.kozadat.hu) oldalon. A regisztrációkor megadott adatokat, a megfelelő aláírással ellátva el kell faxolni a Közadat Programhoz.(06-1/212-9220/105).

A KÖZPONTI HONLAPOT IGÉNYBE VEVŐ ADATGAZDÁKNAK: a [közzétételi szabályzat](#) és az adatszolgáltatást bemutató [dokumentum](#) alapján lehet feltölteni a saját tárhelyre a közérdekű adatokat, valamint elkészíteni a hozzájuk tartozó leíró adatokat. Ezután indítható az adminisztrációs felületen a tesztelés. Amennyiben sikeres volt a tesztelés akkor kérhető az aktiválás, melynek eredményeként a közzétett közérdekű adatokról elkészített metaadatok kereshetővé válnak az egységes közadatkereső rendszerben.

A 305/2005. (XII.25.) Korm. rendelet előírja, hogy a saját honlapon közzétevő a honlapján az egységes közadatkereső rendszerre mutató hivatkozást köteles elhelyezni.

## 3. A közzétételi eljárás szabályai

Az adatfelelős a közzéteendő adatokat elektronikus úton, elektronikus adathordozón, közzétételre alkalmas Word (doc), Excel (xls), kép(jpg) vagy pdf formátumban készíti el és juttatja a honlap működtetésével megbízott szolgáltatóhoz ill. megbízott dolgozóhoz.

A közlésre szánt adatokat az adatfelelős közvetlenül is rögzítheti az adatbázisba.

Az adattovábbítás felelőse a jegyző. A jegyző közvetlenül, a szolgáltató igénybe vétele nélkül is rögzíthet adatokat a honlapon.

Az adattovábbítást, valamint a honlapon történő megjelenítést úgy kell elvégezni, hogy a közzététel időpontja és a közlés időtartama megfeleljen a jogszabályban meghatározott határidőknek.

Az adatfelelős köteles havonta ellenőrizni a honlapon közölt adatok időszerűségét. A közzétett adatok pontatlanná, tévessé vagy időszerűtlenné válása, illetve ilyen adatok feltárása esetén az adatfelelős előállítja a helyesbített vagy frissített közérdekű adatokat tartalmazó közzétételi egységeket és azokat eljuttatja a szolgáltatónak.

Az adatfelelős minden esetben (új adat közlése, vagy pontosítás, javítás során stb.) ellenőrzi az eljuttatott és a közzétett adatok egyezőségét.

A közzétételi egység honlapról történő eltávolításának időpontjára, illetve előző állapota archiválásának (honlapon tartásának) időtartamára a jelen szabályzatban foglaltak az irányadók az alábbiak szerint:

- Amennyiben a közzétételi lista az adat előző állapotának archívumban tartását írja elő, az adat frissítése esetén annak elérhetővé tétele a megőrzési idő elteltéig nem szüntethető meg, és az adat mellett fel kell tüntetni az adatváltozás (frissítés) tényét, idejét, az új állapot fellelhetőségét, az archívumban elérhető adat elavulását.
- Frissített adat új állapota mellett fel kell tüntetni a frissítés tényét és idejét, illetve az adat előző állapotának archív állományban való elérhetőségét.

#### 4. Közzétételi lista

Szervezetünknel a közzeendő adatok megnevezését, az adat közzétételét előíró jogszabály számát, nevét, az adatok közlésének határidejét, frissítés gyakoriságát, az adatszolgáltatásért felelős személy megnevezését a közzétételi lista tartalmazza.

Adat megnevezése	Megjegyzés	Frissítés	Megőrzés	Adatközlésért felelős személy
Szervezet neve	a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól szóló 2004. évi CXL. törvény (Ket.) 164. § alapján közzeendő	az adatváltozást követő egy héten belül.	az előző állapot törlendő	jegyző
Címe				
Telefonszám				
Faxszám				
Elektronikus levélcím				
A honlap URL-je				
Polgármester neve, elérhetősége				
Polgármester ügyfélfogadása				
jegyző neve, elérhetősége, ügyfélfogadása				
Ügyintézők neve, ellátott ügykör, ügyfélfogadás				
Képviselő-testület tagjainak neve				
Bizottságok és tagjainak neve				



### Képviselő-testületek dokumentumai

Adat megnevezése	Megjegyzés	Frissítés	Megőrzés	Adatközlésért felelős személy
Képviselő-testület nyilvános ülésére szóló meghívó	az információs szabadságról szóló 2011. évi CXII. törvény	ülés előtt 5 nap	az ülés időpontjáig	jegyző
Képviselő-testület nyilvános előterjesztései		ülés előtt 5 nap	egy év	jegyző
Képviselő-testület nyilvános ülésének jegyzőkönyvei		ülés után 15 nap	egy év	jegyző
Önkormányzati rendeletek mellékletekkel együtt		elfogadás után 3 munkanap	mindaddig, amíg a rendelet hatályos, ill. a költségvetésről és zárszámadásról szóló rendeletek 5 évig	jegyző

**Az államháztartás alrendszeréből nyújtott, nem normatív, céljellegű, működési és fejlesztési támogatások (társadalmi szervezeteknek, egyesületeknek, egyházaknak stb. nyújtott támogatások)**

Adat megnevezése	Megjegyzés	Frissítés	Megőrzés	Adatközlésért felelős személy
Kedvezményezett szervezet neve, címe	az információs szabadságról szóló 2011. évi CXII. törvény	a döntés meghozatalát követő hatvanadik napig.	az előző állapot öt évig archivumban tartásával	pénzügyi előadó
Támogatás célja				
Támogatás összege				
A támogatási program megvalósítási helye				

### Szerződések közzététele

A nettó ötmillió forintot elérő vagy azt meghaladó értékű - árubeszerzésre, építési beruházásra, szolgáltatás megrendelésre, vagyonértékesítésre, vagyonhasznosításra, vagyon vagy vagyoni értékű jog átadására, valamint koncesszióba adásra vonatkozó szerződések vonatkozásában kell közzétenni.

Adat megnevezése	Megjegyzés	Frissítés	Megőrzés	Adatközlésért felelős személy
Szerződés megnevezése, tárgya	az információs szabadságról szóló 2011. évi CXII. törvény	a szerződés létrejöttét követő hatvan napon belül	az előző állapot öt évig archivumban tartásával	pénzügyi előadó
Szerződést kötő felek megnevezése				
Szerződés értéke				
Szerződés időtartama				

### Közbeszerzések közzététele

Adat megnevezése	Megjegyzés	Frissítés	Megőrzés	Adatközlésért felelős személy
Éves terv	az információs szabadságról szóló 2011. évi CXII. törvény és a Kbt.	negyedévente	egy évig archívumban tartva	jegyző
Az eljárás eredményéről vagy eredménytelenségéről szóló tájékoztatót tartalmazó hirdetmény				
A szerződés megkötéséről szóló tájékoztatót tartalmazó hirdetmény				

