A

Nemesszalóki Közös Önkormányzati Hivatal

Adatvédelmi és Informatikai Biztonsági Szabályzata

I. Bevezetés

A Nemesszalóki Közös Önkormányzati Hivatal jelen szabályzat kiadásával biztosítja az állami és önkormányzati szervek elektronikus információszabadságáról szóló 2013. évi L. törvény, az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény, továbbá az állami és önkormányzati szervek elektronikus információszabadságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre vonatkozó, valamint a biztonsági osztályba és biztonsági szintbe sorolási követelményeiről szóló 77/2013. (XII.19.) NFM rendelet és más hatályos rendelkezések helyi érvényesülését.

II. Általános szabályok

1. A szabályzat célja

A szabályzat célja, hogy biztosítsa A Nemesszalóki Közös Önkormányzati Hivatal és intézményei, 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 a hatályos jogszabályok szerinti kötelezettségnek, mely szerint az állami és önkormányzati adatkezelőknek 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 Nemesszalóki Közös Önkormányzati Hivatalnál foglalkoztatott munkavállalókra terjed ki.
A személyes adatok védelméért, az adatkezelés jogszerűségéért a jegyző felelős.

Az elektronikus információs rendszer biztonságáért felelős személyre.

2.2 A szabályzat tárgyi hatálya

E szabályzat tárgyi hatálya kiterjed:

- a Hivatal tulajdonában lévő valamennyi számítástechnikai, informatikai berendezésre (ideértve az anyakönyvi munkaállomásokat is), 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.

III. Értelmező rendelkezések

A szabályzatban előforduló fogalmak alatt a 2013. évi L. törvény 1. §. által rögzítettek irányadóak.

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 képvisló-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 Nemesszalóki Közös Önkormányzati Hivatal Szervezeti és Működési Szabályzatával, és egyéb szabályzataival összhangban kell alkalmazni.

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, 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 szakszerű végrehajtásáról a Hivatal adatvédelmi felelősének kell gondoskodnia. Az adatvédelmi felelős feladatait az információs önrendelkezési jogról és információszabadságról szóló 2011. évi CXII. törvény 24. § (2) bekezdése tartalmazza

Az elektronikus információs rendszerek biztonságáért felelős személy ellátja az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény 13. §-ában meghatározott feladatokat.
Az elektromos információs rendszer biztonságáért a Hivatal informatikusa felel. Elvégzi az informatikai védelmi rendszer biztosítását, a vírusvédelmi szoftverek frissítését, valamint biztosítja a rendszer üzemképességét, és a műszaki ellátást, közreműködik biztonsági másolatok készítésében, segíti a Hivatal dolgozóinak számítástechnikai munkáját.

Az informatikai biztonság tudatosítására irányuló tevékenység keretében az összes közszolgálati, vagy munkavégzésre irányuló egyéb jogviszonyban álló alkalmazottak, munkavállalóknak, megbízottak képzését biztosítani kell.

4.6. Fizikai, technikai védelem

4.6.1. Tűzvédelem

Az informatikai eszközöket tartalmazó irodák a "D" tűzveszélyességi osztályba tartoznak, amely mérsékelt tűzveszélyes üzemet jelent.

4.6.2. Vagyonvédelem, fizikai biztonság

- az irodákat zárakkal kell felszerelni;
- az ügyfélfogadás rendjét szabályozni kell;
- munkaidőn túl az irodákban csak engedéllyel lehet tartózkodni;
- az irodákba történő illetéktelen behatolás tényét a jegyzőnek azonnal jelenteni kell;
- az irodahelyiségekben elhelyezett számítástechnikai eszközöket csak az arra kijelölt köztisztviselők 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 sérüljenek, károsodjanak;
- az adathordozókat a gyors hozzáférés érdekében azonosító adatokkal kell ellátni;
- adathordozót más intézménynek átadni csak a jegyző engedélyével lehet;
- az adathordozók megőrzésének idejét, ha másképp nincs rendelkezés, a jegyző határozza meg;
- 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 az adatvisszanyerés esélyének kockázata nagy mértékű;
  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 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. 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 a jegyző 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 programokról 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 hőigénybevételtől;
- a számítógép közelében ételt és italt fogyasztani tilos;
- számítógépeknél biztosítani kell a szünetmentes feszültségforrást;
- a számítógép-hálózat vezetékeit külön kábelcsatornában kell vezetni;
- 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;
- eseti rendszerességgel a számítógépeken hardver teszteket kell lefuttatni.

4.7. Informatikai védelem

Az irodákban a folyamatos, higiénikus munkavégzés feltételeit kell megőrizni. A számítógépek biztonságos műszaki üzemeltetésért a hivatali informatikus a felelős.

Az irodákba égő cigarettával belépni és ott dohányozni, valamint tüzet okozó tevékenységet folytatni szigorúan TILOS!

