A Mórahalmi Polgármesteri Hivatal Adatvédelmi, Adatkezelési és Informatikai Biztonsági Szabályzata

2015.

I. Bevezetés

Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. Törvény (a továbbiakban: Isztv.) részletesen szabályozza a személyes adatok védelmével, és a közérdekű adatok nyilvánosságával kapcsolatos legfontosabb teendőket, illetőleg az alapvető jogok érvényesülését

Magyarország Alaptörvényének VI. cikk 82) bekezdése értelmében „Mindenkinek joga van személyes adatai védelméhez, valamint a közérdekű adatok megismeréséhez és terjesztéséhez". Ezen alapvető jogok védelme és tiszteletben tartása az állam és az önkormányzatok elsőrendű kötelessége.

A Mórahalmi Polgármesteri Hivatalának Adatvédelmi, Adatkezelési és Informatikai Biztonsági Szabályzatát az Isztv., Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. tv. (Ibtv.) 15. § (1) bekezdés d) pontja, a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992. évi LXVI. tv. (a továbbiakban: Nytv.), és az annak végrehajtására kiadott 146/1993. (X.26.) Korm. rendeletben, illetve a kutatás és a közvetlen üzletszerzés célját szolgáló név és lakcímadatok kezeléséről szóló 1995. évi CXIX. Törvényben foglaltak alapján, továbbá a Nytv. 30. § (1) bekezdésben kapott felhatalmazás alapján, az államháztartásról szóló 2011. évi CXCV. Törvény (a továbbiakban Áht), a Magyarország helyi önkormányzatairól szóló 2011. évi CLXXXIX. Törvény (a továbbiakban MÖtv.) alapján a Polgármesteri Hivatal (a továbbiakban: Hivatal) adatvédelemmel összefüggő feladatait és eljárási rendjét az alábbiak szerint szabályozom.

II. Általános szabályok

1. A szabályzat célja

A szabályzat célja, hogy biztosítsa a Mórahalmi Polgármesteri Hivatal (továbbiakban: Hivatal), és a Mórahalom városi Önkormányzat (továbbiakban: Önkormányzat) alkalmazottai által kezelt adatok vonatkozásában az adatbiztonság követelményeinek érvényesülését. Megakadályozza a jogosulatlan hozzáférést, az adatok megváltoztatását és jogosulatlan nyilvánosságra hozatalát.

A cél egyrészt biztosítani az alapvető jogok érvényesülését a Hivatalban folyó munkavégzés során, másrészt biztosítani az előírt feladatok ellátása keretében az adatvédelem szabályainak, valamint a lakosság tájékoztatására vonatkozó előírások betartását, továbbá eleget tenni az Isztv. 24. § (3) bekezdése szerinti kötelezettségnek, mely szerint az állami és Önkormányzati adatkezelőknek, e törvény végrehajtása érdekében, adatvédelmi és adatbiztonsági szabályzatot kell készíteniük, amely a polgárokat megillető és a jogszabályok által rögzített jogok érvényesülését biztosítja és meghatározza a Hivatal belső szervezeti egységei ezzel kapcsolatos kötelezettségeit.

A szabályzat célja továbbá, hogy az informatika alkalmazása során biztosítsa a Hivatalban az alábbiakat:

- az adat-, vagyon- és tűzvédelemre vonatkozó védelmi intézkedések betartását,
- az üzemeltetett számítógépek, informatikai eszközök valamint azok kiegészítő eszközeinek rendeltetésszerű használatát,
- a számítógépes rendszerek zavartalan üzemeltetését,
- az üzembiztonságot szolgáló karbantartást és fenntartást,
- az adatok számítógépes feldolgozása és azok további hasznosítása során az illetéktelen felhasználásból származó hátrányos következmények megszüntetését, illetve minimális mértékre csökkentését,
- az adatállományok tartalmi és formai épségének megőrzését,
- munkaállomásokon lekérdezhető adatok körének meghatározását,
- adatállományok biztonságos mentését,
- a feldolgozás folyamatát fenyegető veszélyek megelőzését, elhárítását,
- az adatvédelem és adatbiztonság feltételeit

2. A szabályzat hatálya

2.1 A szabályzat személyi hatálya

E szabályzat személyi hatálya a Hivatallal közszolgálati jogviszonyban álló vezetőkre, ügyintézőkre, valamint a munkaviszony keretében foglalkoztatott ügyviteli és fizikai alkalmazottakra, közszolgálati munkavállalókra terjed ki.
A személyes adatok védelméért, az adatkezelés jogszerűségéért a jegyző felelős.

2.2 A szabályzat tárgyi hatálya

E szabályzat tárgyi hatálya kiteljed:

- az Önkormányzat és a Hivatal tulajdonában lévő valamennyi számítástechnikai, informatikai berendezésre, valamint ezek műszaki dokumentációjára is;
- a rendszer- és felhasználói programokra;
- a védelmet élvező adatok teljes körére, felmerülésük és feldolgozási helyüktől, idejüktől és az adatok fizikai megjelenési formájától függetlenül;
- az adatok felhasználására, tárolására vonatkozó utasításokra;
- az adathordozók tárolására, felhasználására;
- valamint a számítástechnikai folyamatban szereplő összes dokumentációra (fejlesztési, szervezési, programozási, üzemeltetési dokumentáció).

A szabályzat előírásait alkalmazni kell a Hivatal belső szervezeti egységei által vezetett nyilvántartások, adatbázisok és valamennyi egyedileg kezelt adat, elektronikus szolgáltatások illetőleg dokumentumok esetében. A Hivatalban nyilvántartott adatokat védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, nyilvánosságra hozatal, sérülés, törlés vagy megsemmisülés ellen.

Iratokat, adatokat a munkaköri feladat ellátásán kívül a munkahelyről kivinni, a munkahelyen kívül feldolgozni, tárolni csak a jegyző egyetértésével lehet, azzal a feltétellel, hogy az irat, adat tartalmát illetéktelen személy nem ismerheti meg.

Az iratok tárolása, kezelése során fokozottan ügyelni kell arra, hogy illetéktelen személyek ne ismerhessék meg azok tartalmát. A munkavégzés céljára szolgáló irodákat távozáskor kulcsra kell zárni. Az irodahelyiségek nyitva tartása miatti illetéktelen hozzáférés esetén az érintett fegyelmi felelősséggel tartozik.

3. A Mórahalmi Polgármesteri Hivatal osztályba és szintbe sorolása

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény 9. § (2) bekezdése szerint az önkormányzatok biztonsági szintje a szervezet elektronikus információs rendszereinek legmagasabb biztonsági osztályával azonos besorolású, de legalább 2.

Az elvégzett vizsgálatok alapján megállapítható, hogy a Mórahalmi Polgármesteri Hivatal elektronikus információs rendszere védelmének elvárt, illetve jelenlegi erőssége, a szervezet felkészültsége a meghatározott biztonsági feladatok kezelésére a 2-es osztálynak és szintnek megfelelő besorolású, megfelelve ezzel a vonatkozó jogszabályi előírásoknak.

4. A hálózat rövid ismertetése

Az intézményben található kliens számítógépek csavart érpáras UTP kapcsolattal csatlakoznak a helyi szerverhez. A PC-k és a központi szerver közötti hálózati kapcsolatot Windows 2000 kompatibilis hálózati szoftver biztosítja. A Polgármesteri Hivatal optikai kapcsolaton csatlakozik az Internethez, melynek sebessége 10/10 Mbit/sec.

A hálózaton központi szerver üzemel, amely 45 PC számára biztosítja az adatbázisok elérését.

5. Az Informatikai Biztonsági Szabályzat karbantartása, a védelmet igénylő adatok és információk osztályozása, minősítése, hozzáférési jogosultság

Az IBSZ-t az informatikában - valamint a Hivatalnál - a fejlődés során bekövetkező változások miatt időközönként aktualizálni kell.

Az IBSZ folyamatos karbantartása az informatikus tevékenységén keresztül a jegyző feladata.

Az adatokat és információkat jelentőségük és bizalmassági fokozatuk szerint osztályozzuk:
– közlésre szánt, bárki által megismerhető adatok,
– minősített, titkos adatok.

Az adatok feldolgozásakor meg kell határozni írásban és névre szólóan a hozzáférési jogosultságot. A kijelölt dolgozók előtt az adatvédelmi és egyéb szabályokat, a betekintési jogosultság terjedelmét, gyakorlási módját és időtartamát ismertetni kell.

Alapelv, hogy mindenki csak ahhoz az adathoz juthasson el, amire a munkájához szüksége van.

Az információhoz való hozzáférést lehetőség szerint a tevékenység naplózásával dokumentálni kell, ezáltal bármely számítógépen végzett tevékenység – adatbázisokhoz való hozzáférés, a fájlba vagy mágneslemezre történő mentés, a rendszer védett részeibe történő illetéktelen behatolási kísérlet – utólag visszakereshető.

A naplófájlokat rendszeresen át kell tekinteni, s a jogosulatlan hozzáférést vagy annak a kísérletét a Hivatal vezetőjének azonnal jelenteni kell.

A naplófájlok áttekintéséért, értékeléséért a rendszergazda a felelős.

Az adatok védelmét, a feldolgozás – az adattovábbítás, a tárolás - során az operációs rendszerben és a felhasználói programban alkalmazott logikai matematikai, illetve a hardver berendezésekben kiépített technikai megoldásokkal is biztosítani kell (szoftver, hardver adatvédelem).