### Köztisztviselői álláspályázatok

Adat megnevezése	Megjegyzés	Frissítés	Megőrzés	Adatközlésért felelős személy
Pályázatot kiíró szervezet neve, címe	a közszolgálati tisztviselőkről szóló 2011. évi CXCV. törvény 45.§ alapján	a pályázati kiírás meghirdetésével egyidejűleg	a KSZK honlapján történő megjelenést követő legalább 15 napig, legkésőbb a pályázatban meghatározott jelentkezési határidőig	jegyző
Munkakör				
Képesítési követelmények				
Egyéb tudnivalók a pályázattal kapcsolatban	a pályázati eljárás során a pályázatot kiíró szerv köteles a felhívást elektronikus úton megküldeni a kormányzati személyügyi igazgatási feladatokat ellátó szerv a Kormányzati Személyügyi Központ részére, amely azt elektronikusan közzéteszi az egységes hozzáférés biztosítása érdekében			
	az álláspályázatok a saját honlapon is célszerű közzétenni			

## A hatósági, szociális, adó ügyek intézésével kapcsolatos adatok

Adat megnevezése	Megjegyzés	Frissítés	Megőrzés	Adatközlésért felelős személy
Hatósági, szociális és adó ügyekkel kapcsolatos tájékoztatók ügykörönként csoportosítva	Ket. 164. § (1)-(2) bekezdése, valamint a KIEB 19. sz. ajánlás alapján ajánlott a honlapon szerepeltetni	jogszabály változások alapján szükség szerint	az előző állapotot törölni szükséges	szociális ügyintéző adóügyi ügyintéző
A használt formanyomtatványok listája, lehetőleg a formanyomtatványok letölthetőségének biztosításával ügykörönként csoportosítva				
Az ügyintézéshez szükséges dokumentumok, okmányok felsorolása ügykörönként csoportosítva				

### 5. A közérdekű adatok megismerésére irányuló igény és teljesítése

A közérdekű adat megismerése iránt bárki szóban vagy írásban igényt nyújthat be.

Az igénylő a közérdekű adat megismerése iránti igényét írásban benyújthatja az általa írt igénylés formájában vagy a szervezet által e célra rendszeresített nyomtatványon. Az e melléklet szerinti nyomtatvány a szervezetnél igényelhető és benyújtható. A benyújtott igényeket az igényelt adatokat kezelő adatfelelőse teljesíti. Amennyiben az igény nem az annak teljesítésére illetékes szervezeti egységhez érkezik be, akkor az igényt a jegyzőhöz szignálásra kell továbbítani. A szervezet vezetője a beérkezett igénybejelentő lap alapján kijelöli az adatszolgáltatásra köteles szervezeti egységet.

A szóban benyújtott igényről az ügyintéző jegyzőkönyvet készít, majd a jegyzőkönyv alapján, a kérelem felülvizsgálata után teljesíti az adatszolgáltatást.

A közérdekű adat megismerésére irányuló igények elektronikus úton történő fogadását szervezetünk nem biztosítja.

A kérelmező igénylésében köteles az általa igényelt közérdekű adatot (adatokat) egyértelműen és konkrétan megjelölni.

A közérdekű adat megismerésére irányuló kérelemnek a szervezet az igény tudomására jutását követő legrövidebb idő alatt, legfeljebb azonban 15 napon belül tesz eleget. A szervezet a közérdekű adatot tartalmazó adatbázisról történő másolat készítéséért – legfeljebb az azzal kapcsolatban felmerült mértékig terjedően – költségtérítést állapít meg.

Az adatigénylésnek közérthető formában és – amennyiben az aránytalan költséggel nem jár – az igénylő által kívánt technikai eszközzel, illetve módon kell eleget tenni. Az adatigénylést

nem lehet elutasítani arra való hivatkozással, hogy annak közérthető formában nem lehet eleget tenni.

Az igény teljesítésének megtagadásáról, annak indokaival együtt, 8 napon belül írásban, vagy – amennyiben az igény elektronikus levelezési címét közölte – elektronikus úton értesíteni kell az igénylőt.

A közérdekű adat megismerése iránti igény teljesítése nem tagadható meg azért, mert a nem magyar anyanyelvű az igényét anyanyelvén, vagy az általa értett más nyelven fogalmazta meg, amennyiben az igénylő nyilatkozatában vállalja a fordítással járó többletköltségek viselését.

A szóban előterjesztett igényt akkor lehet szóban teljesíteni:

- az igényelt adat a honlapon, faliújságon, hirdetőtáblán vagy más módon jogszerűen már nyilvánosságra került,
- az igényelt adat az önkormányzat tisztségviselőinek, munkatársainak, az önkormányzati hivatal dolgozóinak, valamint az önkormányzati feladatot ellátó szerv feladat- és hatáskörében eljáró személy nevére, beosztására, hivatali elérhetőségére vonatkozik,
- az igény az önkormányzat, a hivatal, illetőleg az önkormányzati szerv hatáskörére, eljárására, az alkalmazott jogszabályokra vonatkozó általános tájékoztatással teljesíthető,
- az igénylő szóban kéri a választ és az számára kielégítő,
- az adatkérés arra irányul, hogy egy adott ügy folyamatban van-e ebben az esetben a szóbeli közlés nem terjedhet túl a folyamat tényének közlésén.

A szóban előterjesztett igény a kért dokumentum faxon történő megküldésével is teljesíthető. Ebben az esetben a küldés bizonylatát feljegyzésnek kell tekinteni.

Amennyiben a szóbeli megválaszolással kért adatok nyilvánossága, illetőleg nyilvánosságra hozhatósága kétséget kizáróan, egyértelműen nem állapítható meg, a kérelemről jegyzőkönyvet kell felvenni és az adatfelelősnek az igényt haladéktalanul a jegyzőhöz kell továbbítania. Kétség esetén a kérelem teljesíthetőségéről minden esetben a jegyző dönt.

A döntés előkészítés szakaszába tartozó adatok, dokumentumok, valamint az önkormányzati hatósági ügyek adatai, közigazgatási, államigazgatási hatósági ügyek adatai tekintetében az adatközlést kizárólag a jegyző engedélyezi.

Nem minősül közérdekű adatigénylésnek az olyan beadvány, amely közigazgatási vagy önkormányzati hatósági eljárás lefolytatását igényli.

Amennyiben a kért közérdekű adat a honlapon, faliújságon már közzétételre került, a válaszban az igénylőt e tényről és a fellelhetőségről tájékoztatni kell. A honlapon történő közzététel azonban nem mentesít a válaszadási kötelezettség alól.

A kért adat kérelmezővel való, helyben történő megismertetéséhez megfelelő időt, tárgyi feltételeket kell biztosítani, melynek során az adatfelelős vagy az általa megbízott személy folyamatos jelenléte szükséges.

A kérelmező jogosult jegyzetet készíteni, és az adatokat tartalmazó dokumentumról vagy dokumentumrészről, annak tárolási módjától függetlenül másolatot kérni. Amennyiben a

közérdekű adatot tartalmazó dokumentum az igénylő által meg nem ismerhető adatot is tartalmaz, a másolaton a meg nem ismerhető adatot törölni vagy felismerhetetlenné kell tenni.