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

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

Az informatikai hálózatba más – nem a rendszerekhez, illetve azok kiszolgálásához tartozó – berendezéseket csatlakoztatni nem lehet.

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 a jegyző fegyelmi felelősségre vonást kezdeményezhet.

Védelmi előírások:

- A számítógépeket csak indítójelszóval lehessen elindítani.
- Induláskor minden esetben vírus-ellenőrző programot kell elindítani.
- A feldolgozáshoz szükséges programok elindításához és az adatok hozzáféréséhez jelszóvédelem kell.
- Az adó és pénzügyi 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 tárgyévi zárást követően mentést kell végezni és ezt a 2. 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. Részletes szabályok

5. A személyes adatok kezelésével kapcsolatos szabályok

5.1. 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 adott feladatra vonatkozó törvények 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;

f) Az érintettel írásban kötött szerződés alapján, ha az abban foglaltak teljesítése érdekében a hozzájárulást megtagadta.

A szerződének tartalmaznia kell:

f.a) a kezelendő adatok meghatározását,

f.b) az adatkezelés időtartamát,

f.c) a felhasználás célját, (például közérdekű adatok keretében történő nyilvánosságra hozatal tényét, és 5 éves nyilvános kezelést),

f.d) az érintett azon nyilatkozatát, hogy a szerződés aláírásával hozzájárul adatainak a szerződésben foglaltaknak megfelelő kezeléséhez, nyilvánosságra hozatalához, amennyiben az adatok továbbításra kerülnek, illetőleg adatfeldolgozó igénybevételre kerül sor, ahhoz is hozzájárulását adja.

5.2. Személyes adatok kezelésének célhoz kötöttsége

5.2.1. 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.

5.2.2. 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 adtakört 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 csatolhatók. 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 Mööt. 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.

5.2.3. 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 az 5.2.2. pontban foglaltak szerint kell kezelni.

5.2.4. 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.

5.3. 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 hozzáférjenek,
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 férjenek 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 során keletkezett iratok illetéktelen személyek birtokába ne kerülhessenek.

5.4. Az érintettek jogai

5.4.1. 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.

5.4.2. 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 a Ket. szerinti határidőn belül kell választ adni.

5.4.3. 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.

5.4.4. 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.

5.5. 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.

5.6. 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.

5.7. Személyes adatok kezelésének különös szabályai

a) Az érintettel kötendő és a kötelezően közzéteendő közérdekű adatok körébe tartozó szerződések esetén a szerződésben rögzíteni kell, hogy az érintett tudomásul veszi és hozzájárul személyes adatai (neve, a szerződés megnevezése, típusa, tárgya, értéke, időtartama, és esetleges módosulásuk) közérdekű adatként történő nyilvánossá tételéhez, és 5 éven keresztül történő nyilvános kezeléséhez. Amennyiben az érintett nem járul hozzá úgy a szerződés megkötésére, nem kerülhet sor.

b) Pályázat kiírásakor, az érintettekkel közölni kell, hogy pályázatuk, ajánlatuk érvényességi feltétele, az a) pont szerinti adatok nyilvánosságra hozatalához történő hozzájárulásuk. Ennek korlátozására irányuló nyilatkozat érvénytelen.

c) 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.

d) A polgárok személyi adatainak és lakcímének nyilvántartásából történő adatszolgáltatás engedélyezése során a kérelem benyújtására és teljesíthetőségének elbírálására, az adatszolgáltatásért fizetendő igazgatási szolgáltatási díjra a mindenkor hatályos jogszabályi előírásokat kell alkalmazni.

VI. Közérdekű adatok megismerésének szabályai

6.1. Közérdekű információk, illetőleg dokumentumok meghatározása

6.1.1. Közérdekű, nyilvános adat különösen a Nemesszalóki Közös Önkormányzati Hivatal, a létrehozásában érintett Önkormányzatok költségvetésével és annak végrehajtásával, vagyonával és annak kezelésével, a közpénzek felhasználásával, szervei feladatkörével, működésével, tevékenységével, átláthatóságával, ellenőrizhetőségével kapcsolatos információk.

6.1.2. A kötelezően közzéteendő közérdekű információk:

e) az Önkormányzat feladat- és hatáskörével, működésével, kapcsolatos információk - dokumentumok - keretében: az Önkormányzat Szervezeti és Működési Szabályzata, éves költségvetése, éves költségvetési beszámolója, a képviselő-testület nyilvános ülésein hozott rendeletei, határozatai;

f) a Hivatal működésével, szervezetével kapcsolatos információk, dokumentumok;

g) továbbá mindaz, amit jogszabály közérdekűvé nyilvánít.

