A NAGYSZENTJÁNOSI KÖZÖS ÖNKORMÁNYZATI HIVATAL

ELEKTRONIKUS INFORMÁCIÓS RENDSZEREK KOCKÁZATELEMZÉSI ÉS KOCKÁZATKEZELÉSI ELJÁRÁSRENDJE

Nagyszentjános

2022

Kiadva / hatályos: 2022.12.01.

Kiadta / jóváhagyta:

Németh Dániel

jegyző

Készítette:

HANGANOV Kft.
Az információbiztonság és az adatvédelem szakértője
www.hanganov.hu

TARTALOM

1 AZ ELJÁRÁSREND CÉLJA

A Nagyszentjánosi Közös Önkormányzati Hivatal (a továbbiakban: Hivatal) elektronikus információs rendszerek (a továbbiakban: EIR) kockázatelemzési és kockázatkezelési eljárásrendjének (a továbbiakban: eljárásrend) célja a Hivatal által használt EIR-ekre ható információbiztonsági kockázatok felmérésével, elemzésével, valamint kezelésével összefüggő tevékenységek, feladatok és felelősségek meghatározása.
Célja továbbá fentiek rögzítésével biztosítani azt, hogy a Hivatal által használt EIR-ekre ható kockázatok kezelése a vonatkozó, hatályos jogszabályokban, úgymint különösen az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben (a továbbiakban: Ibtv.), valamint a végrehajtására kiadott 41/2015. (VII. 15.) BM rendeletben (a továbbiakban: Vhr.) megfogalmazott információbiztonsági követelményeknek megfelelően és elvárt minőségben történjen.

2 AZ ELJÁRÁSREND HATÁLYA

2.1 Az eljárásrend személyi hatálya

Az eljárásrend személyi hatálya kiterjed a Hivatal munkavállalóira, valamint azokra a személyekre, akik részt vesznek a Hivatalnál keletkező, felhasznált, feldolgozott, tárolt, illetve továbbított adatok kezelésében.

Kiterjed továbbá mindazon, a Hivatallal munkavégzésre irányuló szerződéses jogviszonyban lévő személyekre, akik a Hivatal által működtetett informatikai rendszerek kezelésében (üzemeltetésében, karbantartásában, javításában, illetve felügyeletében) részt vesznek.

2.2 Az eljárásrend tárgyi hatálya

Az eljárásrend tárgyi hatálya kiterjed a Hivatalnál keletkezett és a Hivatal által kezelt információk teljes életciklusukon át történő kezelésével, védelmével kapcsolatos eszközökre és tevékenységekre, valamint az informatikai rendszerben üzemeltetett valamennyi hardver és szoftver elemre, amely felhasználja, feldolgozza, felügyeli, ellenőrzi, tárolja, továbbítja a Hivatalnál keletkező, illetve felhasznált adatokat.

2.3 Az eljárásrend időbeli hatálya

Az eljárásrend a kiadása napján lép hatályba és jelenlegi verziója visszavonásig – vagy a következő kiadásra kerülő verzió hatályba lépéséig – hatályos.

3 AZ ELJÁRÁSREND KIADÁSA, KEZELÉSE, FELÜLVIZSGÁLATA

Az eljárásrend kiadása, Hivatalon belüli kihirdetése és rendelkezésre állásának biztosítása (megőrzése) a Jegyző feladata és felelőssége.

Az eljárásrend felülvizsgálatát és frissítését a következő gyakorisággal kell elvégezni:

- a Hivatal kockázatmenedzsment folyamataiban, az alkalmazott módszertanban bekövetkező változás, vagy
- a Hivatal szervezetében, illetve a szerepkörökben történő jelentős változás esetén, illetve
- amennyiben biztonsági értékelés, illetve biztonságelemzés által indokolt.

Az eljárásrend felülvizsgálatának kezdeményezése, a felülvizsgálat eredményeként esetlegesen keletkezett új vagy módosított eljárásrend kiadása, valamint a felülvizsgálat megtörténtét igazoló feljegyzés megőrzése a Jegyző feladata és felelőssége.

Az eljárásrend felülvizsgálatára javaslatot tehet az információbiztonsági felelős.

Az eljárásrend felülvizsgálatát az információbiztonsági felelős köteles végrehajtani és eredményét dokumentáltan átadni a Jegyző számára.

4 DOKUMENTUMVÉDELEM

Az eljárásrend és mellékletei, az általa előírt elkészítendő és megőrzendő dokumentumok jogosulatlanok számára való megismerhetőségük és módosíthatóságuk elleni védelméről a Hivatal elektronikus formában történő tárolásuk, illetve vezetésük esetén hozzáférés- és jogosultsági rendszerrel védett tárterületen történő elhelyezéssel, illetve kizárólag a Hivatal belső hálózatán engedélyezett terjesztéssel, papír alapon a Hivatal iratkezelésre vonatkozó előírásai alapján gondoskodik.

Az eljárásrendben előírt dokumentumok elektronikus, illetve papír alapú formában egyaránt kezelhetők a Jegyző erre vonatkozó döntése szerint.