Az adatok közlésével összefüggésben (a másolat készítéséért; az adathordozóért; az adatok meghatározott szempontok szerinti előállításának, illetve csoportosításának ellenértékéért járó munkadíjként) felmerült költséggel arányos térítés kérhető. A költségtérítés összege megállapításának és megfizetésének módját a jelen szabályzat melléklete tartalmazza.

A fizetendő költségtérítés összegét az adatszolgáltatást megelőzően az igénylő kérésére közölni kell, a nagyobb terjedelmű – a 20 A/4-es, a 10 A/3-as oldalt meghaladó oldalszámú– másolat, valamint a 4 munkaóránál több időt igénylő, adatigénylés szerinti adatcsoportosítás, adat-előállítás esetén a költségtérítés előre történő közlése nem mellőzhető. Az adatigénylés esetén a költségtérítés pontos összegét az adatszolgáltatást megelőzően –annak terjedelmétől függetlenül minden esetben– meg kell határozni.

Az egyéb adatszolgáltatás (pl. vállalkozói adatbázisból, rendezési tervből stb.) igazgatási szolgáltatási díjának meghatározása önköltségszámítás alapján történik.

A költségtérítés összegeként megállapított díj az önkormányzat költségvetési elszámolási számlájára az alábbi módon fizethető meg:

- az önkormányzat házipénztárába készpénzbefizetéssel,
- postai úton, készpénzfizetési megbízással (csekken),
- banki átutalással.

A teljesített szolgáltatásról minden esetben számlát kell kiállítani.

A közérdekű adat megismerésére irányuló kérelemnek a szervezet az igény tudomására jutását követő legrövidebb idő alatt, legfeljebb azonban 15 napon belül tesz eleget.

Nem hozható nyilvánosságra:

- az üzleti titok, különösen az alkalmazott technológiai eljárások, műszaki megoldások, gyártási folyamatok munkaszervezési, és logisztikai módszerek, feltéve, hogy nem akadályozza közérdekű adatok megismerését
- olyan személyes adat, illetve jogi személyek, jogi személyiség nélküli szervezetek, olyan adata, amely nem minősül közérdekből nyilvános adatnak
- képviselő testületi zárt ülésről készült jegyzőkönyv.

## **6. Jogorvoslat a közérdekű adatok teljesítésével kapcsolatban**

Amennyiben az adatkezelő szerv a kért adat közlését megtagadja /azért mert az állami vagy szolgálati titok vagy más minősített adat, illetőleg egyéb okból nem minősül közérdekű adatnak/ 8 napon belül indoklással együtt alakszerű államigazgatási határozat meghozatalával kell értesíteni a kérelmezőt. A megtagadás jogszerűségét és megalapozottságát bizonyítani kell, /ilyen lehet ha az adatszolgáltatási kérelem személyes adat, különleges adat kiadására irányul/ és ehhez az érintett nem járul hozzá /pl.: a szervezet köztisztviselőinek illetménye/ vagy ha a törvény korlátozza a nyilvánossághoz való jogot. /pl.: honvédelmi, nemzetbiztonsági, bűnüldözési érdek/.

A megtagadás ellen 30 napon belül a bírósághoz lehet fordulni.

Ha a szervezet a közérdekű adatra vonatkozó igényt nem teljesíti, az igénylő az Info. tv. 31. §-ban foglalt eljárási rendnek megfelelően bírósághoz fordulhat.

A megtagadás jogszerűségét és megalapozottságát a szervezet köteles bizonyítani.

Az elutasított kérelmekről, illetve azok indokairól nyilvántartást kell vezetni, amelyben foglaltakról a Nemzeti Adatvédelmi és Információszabadság Hatóságot minden év január 31. napjáig tájékoztatni szükséges. A nyilvántartás vezetéséért és az adatok megküldéséért az igazgatási előadó a felelős.

## V.

### **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 szervezet illetékességi területén lakóhellyel, tartózkodási hellyel rendelkező 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 közzlése. Ezen belül:

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

#### **3. Személyes adatok védelme**

A polgárok személyi adatainak és lakcímének helyi nyilvántartásából (a továbbiakban: nyilvántartás) történő adatszolgáltatás engedélyezése során az alábbiak szerint kell eljárni:

A számítógépes rendszerbe történő belépés a jegyző döntése alapján a személyes jelszón kívül a hozzáférési jogosultsággal rendelkező személyi azonosítója megadásával történhet. A belépés csak a legszükségesebb körben engedélyezhető.

A számítógépes rendszerbe való belépés engedélyezéséről a jegyző nyilvántartást vezet.

A belépésre jogosultak nevét és a szervezeti beosztását a *7. számú melléklet* tartalmazza.

Az adatkezelés törvényességének ellenőrzése szervezetünknel a jegyző feladata.

#### **4. Adatszolgáltatás**

Az 1992. évi LXVI. tv. 6. § (1) bekezdése alapján az e törvényben meghatározott feladatokat a települési (fővárosi kerületi) önkormányzat jegyzője, illetve a fővárosi önkormányzat által közvetlenül igazgatott terület tekintetében a fővárosi főjegyző (a továbbiakban együtt: jegyző), fővárosi és megyei kormányhivatal járási (fővárosi kerületi) hivatala (a továbbiakban: járási hivatal), a kormányablak, a fővárosi és megyei kormányhivatal és a nyilvántartást kezelő központi szerv (a továbbiakban: központi szerv) látja el.

##### **A járási hivatal**

a törvényben meghatározott feltételek fennállása esetén adatszolgáltatást teljesít a nyilvántartásból;

közokiratot ad ki a nyilvántartott adatokról;

A települési önkormányzat jegyzője a 14 éven aluli érintett és az egészségügyi okból történő akadályoztatása esetén átveszi a polgár személyazonosító igazolvány iránti kérelmét, ellenőrzi a kérelmező jogosultságát és személyazonosságát, ellátja a kérelem továbbításával kapcsolatban hatáskörébe utalt hatósági feladatokat.

##### **Adatszolgáltatás a nyilvántartásból**

Egyedi adatszolgáltatás az adatigénylő lakó- vagy tartózkodási helye, székhelye, telephelye szerint, illetőleg az érintett polgár ismert lakcíme szerint illetékes járási hivataltól kérelmezhető. A központi szervtől akkor igényelhető az egyedi adatszolgáltatás, ha az a járási hivatal által - a szükséges technikai feltételek hiányában, vagy egyéb okból - nem, illetőleg csak célszerűtlenül teljesíthető.

Csoportos adatszolgáltatás a járási hivatal illetékességi területén lakcímmel rendelkező polgárok adatairól az illetékes járási hivataltól, a polgárok szélesebb körének adatait érintően a központi szervtől igényelhető.

Az adatszolgáltatás iránti kérelmet az 1992. évi LXVI. tv. végrehajtására kiadott, többször módosított 146/1993. (X. 26.) Korm. rendelet 2. sz. melléklete szerinti tartalommal kell benyújtani. A Korm. rendelet 27. § (1) bekezdés alapján a jegyző az általa vezetett nyilvántartásból külön kérelem nélkül is felhasználhat, illetve szolgáltatathat adatot ugyanazon települési önkormányzat képviselő-testületének, polgármesterének, illetve a polgármesteri hivatal ügyintézőjének feladatai ellátásához, feltéve, hogy ezt törvény vagy törvény felhatalmazása alapján önkormányzati rendelet lehetővé teszi.