6.1.3. Nem tehetők hozzáférhetővé azok az adatok,

a. amelyeket törvény alapján az arra jogosult szerv állam- vagy szolgálati titokká nyilvánított,
b. amelyek a nemzetközi szerződésből eredő kötelezettség alapján minősített adatok,
c. amelyek esetében a közérdekű adatok nyilvánosságához való jogot- az adatfajták meghatározásával – törvény más nevesített okból, illetőleg bírósági vagy közigazgatási hatósági eljárásra való tekintettel a nyilvánosságra hozatalt korlátozza,
d. amelyek esetében
d.a) az adatfajtára vonatkozó külön törvény a nyilvánossá tételt kizárja vagy korlátozza,
d.b) a Ptk. előírásai alapján üzleti titok szabályait kell alkalmazni.

6.1.4. A keletkezésüktől számított 10 éven belül nem hozhatók nyilvánosságra a feladat- és hatáskörbe tartozó döntés meghozatalára irányuló eljárás során készített vagy rögzített és a döntés külső befolyástól mentes előkészítését, megalapozását szolgáló adatok, dokumentumok. Ezen adatok megismerését a jegyző hatáskörébe tartozó ügyek esetén a jegyző engedélyezi. Jogszabály egyes adatok megismerhetőségének korlátozására a fent meghatározottnál rövidebb időtartamot állapíthat meg. A döntés megalapozását szolgáló adat megismerésére irányuló igény tíz éves időtartamon belül – a döntés meghozatalát követően akkor utasítható el, ha az adat megismerése a hivatal törvényes működésének rendjét vagy feladat – és hatáskörének illetéktelen külső befolyástól mentes ellátást, így különösen az adatot, keletkeztető álláspontját a döntések előkészítése során történő szabad kifejtését veszélyeztetné.

6.1.5. Azon ügyek, illetőleg dokumentumok esetén, amelyekben mind a személyes, illetőleg az üzleti titkot jelentő, mind a közérdekű adatok előfordulnak, biztosítani kell az adatok pontosítását és a személyes, az üzleti titkot képező adatok elhatárolását. Amennyiben a közérdekű dokumentum az igénylő által meg nem ismerhető adatot is tartalmaz úgy a kiadott másolaton felismerhetetlenné, kell tenni ezen adatokat.

6.2. A közérdekű adatok előkészítése

6.2.1. A közérdekű adatok feldolgozása, előállítása a jogszabály által meghatározott formában és határidőre történő elhelyezése az illetékes belső szervezeti egység feladata.

6.2.2. Az interneten csak hiteles, a jogszabályi előírásoknak megfelelő tartalmú és formájú információk helyezhetők el. Az adatok hitelességéért, megbízhatóságáért, a jogszabályban meghatározott formában történő előállításáért, a szükséges aktualizálásáért a jegyző a felelős. A jegyző felelős azért, hogy a megjelenő jogszabályok által közérdekűvé nyilvánított adatok előírás szerinti publikálását biztosítsa.

6.3. Nyilvántartás az elutasított kérelmekről

A közérdekű adatok megismerésére irányuló kérelmek elutasításáról nyilvántartást kell vezetni.

A nyilvántartás tartalmazza:

a) a közérdekű adatok megismerésére irányuló kérelem benyújtásának időpontját,
b) a megismerni kívánt közérdekű adatok körét, az elérés módját: pl. Portálon, intraneten,
c) az elutasítás a megtagadás, dátumát, indokát nem elérhető nem nyilvános minősítését.

A Hivatal évente, az adatvédelmi biztos közleményében meghatározott időpontra értesíti az adatvédelmi biztost az elutasított igényekről, valamint az elutasítások indokairól.

VII. Jogorvoslati eljárás szabályai

Ha a Hivatal közérdekű adatra vonatkozó igényt nem teljesíti, az igénylő az Isztv. 31. §-ban foglalt eljárási rendnek megfelelően – az elutasítás kézhezvételét követő harminc napon belül – bírósághoz fordulhat. A megtagadás jogszerűségét és megalapozottságát a Hivatal köteles bizonyítani.

A fenti rendelkezések nem alkalmazhatók a közhitelű nyilvántartásból történő – külön törvényben szabályozott – adatszolgáltatásra.

VIII. Hatálybalépés

Jelen szabályzat 2018. február 01. napján lép hatályba, ezzel egyidejűleg az e tárgykörben kiadott szabályzatok hatályukat vesztik.

Nemesszalók, 2018. január 29.

dr. Szabadics Zsuzsanna
jegyző

1. számú melléklet

Megismerési nyilatkozat

A Nemesszalóki Közös Önkormányzati Hivatal jelen Adatvédelmi és Biztonsági Szabályzatát megismertem.