III. Értelmező rendelkezések

1) Adat: a természetes vagy mesterséges objektumok, folyamatok, állapotok jellemzői illetőleg azok részleteinek érzékelhető formában történő megjelenítése. Adat tágabb értelemben jelenthet szöveget, számot, rajzot, térképi részleteket vagy bármely más információt a megjelenési módjára vagy formájára való tekintet nélkül.

2) Adatállomány: az egy nyilvántartásban kezelt adatok összessége.

3) Adatkezelés: az alkalmazott eljárástól függetlenül adatokon végzett bármely müvelet vagy műveletek összessége, így például az adatok gyűjtése, felvétele, rögzítése, tárolása, felhasználása, összekapcsolása, szolgáltatása, megjelenítése, stb.

4) Adatkezelő: az a belső szervezeti egység, amely a személyes, illetőleg a közérdekű adatok körébe tartozó adatok, dokumentumok kezelését, szolgáltatását ellátja.

5) Adatmegsemmisítés: az adatokat tartalmazó adathordozó teljes fizikai megsemmisítése.

6) Adatközlő: az a belső szervezeti egység, amely az adatfelelős által szolgáltatott adatokat a jogszabályokban meghatározott módon közzéteszi.

7) Adatszolgáltatás a polgárok személves adataiból: a nyilvántartásban szereplő polgárok adatainak a törvényben meghatározott tartalmú és terjedelmű közlése. Ezen belül:
   - egyedi adatszolgáltatás: egy polgár adatainak közlése;
   - csoportos adatszolgáltatás: az adatigénylő által vagy jogszabályban meghatározott szempontok szerint képzett csoportba tartozó polgárok adatainak rendszeres vagy eseti közlése.

8) Adattovábbítás: az adatot meghatározott személy számára történő hozzáférhetővé tétele.

9) Adatvédelem: az adatokhoz való illetéktelen hozzáférés, a meghibásodás, a megsemmisülés, stb. megakadályozása; a személyes adatok esetében kiegészül az adott személy személyes adatai jogellenes gyűjtése, kezelése, tárolása, felhasználása elleni védelemmel.

10) Adattörlés: az adatok felismerhetetlenné tétele olya módon, hogy a helyreállításuk többé nem lehetséges.

11) Információ: jelentéssel bíró adat megjelenési módjára vagy formájára való tekintet nélkül.

12) Kötelezően közzéteendő közérdekű adat: az Isztv 26. § (2) - (3) bekezdésében meghatározott körbe tartozó adat.

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

14) 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 személye 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;

15) Különleges adat: a faji eredetre, nemzetiséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdek-képviseleti szervezeti tagságra, a szexuális éltre vonatkozó személyes adat, továbbá az egészségi állapotra, a kóros szenvedélyre vonatkozó személyes adat, valamint a bűnügyi személyes adat;

16) Nyilvánosságra hozatal: az adat bárki számára történő hozzáférhetővé tétele.

17) 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).

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

19) 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;

20) Elektronikus tájékoztató szolgáltatás (tájékoztatás): az elektronikus közigazgatási szolgáltatás körén kívüli ügyintézésről elektronikus úton hozzáférhetővé tett általános jellegű információs szolgáltatás.

21) Interaktív szolgáltatás: az egyszerű tájékoztatáson túlmenően olyan szolgáltatás (például letölthető űrlapok, kereső rendszerek, tematikus tájékoztatók), amely csak a használó aktivitását igényli, a szolgáltatást nyújtó szerv által előkészített dokumentumok kitöltéséhez, felhasználásához.

22) alkalmazói program (alkalmazói szoftver): olyan program, amelyet az alkalmazó saját speciális céljai érdekében vezet be, és amely a hardver és az üzemi rendszer funkcióit használja;
23) felhasználó: az a személy (vagy szervezet), aki (amely) egy vagy több informatikai rendszert használ feladatai megoldásához;

24) felhasználói jog: az a jogosultság a hálózaton, amely a felhasználó számára szükséges és elégséges munkájának elvégzéséhez;

25) gépterem (iroda): az a helyiség, amelyben a Hivatal dolgozói hozzáférhetnek a számítástechnikai eszközökhöz és szolgáltatásokhoz;

26) hálózat: két vagy több számítógép összekapcsolása, amely informatikai rendszerek legkülönbözőbb komponensei között adatcserét tesz lehetővé;

27) hardver: az informatikai rendszer eszközeit, fizikai elemeit alkotó része;

28) informatika: a számítógépes információrendszerek tudománya, amely elméletet, szemléletet és módszertant ad a számítógépes információrendszerek tervezéséhez, fejlesztéséhez, szervezéséhez és működéséhez;

29) informatikai biztonság: olyan előírások, szabványok betartásának eredménye, amelyek az információk elérhetőségét, sérthetetlenségét és bizalmasságát érintik, és amelyeket az informatikai rendszerek vagy komponenseik alkalmazása során biztonsági megelőző intézkedésekkel lehet elemi;

30) munkaállomás: egy operátor vagy felhasználó számára, adott típusú feladathoz felszerelt számítógép vagy terminál;

31) rack szekrény: üvegezett, biztonságos fém szekrény, amelyben hálózati eszközöket, szervereket üzemeltetnek;

32) rendszerprogram (rendszer szoftver): olyan alapszoftver, amelyre szükség van, hogy valamely informatikai rendszer hardvereit használhassuk és az alkalmazói programokat működtethessük. A rendszerprogramok legnagyobb részét az operációs rendszerek alkotják.

33) szerver: olyan hálózatra kapcsolt központi szerepet betöltő számítógép, amelynek alapvető feladata, hogy más, a hálózatra kapcsolt számítógépek vagy terminálok számára az erőforrásait megossza;

34) szerverszoba: az a légkondicionált, biztonsági berendezésekkel ellátott helyiség, ahol a szerverek vannak, és csak a kijelölt köztisztviselők regisztrálás után juthatnak be;

35) vírus: önállóan nem működő programrész, amely illegálisan készült egy felhasználói program részeként. A felhasználói program alkalmazása során átterjedhet más, az informatikai rendszerben lévő rendszer- illetve felhasználói programra, sokszorozva önmagát és egy beépített feltételhez kötötten (pl. konkrét időpont) pusztítást indít el.

IV. Az adatkezelés, az adatvédelem követelmény rendszere

4.1. A Hivatal belső szervezeti egységei

a) szakmai feladataik ellátása során kizárólag az adott feladat, a tevékenység megítélése, az adott döntés előkészítése érdekében, a vonatkozó jogszabályok rendelkezései alapján feltétlenül szükséges - és a személyes adatok körébe tartozó - adatok gyűjtését, tárolását, rendezését, felhasználását, nyilvánosságra hozatalát, archiválását, irattározását, stb. láthatják el;
b) a képviselő-testület, a bizottságai, valamint a Hivatal tevékenységének átláthatóbbá tételét szolgáló, illetőleg a jogszabályok által közérdekűnek - nyilvánosnak - minősített adatok kezelését, majd ezek közzétételét kötelesek biztosítani.

Az adatkezelőt fokozott felelősség terheli az adatok jogszabályszerű kezeléséért és szolgáltatásáért.
E szabályzatot a Polgármesteri Hivatal

- Szervezeti és Működési Szabályzatával,
- Közérdekű adatközlési és közzétételi szabályzatával

4.2. Az adatvédelem tárgya

Az adatvédelem folyamatában a védelem tárgya:

a) a Hivatal működése során keletkezett személyes és közérdekű adatok teljes köre, keletkezésüktől a megsemmisítésükig,
b) az adathordozók fizikai jellegüktől függetlenül, amelyek személyes, illetőleg közérdekű adatokat tartalmaznak. Az adathordozók lehetnek papír alapú iratok, kimutatások, listák, térképek, műszaki dokumentációk, mágneses adathordozók, informatikai rendszerek, hardver, szoftver
c) az a fizikai környezet, ahol az adatállomány kezelése, tárolása történik.

4.3. Az adatkezelés alapkövetelményei

Az önkormányzati feladatok ellátása során az adott feladat szerinti ügymenet részeként biztosítani kell az adatkezelés szabályainak a maradéktalan betartását, a természetes személyek adatainak védelmét a jogellenes felhasználástól.