Az adatszolgáltatások engedélyezéséről az igazgatási előadó nyilvántartást köteles vezetni.

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 tájékoztatást kérhet saját személyes adatai kezeléséről, kérheti személyes adatainak helyesbítését, törlését.

Ügyfélnek és képviselőjének a rá vonatkozó iratba való betekintés lehetőségét és erről másolat készítését oly mértékben kell biztosítani, amennyire ez mások személyiségi jogainak sérelme nélkül lehetséges. Az iratról való másolat készítésének költségeit az ügyfélnek kell megtérítenie.

A KIM Területi Közigazgatásért és Választásért Felelős Államtitkárnak XXII-3/98/10/2013 számú tájékoztatása alapján mind a jegyző, mind a járási hivatal illetékes a nyilvántartott adatokról hatósági bizonyítvány kiadására.

Hatósági bizonyítványt az ügyfél a saját adatairól, vagy a 14 éven aluli kiskorú hozzátartozója adatairól kérhet. Más családtagok esetében két tanú által aláírt meghatalmazás alapján kérhető/ adható ki a hatósági bizonyítvány.

## 5. Ellenőrzés

A szervezet informatikai feladatokkal megbízott vezetője a jegyző, aki rendszeresen köteles ellenőrizni a személyes adatok védelmének érvényesülését, így különösen:

- a szervezet adatvédelmi szabályainak aktualitását, rendelkezései törvényességét,
- az adatszolgáltatások engedélyezésére vonatkozó jogszabályi rendelkezések betartását,
- az adatvédelmi nyilvántartások vezetését,
- a nyilvántartás adatállománya megóvására tett technikai intézkedések megfelelőségét,
- a szervezet vezetője az ellenőrzések tapasztalatairól köteles rendszeresen beszámolni.

## VI.

### INFORMATIKAI BIZTONSÁGI SZABÁLYZAT

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény alapján a szervezet informatikai biztonsági szabályzatát az alábbiak szerint adom ki.

#### Értelmező rendelkezések

*adminisztratív védelem:* a védelem érdekében hozott szervezési, szabályozási, ellenőrzési intézkedések, továbbá a védelemre vonatkozó oktatás;

*auditálás:* előírások teljesítésére vonatkozó megfelelőségi vizsgálat, ellenőrzés;

*bizalmasság:* az elektronikus információs rendszer azon tulajdonsága, hogy a benne tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról;

*biztonsági esemény:* nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat, amely az elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, és amelynek hatására az elektronikus információs rendszer által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül;

*biztonsági esemény kezelése:* az elektronikus információs rendszerben bekövetkezett biztonsági esemény dokumentálása, következményeinek felszámolása, a bekövetkezés okainak és felelőseinek megállapítása, és a hasonló biztonsági események jövőbeni előfordulásának megakadályozása érdekében végzett tervszerű tevékenység;

*biztonsági osztály:* az elektronikus információs rendszer védelmének elvárt erőssége;

*biztonsági osztályba sorolás:* a kockázatok alapján az elektronikus információs rendszer védelme elvárt erősségének meghatározása;

*biztonsági szint:* a szervezet felkészültsége az e törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok kezelésére;

*biztonsági szintbe sorolás:* a szervezet felkészültségének meghatározása az e törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok kezelésére;



*elektronikus információs rendszer biztonsága:* az elektronikus információs rendszer olyan állapota, amelyben annak védelme az elektronikus információs rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos;

*életciklus:* az elektronikus információs rendszer tervezését, fejlesztését, üzemeltetését és megszüntetését magába foglaló időtartam;

*észlelés:* a biztonsági esemény bekövetkezésének felismerése;

*felhasználó:* egy adott elektronikus információs rendszert igénybe vevők köre;

*fenyegetés:* olyan lehetséges művelet vagy esemény, amely sértheti az elektronikus információs rendszer vagy az elektronikus információs rendszer elemei védettségét, biztonságát, továbbá olyan mulasztásos cselekmény, amely sértheti az elektronikus információs rendszer védettségét, biztonságát;

*fizikai védelem:* a fizikai térben megvalósuló fenyegetések elleni védelem, amelynek fontosabb részei a természeti csapás elleni védelem, a mechanikai védelem, az elektronikai jelzőrendszer, az élőerős védelem, a beléptető rendszer, a megfigyelő rendszer, a tápáramellátás, a sugárzott és vezetett zavarvédelem, klimatizálás és a tűzvédelem;

*folytonos védelem:* az időben változó körülmények és viszonyok között is megszakítás nélkül megvalósuló védelem;

*globális kibertér:* a globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttese;

*informatikai biztonságpolitika:* a biztonsági célok, alapelvek és a szervezet vezetői elkötelezettségének bemutatása az e törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok irányítására és támogatására;

*informatikai biztonsági stratégia:* az informatikai biztonságpolitikában kitűzött célok megvalósításának útja, módszere;

*információ:* bizonyos tényekről, tárgyakról vagy jelenségekről hozzáférhető formában megadott megfigyelés, tapasztalat vagy ismeret, amely valakinek a tudását, ismeretkészletét, annak rendezettségét megváltoztatja, átalakítja, alapvetően befolyásolja, bizonytalanságát csökkenti vagy megszünteti;

*kiberbiztonság:* a kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a kibertert megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhez és működtetéséhez;

*kibervédelem:* a kibertérből jelentkező fenyegetések elleni védelem, ideértve a saját kibertér képességek megőrzését;

*kockázat:* a fenyegetettség mértéke, amely egy fenyegetés bekövetkezése gyakoriságának (bekövetkezési valószínűségének) és az ez által okozott kár nagyságának a függvénye;

*kockázatelemzés:* az elektronikus információs rendszer értékének, sérülékenységének (gyenge pontjainak), fenyegetéseinek, a várható károknak és ezek gyakoriságának felmérése útján a kockázatok feltárása és értékelése;

*kockázatkezelés:* az elektronikus információs rendszerre ható kockázatok csökkentésére irányuló intézkedésrendszer kidolgozása;

*kockázatokkal arányos védelem:* az elektronikus információs rendszer olyan védelme, amelynek során a védelem költségei arányosak a fenyegetések által okozható károk értékével;

*korai figyelmeztetés:* valamely fenyegetés várható bekövetkezésének jelzése a fenyegetés bekövetkezése előtt annyi idővel, hogy hatékony védelmi intézkedéseket lehessen hozni;

*létfontosságú információs rendszerrelem:* az európai létfontosságú rendszerrelemmé és a nemzeti létfontosságú rendszerrelemmé törvény alapján kijelölt létfontosságú rendszerrelemek azon elektronikus információs létesítményei, eszközei vagy szolgáltatásai, amelyek

működésképtelenné válása vagy megsemmisülése az európai létfontosságú rendszerelémmé és a nemzeti létfontosságú rendszerelémmé törvény alapján kijelölt létfontosságú rendszerelemeket vagy azok részeit elérhetlenné tenné, vagy működőképességüket jelentősen csökkentené;