Név	Beosztás	Kelt	Aláírás
BEDŐ GÁBOR	KÖZTISZTVISELŐ	2018.01.30.	
DR. SZABADICS ZSUZSANNA	JEGYZŐ	2018.01.30.	
VÁRNAI ZSUZSANNÉ	KÖZTISZTVISELŐ	2018.01.30.	Várnai Zsuzsanna
SZUHNÉ SZABÓ MAGDOLNA	KÖZTISZTVISELŐ	2018.01.30.	
BUZÁSNÉ MÓGOR ADRIENN	KÖZTISZTVISELŐ	2018.01.30.	
SÜLE GYULÁNÉ	KÖZTISZTVISELŐ	2018.01.30.	Süle Gyuláné
PANKOVICS-ORBÁN KATALIN	KÖZTISZTVISELŐ	2018.01.30.	
SZABÓNÉ PIRITI MÁRTA	KÖZTISZTVISELŐ	2018.01.30.	Szabóné
PATKAI GYULA SÁNDORNÉ	KÖZTISZTVISELŐ	2018.01.30.	Patkai Gyuláné
WERSTROH-VARGA SZABINA	KÖZTISZTVISELŐ	2018.10.01.	
GERENCSÉR-VARGA ZSANETT	KÖZTISZTVISELŐ	2020.01.20.	Gere-Varga Zsanett

2. számú melléklet

Felelősök kijelölése

Az adatvédelmi felelősi feladatok ellátásával megbízott köztisztviselő:

- neve: Werstroh-Varga Szabina
- beosztása: ügykezelő, ügyintéző

Kelt: Nemesszalók, 2018. október 1.

dr. Szabadics Zsuzsanna
jegyző

Záradék:

Az adatvédelmi feladatok ellátásra való kijelölést tudomásul veszem, a Szabályzatot és az abban foglaltakat megismertem és magamra nézve kötelezőnek ismerem el.

Kelt: Nemesszalók, 2018. október 1.

.....
aláírás

Az informatikai biztonsági feladatok ellátásával megbízott köztisztviselő:

- neve: Bedő Gábor
- végzettsége: informatikus mérnök
- beosztása: informatikus, ügyintéző

Kelt: Nemesszalók, 2018. január 29.

dr. Szabadics Zsuzsanna
jegyző

Záradék:

Az informatikai biztonsági feladatok ellátásra való kijelölést tudomásul veszem, a Szabályzatot és az abban foglaltakat megismertem és magamra nézve kötelezőnek ismerem el.

Kelt: Nemesszalók, 2018. január 29.

.....
aláírás

3. számú melléklet

A Nemesszalóki Közös Önkormányzati Hivatal
kiemelt rendszer- és felhasználói programjai,
illetve azok mentési rendje

A Hivatal kiemelt rendszer- és felhasználói programjairól napi, heti, valamint éves mentés készül.

Kiemelt felhasználói programok:

- ASP
- Helyi Vizual Regiszter
- WIKT Iktató
- Ms Office
- Anyakönyvi felhasználói rendszer – külső szolgáltatón keresztül.

Rendszerprogramok:

- Windows 7
- Windows 10
- Linux (Anyakönyvi szolgáltató rendszer – külső szolgáltatón keresztül.)

Mentési rend

A program felhasználói útmutatókban leírtak szerint:

napi mentések
heti mentések
éves mentések

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

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

Az adatkezelő munkatárs a veszély legapróbb jelét észlelve azonnal abbahagyja a munkát, az elmentetlen dokumentumokat elmenti és további utasításáig nem nyúl sem a számítógéphez, sem a biztonsági másolatokat tartalmazó lemezekhez.

Az adatvédelmi felelős saját hatáskörében és az adatkezelő munkatárs jelzésére is dönthet úgy, hogy az adatok biztonságára nézve veszélyhelyzetnek értékeli a jeleket és tüneteket.

Az adatvédelmi felelős haladéktalanul értesíti a rendszergazdát.

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

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.

4. sz. melléklet

A Nemesszalóki Közös Önkormányzati Hivatal biztonsági osztályba, biztonsági szintbe sorolása.

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény, továbbá az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre vonatkozó, valamint a biztonsági osztályba és biztonsági szintbe sorolási követelményeiről szóló 77/2013. (XII. 19.) NFM rendelet alapján a

2. biztonsági osztályba sorolja.

Az elektronikus információs rendszer biztonsági osztályba sorolásakor a bizalmasság, sértetlenség és rendelkezésre állás követelményét a rendszer funkciójára tekintettel, ahhoz igazodó súllyal érvényesül.

A Hivatalban bekövetkezhető káresemények:
1. személyes adat sérülhet;
2. az üzlet-, vagy ügymenet szempontjából csekély értékű, és/vagy csak belső (intézményi) szabályzóval védett adat, vagy elektronikus információs rendszer sérülhet;
3. a lehetséges társadalmi-politikai hatás az érintett szervezeten belül kezelhető;
4. a közvetlen és közvetett anyagi kár az érintett szervezet költségvetéséhez, szellemi és anyagi erőforrásaihoz képest csekély.

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény, továbbá az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre vonatkozó, valamint a biztonsági osztályba és biztonsági szintbe sorolási követelményeiről szóló 77/2013. (XII. 19.) NFM rendelet alapján a

2. biztonsági szintbe sorolja.