Az adatkezelés során biztosítani kell:

a) az adott egyén szempontjából fontos adatok helyes, pontos kezelését. A hibás adat előfordulása esetén annak észlelésekor hivatalból, valamint az érintett kezdeményezésekor a pontosítást haladéktalanul teljesíteni kell;

b) az adott személy adatai kizárólag a jogszabály rendelkezéseivel összhangban kerüljenek feldolgozásra, rögzítésre, felhasználásra, illetőleg ne kerüljenek illetéktelenek birtokába;

c) a személyes adatoknak a közérdekű adatokkal való együttes alkalmazásuk esetén nem akadályozhatják a közérdekű adatok nyilvánosságát, szolgáltatását;

d) a különböző célú adatok, adatállományok (adatbázisok) folyamatos vezetését, aktualizálást és az adathordozó fajtájától független folyamatos rendelkezésre állását és elérhetőségét az arra jogosultak számára. A személyes adatok tekintetében minden esetben biztosítani kell a zárt kezelést és a jogszabályok szerinti előírásoknak megfelelő hozzáférést;

e) a különböző adatok, adatállományok (adatbázisok) valódiságát, pontosságát, részletességét, hitelességét;

f) a különböző adatok, adatállományok (adatbázisok) jellegétől függően azok bizalmas, illetőleg az adott területre vonatkozó jogszabályok szerinti kezelését. A pályázatok, ajánlatok elbírálásáig azok tartalmának zárt - nem nyilvános - kezeléslét;

g) a Hivatal gondozásában készült információs rendszerek, adatbázisok folyamatos működését, és szükség szerinti folyamatos hozzáférés lehetőségét, a folyamatos aktualizálást, a közérdekű adatok folyamatos a jogszabályoknak megfelelő szolgáltatását, az érdeklődők véletlenszerű internet állásának a garantálását;

h) az adatrendszer (akár számítógépes, akár manuális) fizikai biztonságát. Az adatok és az adathordozó eszközök összességében jelentős értéket képviselnek. Megsemmisülésük esetén újra előállításuk többletmunkát és költséget igényel.

4.4 Az adatvédelem eszközei

Az adatvédelem eszközeiként kell kezelni és folyamatosan biztosítani mindazon igazgatási, iratkezelési, szervezési, személyi, műszaki, technikai, informatikai és egyéb intézkedéseket, melyek elengedhetetlenek az egyes adatok, adatállományok (adatbázisok) zavartalan működéséhez, és védelmet nyújtanak ahhoz, hogy

a) illetéktelenek ne jussanak a különböző személyes adatokhoz (személyes adatokat tartalmazó adatbázisokhoz), dokumentumokhoz,

b) a különböző adatok (adatbázisok) dokumentumok megsérülésére, meghibásodására ne kerüljön sor,

c) az adatkezelés során ismeretek hiánya, hozzá nem értés miatt, emberi mulasztásból károsodásra, adatok, dokumentumok megsemmisülésére ne kerüljön sor.

4.5. Személyi feltételek biztosítása

A személyes adatok kezelésével kapcsolatos teendőket csak a Hivatal illetékes belső szervezeti egység e feladattal megbízott ügyintézői látnak el. A folyamatos ügyintézés érdekében a megfelelő helyettesítésről gondoskodni kell. A közérdekű adatok folyamatos szolgáltatása érdekében a feladatkör szerint illetékes belső szervezeti egység vezetője felelős a szakterületet jól ismerő és az elektronikus adatkezelésben, tájékoztatásban jártas személy(ek) kijelöléséért.

A jelen szabályzatban foglaltak szakszem végrehajtásáról a Hivatal adatvédelmi, illetve informatikai biztonsági felelősének kell gondoskodnia. Az adatvédelmi, illetve informatikai biztonsági felelősi feladatok ellátásával megbízott köztisztviselő a hivatal informatikusa, feladatait az Isztv. 24 § (2) és az Ibtv. 13. § (2) bekezdése tartalmazza

A Hivatal informatikusa végzi az informatikai védelmi rendszer biztosítását, a vírusvédelmi szoftverek frissítését, valamint biztosítja a rendszer üzemképességét, és a műszaki ellátást, biztonsági másolatot készít, segíti, ellenőrzi a Hivatal dolgozóinak számítástechnikai munkáját.

4.6. Fizikai, technikai védelem

4.6.1. Tűzvédelem

A szerverszoba, illetve az informatikai eszközöket tartalmazó irodák a "D" tűzveszélyességi osztályba tartoznak, amely mérsékelt tűzveszélyes üzemet jelent.
A szerverszobára vonatkozó tűzvédelem feladatait, sajátos előírásait „A Polgármesteri Hivatal tűzvédelmi szabályzata" tartalmazza.

4.6.2. Vagyonvédelem, fizikai biztonság

- a szerverszobát, irodákat biztonsági zárakkal kell felszerelni;
- a szerverszobába való be- és kilépés rendjét szabályozni kell;
- a szerverszoba kulcsát az adatvédelmi felelős és/vagy a hivatali informatikus tárolja, onnan csak az arra feljogosítottak vehetik fel;
- munkaidőn túl az irodákban, illetve a szerverszobában csak engedéllyel lehet tartózkodni;
- a szerverszobába történő illetéktelen behatolás tényét a jegyzőnek azonnal jelenteni kell;
- az irodahelyiségekben elhelyezett számítástechnikai eszközöket csak a kijelölt köztisztviselők, illetve alkalmazottak használhatják;
- a számítástechnikai eszközök rendeltetésszerű működéséért a felhasználó felelős.

4.6.3. Adathordozók védelme, tárolása, hordozása és karbantartása

a munkaasztalon csak azok az adathordozók lehetnek, amelyek az aktuális feldolgozáshoz szükségesek;
- az adathordozókat jól zárható szekrényben kell elhelyezni úgy, hogy tárolás közben ne sémijének, károsodjanak;
- az adathordozókat a gyors hozzáférés érdekében azonosítóval kell ellátni;
- az adathordozók nyilvántartásában az azonosító adaton kívül a felírás és megőrzés dátumát, a védettség tényét, a jogosultsági és illetékességi adatokat, valamint az adathordozó kiadására és visszavételezésére vonatkozó információkat kell feltüntetni;
- az adathordozók szállítása csak megfelelő módon kialakított fémdobozban történhet;
- adathordozót más intézménynek átadni csak az adatvédelmi felelős engedélyével lehet;
- az adathordozók megőrzésének idejét, ha másképp nincs rendelkezés, a felelős vezető határozza meg;
- az adathordozókat félévenként ellenőrizni és tisztítani kell;

- olyan adathordozót, amelyet javíthatatlan fizikai károsodás ért, selejtezni kell. Selejtezendő:
    a) a fizikailag sérült javíthatatlan;
    b) gyári, raktározási hibát követően felhasználásra alkalmatlan (deformálódott);
    c) ha a kapacitás a névleges érték 75%-ánál kevesebb;
    d) véglegesen elhasználódott adathordozót.

Az alkalmatlan adathordozókat fizikai roncsolással használhatatlanná kell tenni. Bizalmas adatokat, felhasználói és rendszerprogramokat tartalmazó adattárolókról törlő program segítségével kell az adatokat törölni, vagy fizikailag kell megsemmisíteni az adathordozót.

A selejtezést a Selejtezési Szabályzatnak és a hivatali Iratkezelési Szabályzatának megfelelően kell lefolytatni, Az adathordozókat a Leltározási Szabályzatnak megfelelően kell leltározni.

4.6.4. Adatvédelemi feladatok:

- az adatbevitel hibátlan műszaki állapotú berendezésen történhet;
  csak hibátlan adathordozóra lehet adatállományt rögzíteni;
- adatrögzítő szoftver védelme: a programokat, adatokat ellenőrző funkciókkal, amennyiben szükséges titkosítással kell ellátni;
- a bejelentkezési azonosítók használatával kell szabályozni, hogy ki milyen hozzáférési szinten férhet hozzá a programokhoz és adatokhoz (alapelv: a tárolt adatokhoz csak az illetékes szervezeti egységek személyei férjenek hozzá);
- az adatok bevitele során alapelv: azonos állomány rögzítését és ellenőrzését ugyanaz a személy nem végezheti.

Az adatállományok file-védelme során gondoskodni kell arról, hogy azok ne károsodjanak. A fontosabb file-okat tartalmazó adattárolókról másolatot kell időnként készíteni. A másolt lemezek csak az illetékes vezető engedélyével adhatók ki.

4.6.5. Vírusvédelem

A munkaállomásokon és szervereken, ha másképp nincs rendelkezés, heti rendszerességgel vírusellenőrzést és vírusirtást kell tartani.

A vírusvédelmi programok adatbázisát naprakészen kell tartani.

Vírusfertőzés okozta hiba gyanúja esetén azonnal szólni kell az illetékes szakembernek, informatikusnak. Amennyiben nincs erre lehetőség (pl. munkaidőn kívül), a feldolgozásban lévő adatokat el kell menteni, majd a programból kilépve a gépet ki kell kapcsolni. A gépet addig bekapcsolni nem szabad, amíg azt az arra illetékes szakember, informatikus meg nem vizsgálta. A vírusfertőzést jelenteni kell a szervezeti egység vezetőjének, még akkor is, ha semmi hiba nem történt a fertőzés folyamán, valamint a szervezeti egység vezetőjének ki kell deríteni a fertőzés lehetséges okait, és a szükséges védelmi intézkedést meg kell hoznia.

4.6.6. Szoftvervédelem

Az üzemeltetésért felelős informatikusnak biztosítani kell, hogy a rendszerszoftver naprakész állapotban legyen és a segédprogramok, programkönyvtárak mindig hozzáférhetők legyenek az illetékes felhasználók számára.

Rendszerszoftver védelem:

a) a rendszerszoftver módosításához az illetékes engedélye szükséges;
b) a módosítással egy időben a dokumentációban is át kell a változtatásokat vezetni;
c) a rendszerszoftver-eseményekről és a változtatásokról nyilvántartást kell vezetni (eseménynapló).