Minden dokumentum esetében biztosítani szükséges annak folyamatos rendelkezésre állását, változás esetén kinyomtatott másodpéldányának az iratkezelési szabályoknak megfelelő helyi tárolásával. A dokumentum új verziójának készítője köteles azt, illetve annak nyomtatható, elektronikus példányát a Jegyző rendelkezésére bocsátani, aki gondoskodik az aktuálisan érvényes nyomtatott példánynak a Hivatal iratkezelésre vonatkozó előírásainak megfelelő módon történő kezeléséről és megőrzéséről.

5 AZ INFORMÁCIÓBIZTONSÁGI KOCKÁZATMENEDZSMENT SZEREPLŐI

A jelen kockázatelemzési és kockázatkezelési eljárásrendben foglaltak végrehajtásának folyamatában a Hivatal információbiztonsági szervezetének alábbi szerep-, illetve felelősségi körei érintettek:

Felelősségi szint	**Szerepkör**
Vezetői általános felelősség, benne koordinációs, kommunikációs felelősség (Hivatal és hatóság, Hivatal és információbiztonsági felelős között)	Jegyző
Információbiztonsági tevékenységek tervezéséért, menedzseléséért való felelősség	Információbiztonsági felelős
Informatikai rendszerelemek működési, üzemeltetési felelőssége	IT üzemeltető
Információbiztonsági szabályok és előírások betartása	Jelen eljárásrend személyi hatálya alá tartozók (a Hivatal munkavállalói, a Hivatallal munkavégzésre irányuló szerződéses jogviszonyban lévők)

6 AZ INFORMÁCIÓBIZTONSÁGI KOCKÁZATMENEDZSMENT

Az információbiztonsági kockázatmenedzsment célja, hogy a Hivatal által a folyamatait érintően végzett általános kockázatelemzési és kezelési tevékenységhez igazodó módszertan alkalmazásával biztosítsa a Hivatal által használt elektronikus információs rendszerek, valamint az általuk kezelt adatok bizalmasságának, sértetlenségének és rendelkezésre állásának megőrzéséhez szükséges egyenszilárd, kockázatokkal arányos védelmi intézkedések kialakítását és működtetését.

A Hivatal által használt EIR-ek esetében a kockázatmenedzsment folyamataihoz kapcsolódó feladatok végrehajtását jelen módszertan szerint kell elvégezni.

6.1 Kockázatfelmérés

Az információbiztonsági kockázatok felmérésének folyamata az alábbi lépéseket foglalja magában:

- a kockázatok azonosítása,
- a kockázatok elemzése,
- a kockázatok értékelése.

A kockázatfelmérést, illetve annak aktualizálását az információbiztonsági felelős hajtja végre – a Jegyző, illetve a hivatali munkatársak közreműködésével és szükség szerint az IT üzemeltető bevonásával – a Hivatal által használt EIR-ek és működési környezetük alábbi változásai esetében:

- új EIR bevezetése,
- új rendszerelem meglévő EIR-be illesztése, illetve
- meglévő EIR más (helyi, illetve külső) elektronikus információs rendszerekhez történő kapcsolódása,

amennyiben a változás (beleértve az új fenyegetések és sebezhetőségek megjelenését is), a megváltozott körülmény vagy a tervezett változtatás az EIR-ben, illetve működési környezetében olyan jelentős eltéréssel vagy módosítással jár, amely befolyásolja az EIR biztonsági állapotát, s az alkalmazott védelmi intézkedéseket.

6.1.1 Kockázatok azonosítása

A kockázatok azonosítása során meg kell határozni azokat a fenyegetettségeket (eseményeket, veszélyeket, gyenge pontokat, sérülékenységeket, illetve védelmi intézkedést érintő hiányosságokat), amelyek a Hivatal által használt EIR-ek, illetve a kezelt adatok bizalmasságát, sértetlenségét vagy rendelkezésre állását bármilyen okból fenyegetik, függetlenül attól, hogy a Hivatalnak az adott fenyegetettségre, a fennállását előidéző helyzetre, illetve körülményre van-e ráhatása vagy sem.

Érintett adatkörök azonosítása

Az EIR által kezelt, tárolt adatok típusa és mennyisége a fenyegetettség kihasználásának lehetséges következményeit, azok hatásait, mértékét jelentősen befolyásolja, emiatt az azonosítás során meg kell határozni, hogy jogszabály által védett adatot (pl.: személyes, különleges vagy minősített), közérdekű vagy közérdekből nyilvános adatot érinthet-e és milyen mennyiségben.

Fenyegetések és forrásaik azonosítása

A fenyegetések azonosítása az iparági tapasztalatok, a fenyegetésekre, azok kihasználásának gyakoriságára vonatkozó kutatások, statisztikák, illetve trendek, valamint a korábbi biztonsági incidensek tapasztalatai alapján történhet, az informatikai infrastruktúra esetében a rendszerelem típusának megfelelő, jellemző sérülékenységek figyelembe vételével.