Az elektronikus információs rendszerek biztonsági szintbe sorolása az érintett szervezet biztonsági szintjét határozza meg. A biztonsági szintbe soroláskor a bizalmasság, sértetlenség és rendelkezésre állás követelményét a szervezet feladataira, a vele szemben fennálló elvárásokra tekintettel, és a kockázatokhoz illeszkedő súllyal érvényesíti.

A Hivatal nem működtet a 2. besorolási osztálynál magasabb elektronikus információs rendszereket és az informatikai folyamatok részben szabályozottak:

1. A biztonsági folyamatoknak nincsenek részletszabályai, azokat az elfogadott magas szintű szabályzatok (informatikai biztonságpolitika, informatikai biztonsági stratégia, informatikai biztonsági szabályzat, valamint a tervezésre, beszerzésre, fejlesztésre, képzésre vonatkozó szakterületi belső előírások) szabályozzák.

2. Az elektronikus információs rendszerek biztonságához kapcsolódó eljárások kialakítására törekszünk, de ehhez megfelelő eszközrendszer nem áll rendelkezésre.

3. Az elektronikus információs rendszerek biztonságával kapcsolatos felelősségek és feladatok egy, az elektronikus információs rendszer biztonságáért felelős, irányítási jogkörében korlátozott személyhez vannak hozzárendelve.

4. Az elektronikus információs rendszerek előállítanak a biztonságra vonatkozó információkat, de azok nem elemezzük.

5. Az elektronikus információs rendszerek biztonságára vonatkozó jelentések nem teljes körűek.

6. Az elektronikus információs rendszerek biztonságát nem a Hivatal teljes körű biztonságának részeként, hanem elsősorban az informatika belső felelősségeként, területeként kezeljük.

7. A fizikai beléptetés ellenőrzésén túlmenően a működtetett rendszer és a kezelt adatok védelme további fizikai védelmi intézkedéseket nem igényel.

ADMINISZTRATÍV VÉDELMI INTÉZKEDÉSEK

Sorszám	Intézkedés típusa
3.1.1.	**Szervezeti szintű alapfeladatok**
3.1.1.1.	Informatikai biztonságpolitika
3.1.1.2.	Informatikai biztonsági stratégia
3.1.1.3.	Informatikai biztonsági szabályzat
3.1.1.4.	Az elektronikus információs rendszerek biztonságáért felelős személy
3.1.1.5.	Pénzügyi erőforrások biztosítása
3.1.1.6.	Az intézkedési terv és mérföldkövei
3.1.1.7.	Az elektronikus információs rendszerek nyilvántartása
3.1.1.10.	Kockázatkezelési stratégia
3.1.1.11.	Az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárás
3.1.2.	**Kockázatelemzés**
3.1.2.1.	Kockázatelemzési eljárásrend
3.1.2.2.	Biztonsági osztályba sorolás
3.1.2.3.	Kockázatelemzés
3.1.3.	**Tervezés**
3.1.3.1.	Biztonságtervezési eljárásrend
3.1.3.2.	Rendszerbiztonsági terv
3.1.3.3.	Személyi biztonság
3.1.3.3.2.	Viselkedési szabályok az interneten
3.1.4.	**Rendszer és szolgáltatás beszerzés**
3.1.4.2.	Beszerzési eljárásrend
3.1.4.4.	A rendszer fejlesztési életciklusa
3.1.4.8.	Külső elektronikus információs rendszerek szolgáltatásai
3.1.6.	**Emberi tényezőket figyelembe vevő – személy – biztonság**
3.1.6.5.	Eljárás a jogviszony megszűnésekor
3.1.6.8.	Fegyelmi intézkedések
3.1.7.	**Tudatosság és képzés**
3.1.7.1.	Képzési eljárásrend
3.1.7.2.	Biztonság tudatosság képzés

FIZIKAI VÉDELMI INTÉZKEDÉSEK

Sorszám	Intézkedés típusa
3.2.1.	**Fizikai és környezeti védelem**
3.2.1.2.	Fizikai védelmi eljárásrend
3.2.1.3.	Fizikai belépési engedélyek
3.2.1.4.	A fizikai belépés ellenőrzése