Programhoz való hozzáférés, programvédelem:

a) A kezelés folyamán az illetéktelen hozzáférést és próbálkozást ki kell zárni.
b) Gondoskodni kell arról, hogy a tárolt programok, adatállományok ne károsodjanak, a követelményeknek megfelelően működjenek
c) A feldolgozás biztonságának megvalósításához naprakész állapotban kell tartani a program dokumentációt.

A programoktól nyilvántartást kell vezetni, amelynek az alábbi adatokat kell tartalmaznia:

a) a program azonosítója;
b) a program készítőjének neve;
c) a feldolgozási rendszer megnevezése.

Programok megőrzése, nyilvántartása:

a) a programokról naprakész nyilvántartást kell vezetni;
b) a nyilvántartásból egyértelműen megállapíthatónak kell lennie a program azonosítására és kezelésére vonatkozó adatok.

Programok fizikai védelme:
A védelem érdekében a felhasználás helyétől elkülönítetten, behatolástól védetten egy-egy duplikált példányt kell tárolni.

4.6.7. Hardver védelem

- A számítógépeket óvni kell folyadéktól, túlzott páratartalomtól és hőigény bevételtől;
- a számítógép közelében ételt és italt fogyasztani tilos;
- a szerverszobában klímaberendezés használata ajánlott;
  szervereknél biztosítani kell a szünetmentes feszültségforrást és rack szekrényben vagy szerverszobában kell elhelyezni;
- a számítógép-hálózat csatornáit lehetőség szerint külön kábelcsatornában kell vezetni, melyre jól látható helyekre rá kell írni a hálózat típusát;
- a fali csatlakozók megbontása szigorúan tilos;
- csak földelt aljzatokat lehet használni számítógép üzemeltetéséhez;
- a lengő kábeleket úgy kell elhelyezni, hogy azok balesetet ne okozhassanak, alapelv: sűrűn használt utat szabadon kell hagyni;
- a számítógépek belsejébe nyúlni, és ott bárminemű változtatást okozni tilos, csak az illetékes szakember (hivatali informatikus), illetve a szervizek szakemberei nyúlhatnak bele;
- havi rendszerességgel a számítógépeken hardver teszteket kell lefuttatni.

4.7. Informatikai védelem

1. A szerverszobában a hivatali informatikuson, valamint az informatikai rendszer üzemeltetését végző gazdálkodó szervezet munkatársán kívül más nem tartózkodhat. Más személyek benntartózkodását a szervezeti egység vezető engedélyezheti.

2. Üzemidőn kívül az ajtókat zárva kell tartani. A szerverszoba kulcsát a hivatali informatikus tárolja, onnan csak az arra feljogosítottak vehetik fel. Munkaidőn kívül idegen személy csak felügyelet mellett tartózkodhat a gépteremben. A szerverszoba áramtalanításáért a hivatali informatikus a felelős.

3. Az irodákban/szerverszobában a folyamatos, higiénikus munkavégzés feltételeit kell megőrizni. A szerverszobai rend megtartásáért és a biztonságos műszaki üzemeltetésért a hivatali informatikus a felelős.

4. A szerverszobába ételt, italt bevinni és ott elfogyasztani szigorúan TILOS!

5. A szerverszobába égő cigarettával belépni és ott dohányozni, valamint tüzet okozó tevékenységet folytatni szigorúan TILOS!

6. A szerverszoba takarítását csak a hivatali informatikus felügyelet mellett, legalább havonta egyszer, a kijelölt személyek végezhetik.

7. A berendezések belsejébe nyúlni TILOS! Bármilyen nem a gépkezeléssel összefüggő beavatkozást csak a hivatali informatikus és a szervizek szakemberei végezhetnek.

8. A számítógépeket csak rendeltetésszerűen és az ütemezett munkák elvégzésére lehet használni. Tilos a számítógépeken játszani, illetve az informatikai rendszer biztonságát veszélyeztető tevékenységet végezni.

9. Adathordozókat csak a hivatali informatikus engedélyével lehet be- és kivinni a szerverszobából.

10. Az elektromos hálózatba más - nem a rendszerekhez, illetve azok kiszolgálásához tartozó - berendezéseket csatlakoztatni nem lehet.

11. A számítógép javításoknak, illetve bármilyen beavatkozásoknak minden esetben ki kell elégíteni a szükséges műszaki feltételeken kívül a balesetmentes használat, a szakszerűség, a vonatkozó érintésvédelmi szabályok és az esztétikai követelményeket. Nem végezhető olyan javítás, szerelés, átalakítás vagy bármely beavatkozás, amely nem elégíti ki a balesetvédelmi előírásokat. A fenti rendelkezések megsértése esetén az elkövetővel szemben az adatvédelmi felelős fegyelmi felelősségre vonást kezdeményezhet

12.Védelmi előírások:

- A számítógépeket csak indítójelszóval lehessen elindítani, az indítójelszavat 30 naponta meg kell változtatni;

induláskor minden esetben vírus-ellenőrző programot kell elindítani;

- a feldolgozáshoz szükséges programok elindításához és az adatok hozzáféréséhez jelszóvédelem kell.
- Az egyes szakági rendszerek felhasználói csak jelszavas azonosítást követően léphetnek be a rendszerbe. A felhasználói névnek és a jelszónak minden esetben egyedinek kell lennie.
  Minden esetben a jelszavaknak különbözniük kell.
- A bizalmas adatállományokat és dokumentumokat titkosítani kell, a titkosítás végezhető az adott szoftverrel, vagy külső programmal is.
- A módosításokról napi mentést kell készíteni, ezeket a heti mentésekig kell megőrizni;
- a teljes anyagról heti mentéseket kell készíteni;
- a teljes anyagról a tárgyévet követő év első munkanapján mentést kell végezni és ezt a 3. számú mellékletben meghatározott módon kell megőrizni. Ezeket a törvényekben meghatározott ideig kell megőrizni (pl. adótörvény, társadalombiztosítási törvény, számviteli törvény).
- A felhasznált programokról biztonsági másolatot kell készíteni, és azokat az eredeti példánytól külön, tűzbiztos helyen kell tárolni.

V.
Hivatali hálózathasználat szabályai

5.1. A hálózat használatának szabályai:

A hivatal hálózata nem használható az alábbi tevékenységekre:

- a hálózat, a kapcsolódó hálóztok, illetve ezek erőforrásainak rendeltetésszem működését és biztonságát zavaró, veszélyeztető tevékenység, ilyen információknak és programoknak a terjesztése
- a hálózatot, a kapcsolódó hálózatokat, illetve erőforrásokat indokolatlanul igénybe vevő tevékenységek
- a hálózat erőforrásaihoz, a hálózaton elérhető adatokhoz történő illetéktelen hozzáférés, azok illetéktelen használata, gépek/szolgáltatások - akár tesztelés céljából történő - túlzott mértékben való szisztematikus próbálgatása
- a hálózat erőforrásainak, a hálózaton elérhető adatoknak illetéktelen módosítása, megrongálása, megsemmisítése, vagy bármely károkozásra irányuló tevékenység
- hálózati üzenetek, hálózati eszközök hamisítása: olyan látszat keltése, mintha egy üzenet más gépről vagy más felhasználótól származna

5.2. Felelősök

A rendszergazda kontrollálja a hálózat egyes részeinek, szolgáltatásainak működését, rendeltetésszem és szabályos használatát, valamint felel a biztonsági előírások betartásáért és betartatásáért.

5.3. A felhasználók kötelességei:

- a felhasználók kötelessége a szabályzat megismerése és az abban foglaltak betartása, valamint együttműködés a hálózat üzemeltetőjével a szabályzat betartása érdekében

a felhasználó viseli a felelősséget minden műveletért, amely az adott felhasználó azonosítóval kerül végrehajtásra.

5.4. A felhasználók jogai:

- Minden hivatali dolgozónak joga van saját felhasználói fiókhoz és levelezéshez (e-mail címhez) és a munkavégzéshez szükséges web szolgáltatáshoz
- A felhasználó személyiségi jogait és a levéltitkot a hálózat üzemeltetője tiszteletben tartja, ettől eltérni csak jogszabály által meghatározott esetekben lehet
- A rendszer technikai karbantartásairól tájékoztatni kell a felhasználókat, hogy kellő idő maradjon a felhasználók felkészülésére. A karbantartásokat lehetőleg hivatali munkaidőn kívül kell lebonyolítani.

5.5. A felhasználók regisztrálásának szabályai:

- Felhasználó a hivatal, önkormányzat dolgozója lehet.
- A felhasználói azonosítók kiadása központilag a felelős rendszergazda által történik
- A felhasználót az azonosító átadásakor tájékoztatni kell a használat feltételeiről és szabályairól. A tájékoztatást követően a felhasználó aláírásával igazolja, hogy azokat megismerte és magára nézve kötelezőnek ismerte el.
- Szakrendszerhez kapcsolódó felhasználói azonosító átadását megelőzően a felhasználót oktatásban kell részesíteni annak használatáról.
- A felhasználói azonosítót le kell tiltani, ha azzal visszaélés történt és az esetet ki kell vizsgálni
- A felhasználó azonosítókat a rendszerből törölni kell, ha felhasználó már nem hivatal dolgozója, illetve az adott rendszer használatához már nincs joga. A törlést az érintett szervezeti egység vezetője kezdeményezi a rendszergazdánál
- A rendszergazda a felhasználói azonosítókról és kapcsolódó hozzáférési jogosultságokról teljes köm és naprakész nyilvántartást vezet. A nyilvántartásnak tartalmaznia kell azon felhasználói azonosítókat és kapcsolódó jelszavakat, hozzáférési jogosultságokat, amelyek más, nem a Hivatal rendszeréhez tartoznak, de valamely feladat kapcsán a Hivatal vagy a Hivatal dolgozója hozzáférést igényelt, kapott ahhoz (pl pályázati rendszerhez történő hozzáférés, hivatali kapuhoz történő hozzáférés) A nyilvántartásba vételt az érintett szervezeti egység vezetője írásban kezdeményezi.