*logikai védelem:* az elektronikus információs rendszerben információtechnológiai eszközökkel és eljárásokkal (programokkal, protokollokkal) kialakított védelem;

*magyar kibertér:* a globális kibertér elektronikus információs rendszereinek azon része, amelyek Magyarországon találhatóak, valamint a globális kibertér elektronikus rendszerein keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok közül azok, amelyek Magyarországon történnek vagy Magyarországra irányulnak, illetve Magyarország érintett benne;

*megelőzés:* a fenyegetés hatása bekövetkezésének elkerülése;

*reagálás:* a bekövetkezett biztonsági esemény terjedésének megakadályozására vagy késleltetésére, a további károk mérséklésére tett intézkedés;

*rendelkezésre állás:* annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek;

*sértetlenség:* az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az az elvárt forrásból származik (hitelesség) és a származás ellenőrizhetőségét, bizonyosságát (letagadhatatlanságát) is, illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható;

*sérülékenység:* az elektronikus információs rendszer olyan része vagy tulajdonsága, amelyen keresztül valamely fenyegetés megvalósulhat;

*sérülékenység-vizsgálat:* az elektronikus információs rendszerek gyenge pontjainak (biztonsági rések) és az ezeken keresztül fenyegető biztonsági eseményeknek a feltárása;

*számítógépes incidenskezelő központ:* az Európai Hálózat- és Információbiztonsági Ügynökség ajánlásai szerint működő, számítástechnikai vészhelyzetekre reagáló egység, amely a nemzetközi hálózatbiztonsági, valamint kritikus információs infrastruktúrák védelmére szakosodott szervezetekben tagsággal és akkreditációval rendelkezik [(európai használatban: CSIRT (Computer Security Incident Response Team), amerikai használatban: CERT (Computer Emergency Response Team)];

*teljes körű védelem:* az elektronikus információs rendszer valamennyi elemére kiterjedő védelem;

*üzemeltető:* az a természetes személy, jogi személy, jogi személyiséggel nem rendelkező gazdasági társaság vagy egyéni vállalkozó, aki vagy amely az elektronikus információs rendszer vagy annak részei működtetését végzi és a működésért felelős;

*védelmi feladatok:* megelőzés és korai figyelmeztetés, észlelés, reagálás, eseménykezelés;

*zárt célú elektronikus információs rendszer:* jogszabályban meghatározott elkülönült nemzetbiztonsági, honvédelmi, rendészeti, igazságszolgáltatási, külügyi feladatokat ellátó elektronikus információs, informatikai vagy hírközlési rendszer;

*zárt védelem:* az összes számításba vehető fenyegetést figyelembe vevő védelem.

Elektronikus információs rendszer az adatok, információk kezelésére használt eszközök (környezeti infrastruktúra, hardver, hálózat és adathordozók), eljárások (szabályozás, szoftver és kapcsolódó folyamatok), valamint az ezeket kezelő személyek együttese:

a) számítástechnikai rendszerek és hálózatok;

b) helyhez kötött, mobil és egyéb rádiófrekvenciás, valamint műholdas elektronikus hírközlési hálózatok, szolgáltatások;

c) rádiós vagy műholdas navigáció;

d) automatizálási, vezérlési és ellenőrzési rendszerek (vezérlő és adatgyűjtő, távmérő, távérzékelő és telemetriai rendszerek);

e) a fentiek felderítéséhez, lehallgatásához vagy zavarásához használható rendszerek.

Egy elektronikus információs rendszernek kell tekinteni az azonos adatkezelő és adatfeldolgozó által, egymással kapcsolatban álló eszközökön (környezeti infrastruktúra, hardver, hálózat), egymással összefüggő eljárásokkal (szabályozás, szoftver és kapcsolódó folyamatok) azonos célból kezelt, kiszolgált, illetve felhasznált adatok, az ezek kezelésére használt eszközök, eljárások, valamint az ezeket kezelő, kiszolgáló és felhasználó személyek együttesét.

### **1. Alapvető elektronikus információbiztonsági követelmények**

Az elektronikus információs rendszerek teljes életciklusában meg kell valósítani és biztosítani kell

a) az elektronikus információs rendszerben kezelt adatok és információk bizalmassága, sértetlensége és rendelkezésre állása, valamint

b) az elektronikus információs rendszer és elemeinek sértetlensége és rendelkezésre állása zárt, teljes körű, folytonos és kockázatokkal arányos védelmével.

Az elektronikus információs rendszernek megfelelő védelme körében a szervezetnek biztosítani kell.

a) a megelőzést és a korai figyelmeztetést,

b) az észlelést,

c) a reagálást,

d) a biztonsági események kezelését.

### **2. Az elektronikus információs rendszer biztonsági osztályba sorolását az elektronikus információs rendszer biztonságáért felelős személy végzi. A Szervezet számára a jogszabályban előírt biztonsági osztály: 2.**

A biztonsági osztályba sorolást legalább háromévenként vagy szükség esetén soron kívül, dokumentált módon felül kell vizsgálni.

### **3. Az elektronikus információs rendszer biztonságáért felelős személy feladatai**

Az elektronikus információs rendszer biztonságáért felelős személy feladata ellátása során a szervezet vezetőjének közvetlenül adhat tájékoztatást, jelentést.

Az elektronikus információs rendszer biztonságáért felelős személy felel a szervezetenél előforduló valamennyi, az elektronikus információs rendszerek védelméhez kapcsolódó feladat ellátásáért.

Ennek körében:

a) gondoskodik a szervezet elektronikus információs rendszereinek biztonságával összefüggő tevékenységek jogszabályokkal való összhangjának megteremtéséről és fenntartásáról,

b) elvégzi vagy irányítja az a) pont szerinti tevékenységek tervezését, szervezését, koordinálását és ellenőrzését,

c) előkészíti a szervezet elektronikus információs rendszereire vonatkozó informatikai biztonsági szabályzatot,

d) előkészíti a szervezet elektronikus információs rendszereinek biztonsági osztályba sorolását és a szervezet biztonsági szintbe történő besorolását,

e) véleményezi az elektronikus információs rendszerek biztonsága szempontjából a szervezet e tárgykört érintő szabályzatait és szerződéseit,

f) kapcsolatot tart a hatósággal és a kormányzati eseménykezelő központtal.

Az elektronikus információs rendszer biztonságáért felelős személy az elektronikus információs rendszert érintő biztonsági eseményről a jogszabályban meghatározottak szerint tájékoztatni köteles a jogszabályban meghatározott szervet.

Az elektronikus információs rendszer biztonságáért felelős személy biztosítja az alábbiak teljesülését:

a) a szervezet valamennyi elektronikus információs rendszerének a tervezésében, fejlesztésében, létrehozásában, üzemeltetésében, auditálásában, vizsgálatában, kockázatelemzésében és kockázatkezelésében, karbantartásában vagy javításában közreműködők,

b) ha a szervezet az adatkezelési vagy az adatfeldolgozási tevékenységhez közreműködőt vesz igénybe, a közreműködők

e törvény hatálya alá tartozó elektronikus információs rendszereit érintő, biztonsággal összefüggő tevékenysége esetén.