LOGIKAI VÉDELMI INTÉZKEDÉSEK

Sorszám	Intézkedés típusa	Alapelvek		
		Bizalmasság	Sértetlenség	Rendelkezésre állás
3.3.1.	**Konfigurációkezelés**			
3.3.1.1.	Konfigurációkezelési eljárásrend	X	X	X
3.3.1.2.	Alapkonfiguráció	X	X	X
3.3.1.8.	Elektronikus információs rendszerelem leltár	X	X	X
3.3.1.10.	A szoftverhasználat korlátozásai	X	X	X
3.3.1.11.	A felhasználó által telepített szoftverek	X	X	X
3.3.2.	**Üzletmenet (ügymenet) folytonosság tervezése**			
3.3.2.1.	Üzletmenet folytonosságra vonatkozó eljárásrend	0	0	X
3.3.2.2.	Üzletmenet folytonossági terv informatikai erőforrás kiesésekre	0	0	X
3.3.2.8.	Az elektronikus információs rendszer mentései	0	X	X
3.3.2.9.	Az elektronikus információs rendszer helyreállítása és újraindítása	0	X	X
3.3.3.	**Karbantartás**			
3.3.3.1.	Rendszer karbantartási eljárásrend	0	X	X
3.3.3.2.	Rendszeres karbantartás	0	X	X
3.3.4.	**Adathordozók védelme**			
3.3.4.1.	Adathordozók védelmére vonatkozó eljárásrend	X	X	X
3.3.4.2.	Hozzáférés az adathordozókhoz	X	X	X
3.3.4.6.	Adathordozók törlése	X	0	0
3.3.4.7.	Adathordozók használata	X	X	X
3.3.5.	**Azonosítás és hitelesítés**			
3.3.5.1.	Azonosítási és hitelesítési eljárásrend	X	X	X
3.3.5.2.	Azonosítás és hitelesítés	X	X	X
3.3.5.4.	Azonosító kezelés	X	X	X
3.3.5.5.	A hitelesítésre szolgáló eszközök kezelése	X	X	X
3.3.5.6.	A hitelesítésre szolgáló eszköz visszacsatolása	X	X	X
3.3.5.8.	Azonosítás és hitelesítés (szervezeten kívüli felhasználók)	X	X	X
3.3.5.8.2.	Hitelesítésszolgáltatók tanúsítványának elfogadása	0	X	X
3.3.6.	**Hozzáférés ellenőrzése**			
3.3.6.1.	Hozzáférés ellenőrzési eljárásrend	X	X	X
3.3.6.2.	Felhasználói fiókok kezelése	X	X	X
3.3.6.3.	Hozzáférés ellenőrzés érvényesítése	X	X	X
3.3.6.12.	Azonosítás vagy hitelesítés nélkül engedélyezett tevékenységek	X	X	X
3.3.6.16.	Külső elektronikus információs rendszerek használata	X	X	X
3.3.6.18.	Nyilvánosan elérhető tartalom	X	X	X
3.3.7.	**Rendszer- és információsértetlenség**			
3.3.7.1.	Rendszer- és információsértetlenségre vonatkozó eljárásrend	0	X	0
3.3.7.3.	Hibajavítás	0	X	0
3.3.7.4.	Kártékony kódok elleni védelem	X	X	X
3.3.7.5.	Az elektronikus információs rendszer felügyelete	X	X	X
3.3.7.12.	A kimeneti információ kezelése és megőrzése	X	X	0
3.3.8.	**Naplózás és elszámoltathatóság**			
3.3.8.1.	Naplózási eljárásrend	X	X	X

3.3.8.2.	Naplózható események	X	X	X
3.3.8.3.	Naplóbejegyzések tartalma	X	X	X
3.3.8.8.	Időbélyegek	X	X	X
3.3.8.9.	A naplóinformációk védelme	X	X	X
3.3.8.11.	A naplóbejegyzések megőrzése	X	X	X
3.3.8.12.	Naplógenerálás	X	X	X
3.3.9.	**Rendszer- és kommunikációvédelem**			
3.3.9.1.	Rendszer- és kommunikációvédelmi eljárásrend	X	X	X
3.3.9.6.	A határok védelme	X	X	X
3.3.9.10.	Kriptográfiai kulcs előállítása és kezelése	X	X	X
3.3.9.11.	Kriptográfiai védelem	X	X	0
3.3.9.12.	Együttműködésen alapuló számítástechnikai eszközök	X	0	0
3.3.9.22.	A folyamatok elkülönítése	X	X	0
3.3.10.	**Reagálás a biztonsági eseményekre**			

A tervezett, vagy már működtetett elektronikus információs rendszerekre alkalmazott biztonsági intézkedések kialakítása során figyelembe kell venni a rendszer célját meghatározó jogszabályi hátteret, funkciót is.
A meghatározott biztonsági intézkedések fokozatosan vezethetők be.

Helyettesítő intézkedésekkel is lehet teljesíteni a védelmi intézkedés katalógusban meghatározott minimális követelményeket, a rendszerre meghatározott biztonsági kockázati szintnek megfelelő intézkedések kiválasztásával, amellett, hogy az érvényes minden kötelezettséget figyelembe kell venni.

A helyettesítő biztonsági intézkedés olyan eljárás, amelyet az irányadó biztonsági szinthez tartozó biztonsági intézkedés helyett alkalmazni lehet, és egyenértékű vagy összemérhető védelmet nyújt az adott elektronikus információs rendszerre valós fenyegetést jelentő veszélyforrások ellen, és a helyettesített intézkedéssel egyenértékű módon biztosít minden külső vagy belső követelménynek (például törvényeknek, vagy szervezeti szintű szabályzóknak) való megfelelést.