5.6. Szankciók:

A szabályzat megsértésnek gyanúja esetén az esetet ki kell vizsgálni és a kijelölt felelősnek meg kell tennie a szükséges intézkedéseket, amelyre a következőek az irányadók:

- a szabályzat gondatlan megszegése esetén az elkövetőt szóbeli figyelmezetésben kell részesíteni
- a szabályzat szándékos megszegése esetén az elkövetőt írásbeli figyelmeztetésben kell részesíteni és köteles megtéríteni az általa okozott károkat a Ptk előírásai szerint.

5.7. Közzétételi feladatok ellátása:

Közzétételt megvalósító személy: informatikus.

Közzétételt elrendelni jogosult személyek: polgármester, jegyző, kabinetvezető.

A közzététel elrendelésére jogosultak által jóváhagyott és megjelent intézményi vagy egyéb hírek, cikkek, közlemények, sajtóanyagok közvetlenül is közzétehetőek, átemelhetőek.

Közzététel elrendelése email útján, vagy kivételes esetekben szóbeli utasítással történhet.

VI. A jelszókezelés szabályai

6.1. A jelszó a hozzáférés kezelés alapvető eszköze, így az informatikai biztonság fontos része. Az informatikai rendszer minden felhasználójának tisztában kell lennie a jelszó fontosságával és a nem megfelelő jelszókezelés következményeivel, mivel egy rosszul megválasztott, könnyen kitalálható jelszó nemcsak a tulajdonosára, hanem a Hivatal informatikai rendszerére is negatív következményekkel járhat.

6.2. Alapelvek:

- Nem szabad könnyen kitalálható jelszavakat választani
  A jelszavakat titokban kell tartani
- Az induló jelszót első bejelentkezéskor meg kell változtatni
  Ha a felhasználónak gyanúja támad, hogy a jelszava kompromittálódott, azonnal meg kell változtatnia
- A jelszavakat nem szabad kódolatlanul tárolni

6.3. Helyes jelszóválasztás:

- nem szabad könnyen kitalálható, személyre jellemző jelszavakat használni
- nem szabad sorozatokat használni (pl abcdefg, 7654321 stb)
- kerülni kell a szótári szavak használatát
- a jelszó tartalmazzon kis és nagybetűket, számokat

6.4. Jelszóvédelem

A felhasználóknak különös figyelmet kell, hogy fordítsanak az alábbiakra:

- a jelszót tilos másoknak elmondani, mások előtt a jelszóról beszélni
- a jelszót a felhasználón kívül kizárólag a rendszergazda ismerheti
- tilos közös jelszavakat használni
- a jelszót nem szabad elérhető helyen tárolni, telefonon, e-mailben továbbítani
- a jelszót tilos kérdőívbe, űrlapokba beírni

VII. A távoli elérés szabályai

7.1. A Hivatal hálózatának távoli elérésére az egyes munkaállomások távoli elérésének keretében van lehetőség (titkosított terminál kapcsolat).

7.2. A távoli elérések szabályai:

- A bejelentkezés időtartamára a felhasználóra kötelezőek a jelen szabályzatban foglaltak

- A távoli elérésnek biztonságos titkosított terminál kapcsolaton keresztül kell megvalósulnia
- A rendszerbe való belépéshez szükséges a belépő személy azonosítása (felhasználói azonosító/jelszó megadása)
- a belépési azonosítókat másra átruházni, illetve más azonosítóját használni tilos
- 5 egymás utáni sikertelen bejelentkezési kísérlet után a hozzáférést le kell tiltani
- a bejelentkezéseket naplózni kell a tűzfalon. A naplózás beállításáért a hálózatért felelős rendszergazda felel

VIII. A személyes adatok kezelésével kapcsolatos szabályok

8.1. Személyes adatok kezelésének jogszerűsége

A Hivatal belső szervezetei egységeinek feladatkörük ellátása céljából részben jogszabály alapján elrendelt nyilvántartások, részben saját készítésű dokumentumok felfektetése, adatbázisok létesítése, aktualizálása, az adott ellátási formát igénybevevők, közfeladatra jelentkezők azonosítása közbeszerzésre, vállalkozási feladatra pályázók, illetve e pályázatok stb. nyilvántartásba vétele, irányítási jogkör gyakorlása, döntés előkészítése érdekében személyes adatkezelésre az Isztv. és az adott feladatra vonatkozó külön törvény előírásai alapján kerül(het) sor,

Ennek megfelelően:

a) az érintett hozzájárulása alapján, a hozzájárulás beszerzésével, illetőleg a hozzájárulás megadásáról szóló dokumentumnak az érintett részéről történő átadásával (aláírásával), és az iratokhoz csatolásával;

b) a kérelem alapján induló eljárás esetén az alapeljárás keretében benyújtott kérelem figyelembevételével az érintett (a kérelmező) az eljárás szerint szükséges adatai kezeléséhez való hozzájárulásának a vélelmezésével kerülhet sor; mely tényre az érintett figyelmét fel kell hívni. Ennek megtörténtét az iraton rögzíteni kell.

c) A közszereplés során az érintett által már nyilvánosságra hozott (a nyilvánosságra hozatal dokumentálható helyének, idejének, módjának az iraton történő feltüntetésével), illetőleg kifejezetten a nyilvánosságra hozatal céljából átadott adatok esetében a hozzájárulást megadottnak kell tekinteni;

d) Ha jogszabály a következő adatkezelést az adatkezelés céljának és feltételeinek, a kezelendő adatok körének és megismerhetőségének, az adatkezelés időtartamának, valamint az adatkezelő személyének a meghatározásával elrendelte;

e) A különleges adatok esetében az érintett előzetes írásbeli nyilatkozata alapján, annak csatolásával, valamint az Isztv. 3. § 3. a. pontban foglalt adatok esetében nemzetközi egyezményen alapul vagy az Alaptörvényben biztosított alapvető jog érvényesítése érdekében törvény elrendeli;

8.2. Személyes adatok kezelésének célhoz kötöttsége

8.2.1 Az Adtakezelő a személyes adatokat - azok keletkezésétől a megsemmisítésükig - kizárólag az eredeti rendeltetési célra használhatja. Az eredeti rendeltetéstől eltérő célú felhasználásra csak akkor kerülhet sor, ha a törvény azt lehetővé teszi, vagy az érintett ahhoz írásban hozzájárult.
A közérdekű feladatok, illetőleg a jogszabályon alapuló kötelezettségek teljesítése során felmerült személyes adatok csak a jogszabályi előírásoknak megfelelő célra és ideig használhatóak fel. Az Adatkezelő felelős azért, hogy a tudomásra jutott személyes adatokat, illetőleg ilyen adatokat tartalmazó dokumentumokat kizárólag a jogszabály előírásainak megfelelően használja fel, és azokat harmadik személyek részére nem teheti hozzáférhetővé.

8.2.2. A képviselő-testület, illetőleg bizottságai részére készülő előterjesztések, tájékoztatók és azok mellékletei személyes adatokat csak a jogszabály szerinti kötelezettség teljesítése érdekében és csak a jogszabály szerinti terjedelemben tartalmazhatnak.

Az irányítási jogkör gyakorlása, a döntés előkészítés keretében az Isztv. 26.§ (1) - (3) bekezdésében, illetőleg az egyéb jogszabályokban meghatározott adatkört meghaladó, a személyes, az üzleti titok fogalomkörébe tartozó adatokat vagy ilyen adatokat tartalmazó dokumentumokat keletkezésüktől, illetőleg a Hivatal belső szervezeti egységeihez érkezéstől számítottan elkülönítetten „nem nyilvános" adat vagy dokumentumként kell kezelni, és azokat csak az adott ügyben hozandó döntés során lehet felhasználni.

A kezelés során folyamatosan dokumentálni kell egyrészt a betekintésre feljogosítottak nevét, besorolását, másrészt, hogy az adott iratokat, dokumentumokat, ki, mikor és milyen célból tekintette meg.

Ezen dokumentumok nem sokszorosíthatók az ezzel kapcsolatosan a képviselő-testület vagy az illetékes bizottságok részére készülő előterjesztéshez nem csatolhatok. Az előterjesztésben a megjelölt helyen tekinthetik meg a betekintésre jogosultak. (A dokumentumok megtekinthetők az előterjesztés előkészítésért felelős belsőszervezeti egység meghatározott helyiségében, a betekintésre megjelölt időpont, vagy időtartam meghatározásával.)
Az ezzel kapcsolatos előterjesztések a Mötv. szerint zárt ülés keretében tárgyalhatók és a zárt ülésen résztvevők tekinthetik meg a dokumentumokat.

Ezen adatokat, illetőleg dokumentumokat az Isztv. 4. § (2) bekezdése szerint csak a cél megvalósításához szükséges mértékben és ideig lehet kezelni.