Az elektronikus információs rendszer biztonságáért felelős személy és az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személyek miniszteri rendeletben meghatározott rendszeres szakmai képzésen, továbbképzésen vesznek részt.

Az elektronikus információs rendszer biztonságáért felelős személy a feladatait megbízás alapján látja el, adatai a Nemzeti Elektronikus Információbiztonsági Hatóság (NEIH) számára jelentésre kerülnek.

#### **Az elektronikus információs rendszerek védelméért felelős vezető szervezetünknél:**

dr. Szigethy Balázs jegyző  
96-352-012

[jegyzo@dunaszeg.hu](mailto:jegyzo@dunaszeg.hu);

#### **Az elektronikus információs rendszer biztonságának megteremtésében közreműködik:**

Rendszergazda neve, beosztása, elérhetősége:

SZIGETKÖZ NET Kft.  
Borbényi András  
ügyvezető  
9174 Dunaszeg, Nefelejcs u. 23.  
Mobil: 70/313-9859  
e-mail: andras.borbenyi@szigetkoz.net

#### **4. Adatok és programok védelme**

A szervezet számítógépes adat-feldolgozási folyamatába kerülő információkat és programokat fokozott biztonsági szabályok szerint kell kezelni.

A szervezetnél működő számítógépeken csak előzetesen ellenőrzött tanúsítással rendelkező 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.

A szervezet a használatban lévő programjairól nyilvántartást vezet. A nyilvántartás vezetéséért, aktualizálásáért a szervezet vezetője a felelős.

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

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

Vásárolt, vagy átvett lemezen 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 munkavállaló 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 üzemeltetésért felelős vállalkozót 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 a számítógép merevlemezére és a hálózati rendszerbe is. Év végén az elektronikusan lezárt adatállományt lemezre kell menteni.
- 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 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 (**13. számú melléklet**).

## **5. Számítógépek, eszközök és dokumentációk védelme**

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

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 munkavállaló köteles a munkaidő végzetével 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 rendszerleírások, rendszerprogram dokumentációk, felhasználói dokumentációk tárolása zárható és tűzmentes szekrényben történik.

Elektromos érintésvédelmi szempontból a számítástechnikai eszközöket csak védőföldeléses, minden számítógéphez leltár szerint tartozó biztonsági kapcsolóval ellátott dugaszoló aljzatba lehet csatlakoztatni. A Szervezet számítógépeinek folyamatos működését szünetmentes áramforrás biztosítja. 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.

## **6. 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

## **7. 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 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.

## **8. Nemzeti Elektronikus Információbiztonsági Hatóság**

A Nemzeti Elektronikus Információbiztonsági Hatóság feladatait és hatáskörét a 301/2013. (VII. 29.) Korm. rendelet rögzíti.

Címe: 1440 Bp., Pf.: 1.

A hatóság nyilvántartja és kezeli:

- a szervezet elektronikus információs rendszereinek megnevezését, az elektronikus információs rendszerek biztonsági osztályának és a szervezet biztonsági szintjének besorolását, az elektronikus információs rendszerek külön jogszabályban meghatározott technikai adatait,
- a szervezetnek az elektronikus információs rendszer biztonságáért felelős személye természetes személyazonosító adatait, telefon- és telefaxszámát, e-mail címét, a 13. § (8) bekezdésében meghatározott végzettségét,
- a szervezet informatikai biztonsági szabályzatát,
- a biztonsági eseményekkel kapcsolatos bejelentéseket.

A hatóság az elektronikus információs rendszerek, és az azokban kezelt adatok biztonsága érdekében jogosult megtenni, elrendelni, ellenőrizni minden olyan, az elektronikus

információs rendszer védelmére vonatkozó intézkedést, amellyel az érintett elektronikus információs rendszert veszélyeztető fenyegetések kezelhetőek. Ennek érdekében jogosult: az érintett szervezeteknél a jogszabályokban foglalt biztonsági követelményeket és az ehhez kapcsolódó eljárási szabályok teljesülését ellenőrizni,

A szervezet informatikai biztonsági szabályzatát, valamint a biztonsági felelős személy természetes személy azonosító adatait, telefon és fax számát, e-mail címét, végzettségét adatait a NEHI részére 2014. február 5-ig meg kell küldeni. Az adatközlés felelőse a jegyző.

## VII. KATASZTRÓFA-ELHÁRÍTÁSI SZABÁLYOK

### 1. Vészhelyzetek

Minden megelőző intézkedés dacára előfordulhatnak vészhelyzetek:

- **Hardverhiba:** A merevlemezeknél is felmerülhet időnként mechanikus hiba (hiszen végső soron mozgó elemekből állnak), rossz szektor jöhet létre, vagy elromolhat valamelyik elektromos alkatrész.
- **Szoftverhiba:** Alkalmazáshiba, az operációs rendszer összeomlása vagy torlódás (lockup) is károsíthatja az adatokat. Rosszindulatú számítógépes vírusok okozta adatvesztés.
- **Természeti katasztrófák:** A számítógép elemeinek (és a rajta tárolt adatoknak) általában nincs túl sok esélyük a természeti csapásokkal (tűz, árvíz, áramkimaradás) szemben.
- **Emberi hiba:** Emberi mulasztás véletlenül megváltoztathatjuk vagy letörölhetjük a számunkra fontos adatokat.

Ilyen esetekben négy fontos célt kell szem előtt tartani:

- Lehetőség szerint előzzük meg a további károkat.
- Hozzunk megfelelő intézkedéseket a hasonló esetek elkerülésére.
- Segítsük elő a normál üzem visszaállítását.
- Segítsük elő az okok kiderítését vagy a nyomozást.

### 2. További károk megelőzése

Hardverhiba vagy véletlen adatvesztés esetén hívjunk szakembert. Szoftverhiba esetén értesítsük a szoftver gyártóját vagy telepítőjét. A további károk megelőzésére a külső hálózati kapcsolatot szakítsuk meg. A belső hálózat particionálása történjen meg a támadás, vírusfertőzés továbbterjedésének megakadályozására. A védett rendszereket kapcsoljuk le. Természeti katasztrófák esetén a Szervezet ide vonatkozó szabályzatai (Tűzvédelmi, Munkavédelmi) szerint járjunk el.

Fontos arra figyelni, hogy megtaláljuk a kellő kompromisszumot a kár megelőzése és a rendszer ezen célú megállítása között, hiszen nem szerencsés, ha bármely vészhelyzetre azzal válaszolunk, hogy megszüntetjük rendszerünk működését. A megfelelő logikai zónák kialakításával a támadás súlyosságától függően van lehetőségünk arra, hogy milyen mértékben avatkozzunk be a rendszer működésébe.



Néha célszerű a támadásra úgy reagálni, hogy hagyjuk a támadást folyni, de közben, a támadó számára lehetőleg észrevétlenül, megfigyeljük tevékenységét. Ez segíthet a következő pont megvalósításában.