Az alábbi feltételek teljesülése esetén alkalmazható helyettesítő intézkedés:

1. Ha az elektronikus információs rendszerek biztonságára vonatkozó szabványokban, vagy hazai ajánlásokban fellelhető helyettesítő intézkedés, vagy ha ezekben nincs megfelelő helyettesítő intézkedés, akkor kivételesen alkalmazható egy, az adott helyzetben megfelelő helyettesítő intézkedés.

2. A helyettesítő intézkedések kiválasztásánál törekedni kell arra, hogy a védelmi intézkedés katalógusból legyen kiválasztva az intézkedés. A helyileg meghatározott helyettesítő intézkedéseket csak végső esetben szabad használni, amennyiben a biztonsági intézkedések katalógusa nem tartalmaz az adott viszonyok között alkalmazható intézkedést.

3. A helyettesítő intézkedés alkalmazása előtt be kell mutatni, hogy a helyettesítő intézkedés hogyan biztosítja az elektronikus információs rendszer egyenértékű biztonsági képességeit, védelmi szintjét, és azt, hogy miért nem használhatók a vonatkozó alapkészlet biztonsági intézkedései.

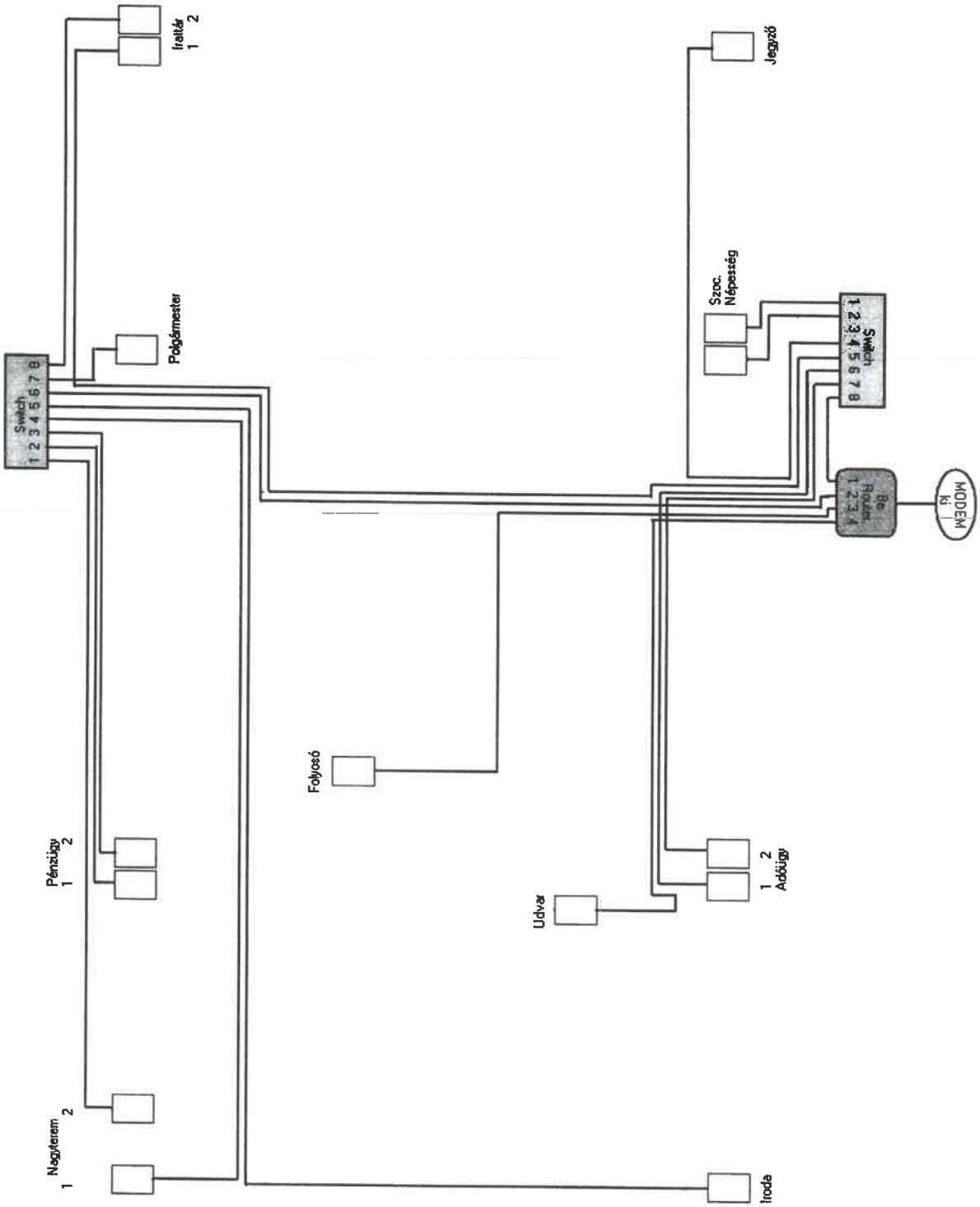
4. A helyettesítő intézkedésnek az elektronikus információs rendszerre megállapított biztonsági szintnek megfelelőnek kell lennie.