8.2.3. A pályázatok, ajánlatok keretében benyújtott dokumentumokat azok tartalma szerint kell megítélni, és a vonatkozó jogszabályok előírásai szerint kell kezelni.

Amennyiben az ajánlatok bontása során megállapításra kerül, hogy az ajánlattevő az üzleti titok körébe tartozó adatokat, dokumentumokat közöl, csatol be azokat a bontást követően elkülönítetten a 8.2.2. pontban foglaltak szerint kell kezelni.

8.2.4. Az érintett írásbeli hozzájárulása alapján olyan adatok kezelésére is sor kerülhet, amelyet jogszabály nem ír elő. Az így kezelt adatok csak arra a célra használhatóak, amelyekre az érintett hozzájárulását megadta.

8.3. A személyes adatok kezelésének biztonsága

Az adatkezelés teljes folyamatában az Adatkezelő köteles biztosítani, hogy a személyes adatokhoz mind a manuális, mind az automatizált feldolgozás (nyilvántartás), mind az elektronikus ügyintézés során csak az Isztv. És a külön törvény szerinti felhatalmazással rendelkezők férhessenek hozzá. Az automatizált feldolgozás során olyan intézkedések szükségese, amelyek:

a) megakadályozzák, hogy illetéktelen személyek a számítógépes adatállományhoz hozzáféljenek,
b) megakadályozzák a tárolóeszközök jogosulatlan olvasását, másolását, módosítását, eltávolítását, megváltoztatását, stb;
c) megakadályozzák, hogy illetéktelen személyek az adatfeldolgozó rendszert adatátviteli eszközök útján elérjék, károsítsák,
d) biztosítják, hogy a jogosult felhasználók csak a hozzáférési joguk szerinti személyes adatok köréhez féljenek hozzá,
e) rögzítik, hogy az adatfeldolgozó rendszert ki, mikor milyen célból érte el továbbá ki és milyen adatrögzítést, módosítást, másolást, stb. hajtott végre,
f) biztosítsák annak az ellenőrzését, hogy mikor, mely személyes adat került kezelésre és azt ki végezte.

A konkrét egyedi ügyekben az eljáró belső szervezeti egység vezetője felelős azért, hogy az eljárás minden mozzanata és az abban közreműködő személyek megállapíthatóak legyenek, az eljárás sorén keletkezett iratok illetéktelen személyek birtokába ne kerülhessenek.

8.4. Az érintettek jogai

8.4.1. Az érintett jogosult tájékoztatást kérni személyes adatai kezeléséről: sor került-e személyes adatai kezelésére, nyilvántartására, ha igen tájékoztatást kérhet, az adatkezelés céljáról, jogalapjáról, időtartamáról, kik és milyen célból kapták meg az adatait.

Az érintett kérelmére lehetővé kell tenni, hogy személyes adatait tartalmazó nyilvántartásba, az adott feladat ellátására vonatkozó külön törvény szabályai szerint betekinthesse.

8.4.2. Az érintett elírás, tévedés esetén kérheti azok helyesbítését. Amennyiben a pontosítást jogszabályi feltételei biztosítottak úgy az Adatfelelős a jogszabályi előírásoknak megfelelően a szükséges intézkedést megteszi, ellenkező esetben tájékoztatja az érintettet a helyesbítés jogszabály szerinti lehetőségekről.

Az érintett személyes adatai kezelésével kapcsolatos kérelmét szóban vagy írásban terjesztheti elő. A szóban előterjesztett kérelemről jegyzőkönyvet kell felvenni. Az előterjesztett kérelemre 30 napon belül kell választ adni.

8.4.3. A betekintésnél biztosítani kell, hogy a betekintő csak a rá vonatkozó, és a külön törvény előírásai szerint általa megismerhető adatokat tekintse, illetőleg ismerje meg. A betekintésről szükség szerint jegyzőkönyvet kell felvenni, vagy azt az iraton rögzíteni kell, úgy hogy az tartalmazza:

a) a betekintés időpontját és célját
b) a jelenlévők nevét és minőségét
c) a betekintés során tett megállapítást vagy észrevételt
d) a jelenlévők aláírását.

8.4. Az érintett tiltakozhat személyes adatai kezelése ellen, ha

a) a személyes adatok kezelése (továbbítása) kizárólag az adatkezelő vagy az adatátvevő jogának vagy jogos érdekének érvényesítéséhez szükséges, kivéve, ha az adatkezelést törvény rendelte el;
b) a személyes adat felhasználása vagy továbbítása közvetlen üzletszerzés, közvélemény-kutatás vagy tudományos kutatás céljára történik;
c) a tiltakozás jogának gyakorlását egyébként jogszabály lehetővé teszi.

Az érintett tiltakozásában foglaltakat haladéktalanul ki kell vizsgálni, és a vizsgálat eredményéről az érintett legkésőbb 15 napon belül írásban tájékoztatni.

A személyes adatok törlésére kerül sor. Ha azok nyilvántartása törvényellenes, vagy az adatok a valóságnak nem felelnek meg és nem korrigálhatóak, az adatkezelés megszűnt, illetőleg a tárolásra a jogszabály által megállapított határidő lejárt, vagy a törlést arra jogosult szerv elrendelte.

8.5. Az adatkezelés, az adattovábbítás összekapcsolása

A Hivatal belső szervezeti egységei által kezelt személyes adatokat tartalmazó rendszerek összekapcsolására, továbbítására csak akkor kerülhet sor,

a) ha azt törvény megengedi, vagy

b) az érintett ahhoz előzetesen hozzájárult

és az adatkezelés jogszabályi feltételei minden esetben teljesülnek.

8.6. A személyes adatokkal kapcsolatos nyilvántartások

A nyilvántartás során - egyedi ügyben az iraton vagy az előadói íven - rögzíteni kell, hogy:

a. ki, vagy mely szervezet kérte a személyes adatok kiadását, illetőleg a betekintés lehetőségét,
b. milyen célból,
c. a teljesítésre milyen jogcímen került sor.

c.a) törvény alapján
c.b) az érintett írásbeli hozzájárulásával vagy az Isztv. 6. § (7) bekezdése alapján a közszereplése során általa már közölt vagy nyilvánosságra hozatal céljából átadott adatokról van szó,
c.c) az Isztv. 6. § (6) bekezdése alapján az - érintett kérelmére – indult eljárásban a hozzájárulás vélelmezésével,
d) mikor történt az adatszolgáltatás, a betekintés.

Az érintett kérheti, hogy a rá vonatkozó adatokat, illetőleg a személyes adatait megismerőkről információt kapjon.

8.7 Személyes adatok kezelésének különös szabályai

a) Amennyiben az érintett személyes adatának kiadását harmadik személy (természetes vagy jogi személy) az adatszolgáltatás jogcímének megjelölésével kéri, és az nem tartozik az a) vagy a b) pont hatálya alá, és azt törvény nem zárja ki úgy az adatszolgáltatás teljesítése előtt az érintettet tájékoztatni kell törvényes jogairól és az adatszolgáltatás teljesítésére nyilatkozata alapján kerülhet sor.

b) A polgárok személyi adatainak és lakcímének nyilvántartásából történő adatszolgáltatás engedélyezése során a kérelem benyújtására és teljesíthetőségének elbírálására az Nytv. valamit a végrehajtására kiadott 146/1993. (X. 26.) Korm. Rendelet rendelkezéseit kell alkalmazni. Az adatszolgáltatásért fizetendő igazgatási szolgáltatási díjra - a 16/2007. (III. 13.) IRM-MeHVM együttes rendelet előírásait kell alkalmazni.

IX. Adatok mentése, mentési rend

A szerverszobában elhelyezett NAS adattároló eszközre történik a mentés az alábbi eljárás szerint:

- napi mentések: hétfőtől - péntekig; változás mentés 00.00-01.00 között
- heti mentések: szombatonként automatizált módon;
- éves mentések: tárgy év utolsó munkanapját követő nap.

A tárgy év utolsó mentésének (az éves mentés) megtörténte után a NAS adattároló eszköz tükör merevlemeze cserélődik, egy új merevlemezre. A mentést tartalmazó HDD a jegyzői titkárságon páncélszekrényben kerül elhelyezésre.

9.1 Az adatok mentése, az adathordozók biztonsága

A napi adatmentés a következő módon történik

(1) Az adatvédelmi felelős által meghatározott fájlokat naponta, a munka befejezésével AES-256 erősségű jelszóval védett .zip fájlba tömörítve az adatmentés helyének kijelölt külső

merevlemezre kell másolni, az aznapi dátumra utaló megnevezéssel ellátott, új, erre a célra létrehozott könyvtárba (vagy feltöltheti az erre a célra létrehozott FTP tárhelyre).

(2) A külső, biztonságos másolatokat tartalmazó merevlemezt csak az adatmentés idejére szabad üzembe állítani, az adatmentés befejeztével szabályszerűen el kell távolítani a rendszerből, és az adatvédelmi felelős által kijelölt helyre kell elzárni (FTP tárhelyre való feltöltés esetén ez úgy módosul, hogy csak a feltöltés idejére szabad az FTP kapcsolatot élővé tenni, adatfeltöltés után a kapcsolatot meg keli szakítani).