### **3. Hasonló esetek megelőzése**

Megtörtént eseményt követően nem elegendő az aktuális veszélyhelyzetet megszüntetni, pl. vírustámadás esetén a hálózati kapcsolat megszakításával, hiszen várható, hogy azon a módon, ahogy ez a támadó bejutott, más is be fog jutni. Meg kell keresni és be kell tölteni a biztonsági rést! Ebben nagy segítségre lehet, ha megfigyeljük a támadás folyamatát, ugyanis ekkor könnyebben tudunk következtetni arra, hogy mi is volt az a tényező, amelyet kihasználva bejutott a támadó.

### **4. Normál üzem visszaállítása**

A normál üzem visszaállítása egy káresemény után igényli nem csak a sérült adatok visszaállítását, de a rendszer integritásáról való megbizonyosodást is. Erre célra különböző eszközök léteznek, amelyek a rendszer aktuális állapotát összehasonlítják valamely korábban elmentett állapottal (rendszerint ellenőrzőösszegek alapján).

Természetesen kétséges helyzetben legcélszerűbb a rendszer újratelepítése, ez azonban általában munkaigényes és nagy fennakadással áll. Célszerű lehet a telepített és felkonfigurált rendszerről egy „pillanatfelvételt” készíteni, amely lehet a merevlemez másolata Norton Ghost programmal. Probléma esetén csak ezt a másolatot kell visszatölteni és visszaáll az eredeti állapot. Ez a megoldás kellő körültekintéssel használva nagyon gyors visszaállást tesz lehetővé, de nem szabad megfeledkezni a mentés óta történt változtatások (és biztonsági javítások!) feltöltéséről.

### **5. A hiba okainak felderítése**

Gyakori, hogy a normál üzem visszaállítása után szeretnénk kideríteni az okokat, vagy akár más lépésekre, pl. rendőrségi feljelentés is sor kerülhet. A fontosabb lépések:

- Készítsünk egy-az-egy másolatot a merevlemezekről! Erre alkalmas a Norton Ghost Windows alatt. Természetesen szükség van egy legalább akkora méretű lemezre, mint amelyről másolatot készítünk. A további vizsgáldást ezen a másolaton végezzük.
- Mentsük el, esetleg nyomtassuk ki a releváns napló állományokat! Gyakori, hogy a normál működés során a napló állományok előbb-utóbb felülíródnak, így a régebbiek elvesznek. Ezt meg kell akadályozni!
- Jegyezzünk fel minden fontos adatot (rendszerben futó programok, felhasználók, stb. listája).

## **VIII. VÍRUSVÉDELMI ELJÁRÁSOK**

### **1. Vírusvédelmi eljárások**

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

- a vírusvédelmi szoftvernek jó minőségűnek és kellő gyakorisággal aktualizáltnak (frissítettnek) kell lennie, hogy felismerési hatékonysága maximális legyen;

- a vírusvédelmi szoftvernek minden támadási ponton aktívan üzemelnie kell.

A szervezet egészére kiterjedően a vírusfertőzések megelőzése, kiszűrése és megszüntetése céljából korszerű vírusvédelmi szoftvert kell alkalmazni.

Szervezetünknel a használt vírusvédelmi szoftver az ESET NOD 32 Endpoint Security

A szoftver teljes számítástechnikai gépparkot lefedő (beleértve a mobil eszközöket is) telepítéséért, naprakész és folyamatos üzemeltetéséért, frissítéséért, a vírustámadások elleni védekezés megszervezéséért a rendszergazda 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 víruseszteszt 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.

## **2. A vírusvédelem szabályai a felhasználó részéről**

Biztosítani kell, hogy a szervezetnél alkalmazott vírusvédelmi rendszer a számítógépek működése közben folyamatosan dolgozzon, így a felhasználói munka során igénybe vett állományok (programok, adatok, dokumentumok) közvetlenül már a használat előtt vírusellenőrzése kerülnek. A számítástechnikai eszközökön beállított aktív védelmi 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 az informatikai munkatárs felé, aki feljegyezi a vírus és a fertőzött file nevét, továbbá a munkaállomás számát (helyét). Az informatikai munkatárs gondoskodik a vírus további terjedésének megakadályozásáról, és – amennyiben a felhasználói gépen futó program automatikusan nem törölte – a vírus szakszerű kiirtásáról.

## **3. Az elektronikus levelezés vírusvédelme**

Ha a szervezet elektronikus levelezési rendszerén keresztül fertőzött levél, vagy csatolt állomány érkezik, arról a víruskereső szoftver értesíti a felhasználót. 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.

## **IX. ELEKTRONIKUS CSATORNÁK HASZNÁLAT**

### **1. Internet Etikai Kódex**

Minden internet szolgáltatás előfizetőjének, igénybevevőjének az internet nemzetközi számítógépes hálózat használata során be kell tartania a hálózati viselkedés általános etikai szabályait. Az internethálózat olyan módon történő használata, amely sérti ezeket a szabályokat, az információkat szolgáltató-szervereken nyomon követhető és a szabályok be nem tartása az igénybevevő internet szolgáltatójának figyelmeztetését, illetve az internetből való kizárását, a szerződés egyoldalú – és azonnali – felmondását vonhatja maga után.

### **2. Internet használata**

A szervezeténél a munkatársak a saját gépeiken internet hozzáféréssel rendelkeznek. A bejelentkezés egyedi felhasználói azonosítóval, és jelszóval történik.

Az internet használatának elsődleges/kizárólagos célja a munkavégzés. A felhasználó nem jogosult magáncélra használni az internetet. A weben található tartalom egy része potenciális veszélyforrás. A veszélyes oldalak körét nem lehet behatárolni, de a felhasználó köteles távol tartani magát a pornográf, szerencsejátékot tartalmazó oldalaktól, valamint a közösségi-, videomegosztó- és blogoldalaktól.

### **3. E-mail használata**

Az e-mail használatának elsődleges/kizárólagos célja a munkavégzés. A felhasználó nem jogosult magáncélra használni a levelező rendszert. A szervezetnél kiosztott minden email cím a munkavégzést a szervezet ügyinek intézését szolgálja függetlenül attól, hogy egy-egy felhasználó személyéhez kötött az elnevezés. A munkáltató jogosult a email címmel és az ottani adatokkal minden egyéb műveletre is. A felhasználó munkavállaló nem jogosult a szervezet levelezését kívülre átirányítani.

A felhasználó nem jogosult a szervezet belső informatikai rendszerén kívüli helyszínen vagy helyszínről publikus eszközről, vagy publikus csatornán elérni leveleit, sem egyéb belső informatikai szolgáltatást, kizárólag a szervezet igényei szerint megfelelően védett eszközről, védett csatornán.

Biztonságos eszköz a saját otthoni, vagy mobil számítógép amennyiben a belső eszközökkel azonos védelmi eszközökkel rendelkezik, és nincs másik felhasználója. Nem biztonságos eszköz internet terminál, más cég, szervezet számítógépe.

A felhasználó nem jogosult a cégen kívüli levelezését elérni, csak úgy hogy a szervezet mail címére átirányítja a külső leveleket.

### **4. Mobil eszközök használata**

A mobil eszközök abból adódóan, hogy használatba kerülhetnek a belső védett környezetben kívül is, különös körülmények között igényelnek. A szervezet területén kívül a felhasználó felelős a mobil eszköz fizikai védelméért, lopás elleni védelméért, és a megfelelő környezetben való használatért. A mobil eszközt autóban hagyni, nyilvános helyen lopás lehetőségének kitenni tilos.