Az elektronikus információs rendszer fejlesztése csak olyan eszközökkel megengedett, amelyek megfelelnek a biztonsági előírásoknak, illeszkednek a meglévő architektúrához és támogatják azt.

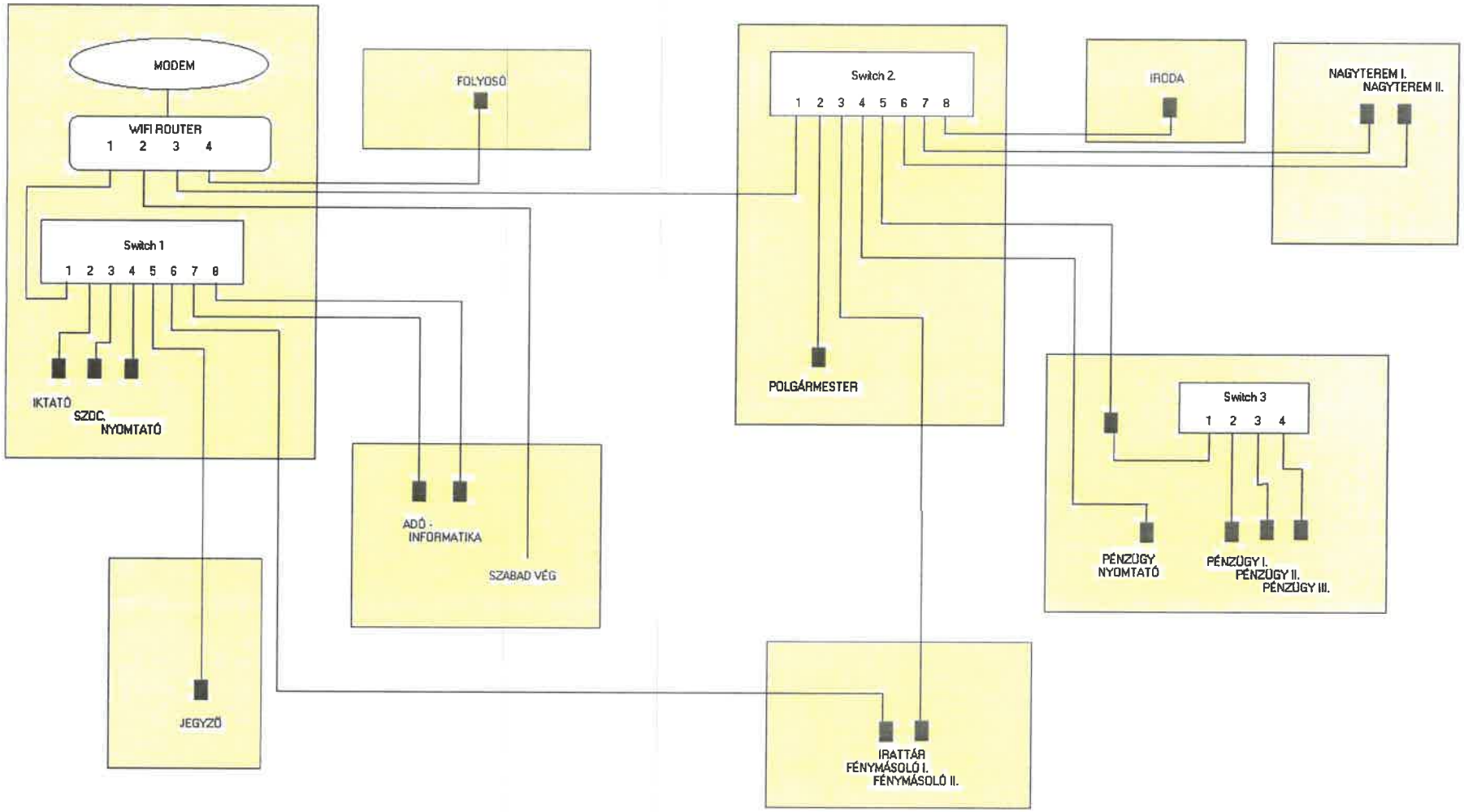
A költségvetés tervezés, és a beruházások, beszerzések során tervezni kell az informatikai biztonsági stratégia megvalósításához szükséges forrásokat.

5. sz. melléklet

A Nemesszalóki Közös Önkormányzati Hivatal informatikai hálózatának vázlata



A Nemesszalóki Közös Önkormányzati Hivatal
informatikai hálózatának vázlata



5. sz. melléklet