(3) A korábbi adatmentéseket csak az adatvédelmi felelős írásbeli utasítására szabad törölni, általánosan a 14 napnál régebbi fájlok kerülhetnek törlésre, de csak abban az esetben, ha már létezik legalább 13 frissebb adatmentés az állományokról.

A heti adatmentés a következőmódon történik

(1) Az adatvédelmi felelős által meghatározott, de általánosságban elmondható, hogy a merevlemezen lévő összes fájlról hetente egyszer teljes körű biztonsági másolatot kell készíteni. Az adathalmazok méretének megfelelően vagy a napi mentésnél már szokásos AES-256 erősségű jelszóval védett .zip fájlba tömörítve, vagy az eredeti állapotban; az adatmentés helyének kijelölt külső merevlemezre kell másolni, az aznapi dátumra utaló megnevezéssel ellátott, új, erre a célra létrehozott könyvtárba, a könyvtár nevében utalva arra, hogy heti és teljes körű, minden adatot érintő biztonsági másolatról van szó.

(2) A külső, biztonsági másolatokat tartalmazó merevlemezt csak az adatmentés idejére szabad üzembe állítani, az adatmentés befejeztével szabályszerűen el kell távolítani a rendszerből és az adatvédelmi felelős által kijelölt helyre el kell zárni.

(3) A korábbi, heti, teljes köm adatmentéseket csak az adatvédelmi felelős írásbeli utasítására szabad törölni, általánosan az 1 hónapnál régebbi biztonsági mentést tartalmazó könyvtárak kerülhetnek törlésre, de csak abban az esetben, ha már létezik 3 frissebb adatmentés az állományokról.

Az éves adatmentés a következő módon történik

A tárgy év utolsó teljes körű biztonsági mentésének megtörténte után, az adatmentés helyének kijelölt külső adattároló eszköz tükör merevlemeze cserélődik egy új merevlemezre. A mentést tartalmazó merevlemez páncélszekrényben kerül elhelyezésre.

9.2 Adatvesztés, elemi kár, bármilyen, adatokat érintő probléma esetén követendő eljárás

(1) Az adatkezelő munkatárs az adatok épségét, hozzáférhetetlenségét veszélyeztető legapróbb jelet észlelve köteles értesíteni az adatvédelmi felelőst.

(2) Az adatkezelő munkatárs a veszély legapróbb jelét észlelve azonnal abbahagyja a munkát, az elmentetlen dokumentumokat elmenti és az adatvédelmi felelős további utasításigi nem nyúl sem a számítógéphez, sem a biztonsági másolatokat tartalmazó merevlemezhez.

(3) Az adatvédelmi felelős (amennyiben nem azonos a rendszergazdával) saját hatáskörében és az adatkezelő munkatárs jelzésére is dönthet úgy, hogy az adatok biztonságára nézve veszélyhelyzetnek értékeli a jeleket és tüneteket.

(4) Az adatvédelmi felelős (amennyiben nem azonos a rendszergazdával) haladéktalanul értesíti a Hivatal rendszergazdáját.

(5) A rendszergazda kiérkezéséig az adatvédelmi felelős biztosítja az érintett számítástechnikai eszközök elkülönítését (senki nem nyúlhat hozzá, még az adatvédelmi felelős sem).

9. 3 Adatok visszatöltése, adatmentési pontok visszaállítása

A napi és heti rendszerességgel mentett adatokat csak az adatvédelmi felelős tudtával és írásbeli beleegyezésével szabad visszatölteni. Az adatok visszatöltéséről jegyzőkönyvet kell készíteni.

X. Záró rendelkezések

Jelen szabályzat 2015. május ..... napján lép hatályba, ezzel egyidejűleg a 2013. szeptember 26. napján kelt Mórahalom Város Polgármesteri Hivatalának Informatikai Biztonsági Szabályzata hatályát veszti.

Függelék lista:

1. sz. függelék: Megismerési nyilatkozat
2. sz. függelék: Adatvédelmi felelős
3. sz. függelék: Nyilvántartás
4. sz. függelék: Elektronikus levelezés szabályozása
5. sz. függelék: Informatikai veszélyhelyzetek elhárítási terve

Mórahalom, 2015. május 28.

1. melléklet

Nyilatkozat
a szabályzatban foglaltak tudomásul vételéről

A szabályzatban foglaltakat megismertem, annak előírásait magamra nézve kötelezőnek ismerem el, annak rendelkezéseit, szabályait következetesen megtartom, s a fentieket aláírásommal igazolom.

	Név	Aláírás
1.	DR. BÍRÓ MÓNIKA	
2.	Tóthné Mamik Gyöngyi	
3.	Szűcs Sándorné	
4.	Csípek Andrásné	
5.	RUTAINÉ SOLDES DIÁNA	
6.	PINTÉR ATTILA	
7.	SOMOGYI JÁNOSNÉ	
8.	FÁBIÁN MAGDOLNA	
9.	GYURIS KRISZTINA	
10.	SZIRAKINÉ NYÁRI MÁRIA	
11.	MÁROSTER EMÍLIA	
12.	ANTAL DÁNIEL	
13.	TANDARI RÓBERT	
14.	KLEIN ILONA	
15.	GÁRGYÁN ANTALNÉ	
16.	JAMBRIK ERIKA	
17.	Pásztor József	
18.	BALOG LÁSZLÓ	
19.	Major Imre	
20.	A. TÓTH Krisztián	
21.		
22.		
23.		
24.		
25.		
26.		
27.		
28.		
29.		
30.		
31.		
32.		
33.		
34.		
35.		
36.		
37.		
38.		
39.		
40.		
41.		
42.		
43.		
44.		

Kelt: .....

2. számú függelék

Adatvédelmi felelős és az elektronikus információs rendszer biztonságért felelős személy kijelölése

Az adatvédelmi felelősi és az elektronikus információs rendszer biztonságért felelős személy feladatainak ellátásával megbízott köztisztviselő:

- neve: dr. Elekes Petra

- beosztása: jegyző

Kelt: Mórahalom, **2015.** május 28.

Záradék: az adatvédelmi felelősi és az elektronikus információs rendszer biztonságért felelős személy feladatainak ellátására való kijelölést tudomásul veszem, a Szabályzatot és az abban foglaltakat megismertem és magamra nézve kötelezőnek ismerem el.

Kelt: Mórahalom, **2015.** május 28.

Elektronikus levelezés szabályozása

Mórahalom Város Polgármesteri Hivatalában E-mail szolgáltatás használatáról a lakossági elektronikus úton történő megkeresések teljesítése, a papír alapú dokumentumok csökkentése, valamint a szolgáltatással való visszaélések kizárása érdekében az elektronikus levelezést az alábbiakban szabályozom:

I. Általános rendelkezések:

1. A szabályozás célja

A szabályzat célja, hogy az E-mail szolgáltatás használata során biztosítsa a Mórahalom Város Polgármesteri Hivatalnál (továbbiakban: Hivatal) a hivatali munka elsődlegességét, megteremtse az ügyintézés érdekében az azonosíthatóság követelményét, valamint elősegítse a papír alapú dokumentumok csökkentését.

2. A szabályozás hatálya

A szabályzat hatálya kiterjed:

a) a Hivatalban munkaviszonyban, munkavégzésre irányuló jogviszonyban álló, fő és részfoglalkozású dolgozójára, akinek munkakörével összefügg az E-mail szolgáltatás használata, illetve azokra, akik valamilyen jogviszony alapján illetékesek a hivatali elektronikus levelezőrendszer használatára (a továbbiakban: munkatárs);
b) a hivatali E-mail szolgáltatás használatra;
c) a hivatali E-mail szolgáltatásra.

3. Értelmező rendelkezések

a) E-mail: elektronikus levél angol mozaikszava Az írás és továbbítás módja teljes egészében elektronikus úton megy végbe.
b) Elektronikus levelezés: olyan szolgáltatás, amely lehetővé teszi, hogy más felhasználók számára fájlok vagy üzenetek továbbítását, valamint dokumentumok fogadását, tárolását.

II. Az e-mail szolgáltatás használatával kapcsolatos általános rendelkezések

4. Az e-mail szolgáltatás biztosítása

4.1. A hivatal minden munkatársa részére biztosítani kell a külső és belső levelezési rendszerhez való hozzáférés lehetőségét, és a megfelelő oktatás mellett követelményként kell érvényesíteni az E-mail cím rendszeres figyelemmel kisérését.
4.2. A munkatársnak a hivatali belépéskor adják ki az informatikus az E-mai szolgáltatás használatához szükséges felhasználónevet és jelszót, valamint személyre, vagy szervezeti egységre szabott levelezési címet. A munkatársat tájékoztatni kell a levelező rendszer biztonságos használatáról. A tájékoztatás megadása az informatikus feladata.
4.3. A munkatárs munkavégzésre irányuló jogviszonyának megszűnése napján felhasználónevet és jelszót, valamint a levelezési címet deaktiválni kell. A deaktiválás az informatikus feladata.

4.4. A levelezőrendszerek tekintetében a szükséges képzéseket, változásokról való tájékoztatásokat az informatikus biztosítja.