A mobil eszközt tilos úgy idegen hálózaton használni, hogy a felhasználó nem bizonyosodott meg az előírt adatvédelmi eszközök helyes működéséről a mobil eszközön.

X.

## ZÁRÓ RENDELKEZÉS

Ez a szabályzat 2014. június 1-jén lép hatályba.

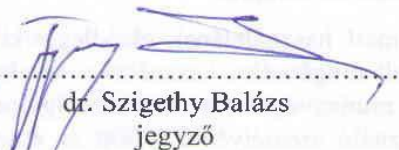
A szervezetnél a jegyző köteles gondoskodni arról, hogy e szabályzatot valamennyi munkatárs megismerje, és ennek tényét a szabályzathoz csatolt iven aláírásával igazolja a hatálybalépés napjával egyidejűleg.

Jelen szabályzat hatálybalépésével egyidejűleg minden korábbi, jelen szabályzattal azonos szabályozási tárgyú rendelkezés hatályát veszti.

A mellékletekben foglalt adatok változtatása nem minősül a szabályzat módosításának, de kizárólag a jegyző engedélyével történhet.

Dunaszeg, 2014. május 25.



  
dr. Szigethy Balázs  
jegyző













## 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.	Babos Attila	polgármester
2.	Lendvai Ivánné	polgármester
3.	Csontos Attila	polgármester
4.	dr. Szigethy Balázs	jegyző
5.	Ámont Henriett	igazgatási előadó
6.	Süle Tamásné	igazgatási előadó
7.	Márton Attila Tiborné	igazgatási előadó
8.	Reizingerné Klemm Erika Mária	adóügyi előadó
9.	Kiss Józsefné	pénzügyi-gazdálkodási előadó
10.	Bodó Tamásné	pénzügyi-gazdálkodási előadó
11.	Szabóné Süle Zita	pénzügyi-gazdálkodási előadó
12.	Tulokné Kovács Beatrix	pénzügyi-gazdálkodási előadó
13.	Stoller Ernőné	általános önkormányzati előadó
14.	Nagyné Sztítás Judit	ügykezelő
15.		
16.		
17.		
18.		
19.		
20.		
21.		
22.		
23.		
24.		
25.		
26.		
27.		
28.		
29.		
30.		



**Tárgy:** Közérdekű adatok megismerésére  
irányuló kérelem

*Címzett*

**Polgármesteri Hivatal / Államigazgatási Szervezet  
vezetőjének**

**Település**

*Tisztelt .....* !

Alulírott ..... kérem, hogy az információszabadságról szóló 2011. évi CXII. törvény alapján az általam készítendő egyetemi szakdolgozat témájához (a közigazgatási szervek szervezeti felépítése a települések lakosság számának arányában) kapcsolódóan kérem, hogy a Szervezeti és Működési Szabályzatát valamint a szervezetnél dolgozó köztisztviselők létszámát mint közérdekű adatokat tartalmazó dokumentumokat részemre másolatban – költségtérítés ellenében – 15 napon belül megküldeni szíveskedjen.

Kelt,....., 200...év.....hó.....nap

.....  
*aláírás*

## HOZZÁFÉRÉSI JOGOSULTSÁG

Sor-szám	Adatfeldolgozás megnevezése	Név	Beosztás
1.	Ügyirat nyilvántartás		Minden köztisztviselő /jegyző
2.	Közzolgálati alapnyilvántartás		Személyzeti ügyintéző/jegyző
3.	Illetmény		Pénzügyi ügyintéző/jegyző
4.	Helyi népesség nyilvántartás		Hatósági ügyintéző/jegyző
5.	Hatósági statisztika		Hatósági ügyintéző/jegyző
6.	Szabálysértési statisztika		Hatósági ügyintéző/jegyző
7.	Gyámügyi Statisztika		Gyámügyi ügyintéző/jegyző
8.	Vagyonnyilvántartás		Pénzügyi ügyintézők/jegyző

**IGÉNYLŐLAP**  
**közérdekű adat megismerésére irányuló kérelemhez**

**I. Az igénylő személy vagy szervezet\***

neve: \_\_\_\_\_

lakcíme/levelezési címe: \_\_\_\_\_

telefonszáma: \_\_\_\_\_

e-mail címe: \_\_\_\_\_

fax-száma: \_\_\_\_\_

**II. A kért közérdekű adat(ok) megjelölése:**

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

**III. Az adattovábbítás igénylő által megkívánt módja:**

\_\_\_\_\_

**IV. Az adatkérés időpontja:** \_\_\_\_\_

**V. Nyilatkozat:**

Alulírott igénylő nyilatkozom, hogy az adatigényléssel kapcsolatban felmerülő költségeket (fénymásolási, nyomtatási költség, adathordozó –papír, floppy, CD, DVD– költsége, munkaköltség, idegen nyelven benyújtott kérelem esetén a fordítás költsége) az önkormányzat által kiállított számla ellenében megfizetem; a befizetést igazoló csekkszelvényt, illetőleg az átutalási bizonylatot bemutatom.

\_\_\_\_\_  
Igénylő

## Szoftver Nyilvántartási Adatlap

A szoftvernyilvántartási adatlap a vállalkozás által használt szoftverek licencit tartalmazza, és egyben igazolja, hogy a vállalkozás az alább felsorolt szoftver licencek jogos felhasználója. A szoftver nyilvántartási adatlap felhasználható egy esetleges hatósági ellenőrzésnél a szoftver licencek eredetének igazolására, illetve a vállalkozás könyvelésében szereplő immateriális javak nyilvántartásának mellékletként.

### A SZERVEZET ADATAI

SZERVEZET NEVE: \_\_\_\_\_

CÍM : \_\_\_\_\_

CÍM : \_\_\_\_\_

A NYILVÁNTARTÁST VÉGZŐ NEVE: \_\_\_\_\_

A NYILVÁNTARTÁST VÉGZŐ E-MAIL CÍME: \_\_\_\_\_

### FELHASZNÁLÓ ADATAI

FELHASZNÁLÓ NEVE: \_\_\_\_\_

SZÁMÍTÓGÉP AZONOSÍTÓ \_\_\_\_\_

FELHASZNÁLÓI PROFIL \_\_\_\_\_

FELHASZNÁLÓ E-MAIL CÍME: \_\_\_\_\_

SZOFTVER GYÁRTÓJA	SZOFTVER NEVE ÉS VERZIÓSZÁMA	A SOFTVER SOROZATSZÁMA, AZONOSÍTÓJA	NYELV	TELJES LICENC VAGY FRISSÍTÉS	LICENCEK SZÁMA	LICENC KONSTRUKCIÓ	EREDETISÉGET IGAZOLÓ OKIRAT (SZÁMLASZÁM, SZERZŐDÉSSZÁM)	TELEPÍTÉS/UPGRADE DÁTUMA	TELEPÍTŐ/FRISSÍTŐ SZERVEZET

Kijelentem, hogy a jelen űrlapon általam megadott adatok helyesek, és a valóságnak megfelelően tükrözik a Szervezet szoftverállományának állapotát