5. Az elektronikus levelezés névhasználati szabályai

5.1. A levelezési címet a következő formában kell megalkotni:
<azonosítható megjelölés(lehetőleg név vagy funkció megjelölése)>@morahalom.hu
5.2. Nem személyhez kötött levelezési címek formátuma:
<szervezeti egység>@morahalom.hu
de minden ilyen esetben is valós személynek kell állnia a cím mögött.
5.3. A levelezési szolgáltatás mind a munkatársak közötti, mind a Hivatalon kívüli kapcsolattartásra felhasználható.
5.5. A levelezési rendszereket a belső és külső kapcsolattartásban fel kell használni a papíralapú anyag továbbítások csökkentésére.

III. Az elektronikus levelezéssel kapcsolatos biztonsági szabályok

6.1. Az elektronikus levelező szerver kizárólag a rendszergazda által üzemeltetett levelezési kapun keresztül küldhet vagy fogadhat levelet.
6.2. A levelezési kapun spam szűrő és víruskereső szoftvert üzemeltetése kötelező a vírusok és a kéretlen levelek eltávolítására mind a kimenő, mind a bejövő levelek vonatkozásában.
6.3.Az elektronikus levélhez fájl csatolható, amelynek mérete korlátozott.
6.4. A munkatárs csak saját nevében küldhet levelet, kivéve, ha erre felelős vezető utasítja.
6.5. Az elektronikus levelezés szolgáltatás használata során az alábbi szabályokat kell betartani:

a) Az elektronikus levelezés nem veszélyeztetheti az informatikai infrastruktúra működését.
b) A levél nem tartalmazhat a hatályos magyar jogszabályokba ütköző tartalmat.
c) Az elektronikus levélhez csatolt fájl nem lehet futtatható állomány, nem lehet továbbított reklám.
d) A levelezési rendszeren tilos biztonsági szempontból érzékeny anyagot továbbítani.
e) Tilos a levelezési rendszeren keresztül olyan tartalmú levelet küldeni, amely bármilyen más személy, csoport vagy társaság személyes, illetve üzleti érdekeit sértheti.
f) Tilos rasszista, szemérmet és jó ízlést sértő, valamint szélsőséges politikai nézeteket képviselő tartalmú levelet küldeni.
g) Tilos levélbombák, levelezési láncok küldése, továbbítása;
h) Tilos kéretlen vagy vírusos levelek küldése, továbbítása.

IV. A Hivatal elektronikus címére érkező levelek kezelésének szabályai és az Interaktív kapcsolat

7.1. A Hivatal címére érkezett központi E-maileket az informatikus kezeli.
4.2. A munkatársak a saját elektronikus címére érkező leveleket kötelesek kezelni.
7.3.1. Hivatalos beadvány: Tartalma szerint a Hivatal valamely szervezeti egységének hatáskörébe tartozó küldemény. Az elektronikus úton érkezett „hivatalos beadványt" és a választ ki kell nyomtatni és az iratkezelési szabályzat szerint kell kezelni.
7.3.2. Megválaszolandó kérdés, vélemény: Tartalma szerint hivatalos beadványnak nem minősülő, de reagálást igénylő kérdéseket, véleményeket a szervezeti egység tartalom felelősei kezelik. A küldőt, a szervezeti egység vezetőjével egyeztetett, válaszban öt munkanapon belül, elektronikus úton tájékoztatja a hivatal álláspontjáról. Az elektronikus

úton érkezett „megválaszolandó kérdést, véleményt" és a választ ki kell nyomtatni és az iratkezelési szabályzat szerint kell kezelni.
7.4. Az intézkedést igénylő, központi címre érkező e-maileket továbbítani szükséges a Polgármester és a Jegyző részére.
7.5. Az elektronikus levelekre adott, hivatali ügyet érintő válaszok, tájékoztatások esetében a válaszadónak a közvetlen megküldés előtt, minden esetben a vezetőjével egyeztetni szükséges, a válaszlevelet másolati címzettként minden esetben a felettes vezető részére is továbbítani szükséges.
7.6. Sürgős intézkedést igénylő esetekben (például rövid határidő, soronkívüli intézkedési kötelezettség stb.) azonnal továbbítani kell szignálásra és a tárgy szerinti vezető irányításával az elektronikus levél alapján szükség teendőket (soronkívüli véleményezés, válaszadás, adatszolgáltatás, közérdekű információk továbbítása, berendelés stb.) azonnal el kell végezni.

V. Felelősség

8. A Szabályzatban foglaltak betartásáért a E-mail szolgáltatás használata tárgyban érintett munkatárs személyi felelősséggel tartozik.

Mórahalom, 2015.05.28.

Mórahalmi Polgármesteri Hivatal Jegyzője

dr. Elekes Petra
jegyző

5. sz. függelék

Informatikai veszélyhelyzetek elhárítási terv

1. Az informatikai eszközbázist veszélyeztető helyzetek

Az információk előállítására, feldolgozására, tárolására, továbbítására, megjelenítésére alkalmas informatikai eszközök fizikai károsodását okozó veszélyforrások ismerete azért fontos, hogy felkészülten megelőző intézkedésekkel a veszélyhelyzetek elháríthatók legyenek.

1.1. Környezeti infrastruktúra okozta ártalmak

- Elemi csapás:
  - árvíz,
  - földrengés
  - tűz
  - villámcsapás, stb.
- Környezeti kár:
  - légszennyezettség,
  - nagy teljesítményű elektromágneses térerő,
  - elektrosztatikus feltöltődés,
  - a levegő nedvességtartalmának felszökése vagy leesése,
  - piszkolódás (pl. por).
- Közüzemi szolgáltatásba bekövetkező zavarok:
  - feszültség-kimaradás,
  - feszültségingadozás,
  - elektromos zárlat,
  - csőtörés.

Áramszünet:

Előre tervezett áramszünet esetén, amennyiben az munkanapra esik minden munkaállomás kezelőjét, a felhasználókat értesíteni szükséges, hogy munkáját ennek megfelelően ütemezhesse.
Áramszünet után a munkaállomásokat a hálózat elérése érdekében újra kell indítani.
A váratlan áramszünet esetén a rendszergazda köteles a rendszer újraindíttatásáról gondoskodni.
Váratlan áramkimaradás esetére a szervereket intelligens UPS–sel kell ellátni (szünetmentes tápegység), mellyel az áramkimaradás folyamatosságát biztosítani lehet.

Vírusveszély:

A rendszer beépített víruskezelő rendszerrel rendelkezik, amely a vírusgyanús jelenségeket is figyeli.
A gépek bekapcsolásakor a víruskezelő leellenőrzi a munkaállomások memóriáját.
Amennyiben a felhasználó vírusfertőzést észlel, írja fel a hibaüzenetet, a gépet azonnal kapcsolja ki, lássa el figyelmeztető felirattal (Vírusveszély, kérlek ne kapcsold be!) és szóljon a rendszerfelügyeletnek.

Hibajelenségek kezelése:

Amennyiben a felhasználó a rendszer működése során bármilyen hibát észlel (miután meggyőződött róla, hogy a számítógépe kap elektromos áramot, a perifériák kapcsolatban vannak a számítógéppel, nem maradt a meghajtóban hajlékony lemez, jó nyomtatóba küldte el a nyomtatási parancsot) köteles amennyiben van, a hibaüzenetet felírni és a rendszergazdának jelenteni, hogy a szükséges intézkedéseket megtegye. Amennyiben a hiba elhárítása miatt a szerver újraindítása szükséges, erről a felhasználókat értesíteni szükséges, a felhasználói munkaállomásokat a hiba elhárítása után célszerű újraindítani.

1.2. Emberi tényezőre visszavezethető veszélyek

Szándékos károkozás:

- behatolás az informatikai rendszerek környezetébe,
- illetéktelen hozzáférés (adat, eszköz),
- adatok- eszközök eltulajdonítása,
- rongálás (gép, adathordozó),
- megtévesztő adatok bevitele és képzése,
- zavarás (feldolgozások, munkafolyamatok).

Nem szándékos, illetve gondatlan károkozás:

- figyelmetlenség (ellenőrzés hiánya),
- szakmai hozzá nem értés,
- a gépi és eljárásbeli biztosítékok beépítésének elhanyagolása,
- a megváltozott körülmények figyelmen kívül hagyása,
- vírusfertőzött adathordozó behozatala,
- biztonsági követelmények és gyári előírások be nem tartása,
- adathordozók megrongálása (rossz tárolás, kezelés),
- a karbantartási műveletek elmulasztása.

A szükséges biztonsági-, jelző és riasztó berendezések karbantartásának elhanyagolása veszélyezteti a feldolgozás folyamatát, alkalmat ad az adathoz való véletlen vagy szándékos illetéktelen hozzáféréshez, rongáláshoz.

2. Az adatok tartalmát és a feldolgozás folyamatát érintő veszélyek

2.1. Tervezés és előkészítés során előforduló veszélyforrások

- a rendszerterv nem veszi figyelembe az alkalmazott hardver eszköz lehetőségeit,
- hibás adatrögzítés, adatelőkészítés, az ellenőrzési szempontok hiányos betartása.

2.2. A rendszerek megvalósítása során előforduló veszélyforrások

- hibás adatállomány működése,
- helytelen adatkezelés,
- programtesztelés elhagyása.

3.3. A működés és fejlesztés során előforduló veszélyforrások

- emberi gondatlanság,
- szervezetlenség,
- képzetlenség,
- szándékosan elkövetett illetéktelen beavatkozás,
- illetéktelen hozzáférés,
- üzemeltetési dokumentáció hiánya.