A fenyegetések azonosítása során az alábbi területeket kell vizsgálni:

- hardver-, szoftver, illetve hálózati- (kommunikációs) eszközök,
- fizikai környezet,
- szervezet és működése (folyamatok, eljárások),
- vezetői (menedzsment) tevékenységek,
- munkavállalók (pl.: kulcsfelhasználók),
- külső felek (pl.: szolgáltatók), tőlük való függőség.

A fenyegetés forrását tekintve lehet:

- véletlen vagy szándékos károkozás következménye,
- belső vagy külső forrásból származó,
- a műszaki paraméterekből adódó.

Kontroll környezet vizsgálata

Egy adott EIR fenyegetettségét a meglévő kontrollok hiánya vagy nem megfelelő alkalmazása (pl.: hibás vagy hiányos konfigurációs beállítás) szintén okozhatja. A kockázatok azonosítása során emiatt célszerűen a Hivatal szervezeti biztonsági szintbe sorolásának, illetve az általa használt EIR biztonsági osztály besorolásának megfelelően jogszabályban meghatározott adminisztratív, fizikai, illetve logikai védelmi intézkedések megvalósításának státuszát, működésének, hatékonyságának megfelelőségét kell elsődlegesen figyelembe venni.

Az azonosított kockázatok adatait a védelmi intézkedések típusának (adminisztratív, fizikai, logikai) megfelelő tagolásban az 1. számú melléklet – Kockázatelemzési jelentés 2 – 4. soraiban kell rögzíteni.

6.1.2 Kockázatok elemzése

A kockázatelemzés célja, hogy feltárja és értékelje a Hivatal által használt EIR-ekre vonatkozóan az azonosított kockázatok bekövetkezése esetén a lehetséges következményeket, azok kiterjedését, hatásait, a várható kár mértékét, az azonosított kockázatok bekövetkezésének reális valószínűségét, s ezek alapján meghatározza a kockázati besorolási értékeket.

A következmények értékeléséhez, az azokhoz kapcsolódó kockázati besorolási értékek meghatározásához a Vhr.-ben alkalmazott szempontrendszer alkalmazása javasolt, az alábbiak szerint:

Hatás (kár) értéke	Következmények
1	az elektronikus információs rendszer nem kezel jogszabályok által védett (pl.: személyes) adatot;
	nincs bizalomvesztés, a probléma az érintett szervezeten belül marad, és azon belül meg is oldható;
	a közvetlen és közvetett anyagi kár az érintett szervezet költségvetéséhez képest jelentéktelen;
2	személyes adat sérülhet;
	az érintett szervezet üzlet-, vagy ügymenete szempontjából csekély értékű, és/vagy csak belső (intézményi) szabályzóval védett adat vagy elektronikus információs rendszer sérülhet;
	a lehetséges társadalmi-politikai hatás az érintett szervezeten belül kezelhető;
	a közvetlen és közvetett anyagi kár eléri az érintett szervezet költségvetésének 1%-át.
3	különleges személyes adat sérülhet, személyes adatok nagy mennyiségben sérülhetnek;
	az érintett szervezet üzlet-, vagy ügymenete szempontjából érzékeny folyamatokat kezelő elektronikus információs rendszer, információt képező adat, vagy egyéb, jogszabállyal (orvosi, ügyvédi, biztosítási, banktitok, stb.) védett adat sérülhet;
	a lehetséges társadalmi-politikai hatás: bizalomvesztés állhat elő az érintett szervezeten belül, vagy szervezeti szabályokban foglalt kötelezettségek sérülhetnek;
	a közvetlen és közvetett anyagi kár eléri az érintett szervezet költségvetésének 5%-át.
4	különleges személyes adat nagy mennyiségben sérülhet;
	személyi sérülések esélye megnőhet (ideértve például a káresemény miatti ellátás elmaradását, a rendszer irányítatlansága miatti veszélyeket);
	az érintett szervezet üzlet-, vagy ügymenete szempontjából nagy értékű, üzleti titkot, vagy különösen érzékeny folyamatokat kezelő elektronikus információs rendszer, vagy információt képező adat tömegesen, vagy jelentősen sérülhet;
	a káresemény lehetséges társadalmi-politikai hatásaként a jogszabályok betartása, vagy végrehajtása elmaradhat, bekövetkezhet a bizalomvesztés a szervezeten belül, az érintett szervezet felső vezetésében, vagy vezetésében személyi felelősségre vonást kell alkalmazni;
	a közvetlen és közvetett anyagi kár eléri az érintett szervezet költségvetésének 10%-át.
5	különleges személyes adat kiemelten nagy mennyiségben sérülhet;
	emberi életek kerülnek közvetlen veszélybe, személyi sérülések nagy számban következhetnek be;
	a nemzeti adatvagyon helyreállíthatatlanul megsérülhet;
	az ország, a társadalom működőképességének fenntartását biztosító létfontosságú információs rendszer rendelkezésre állása nem biztosított;
	a lehetséges társadalmi-politikai hatás: súlyos bizalomvesztés az érintett szervezettel szemben, alapvető emberi, vagy a társadalom működése szempontjából kiemelt jogok sérülhetnek;

Hatás (kár) értéke	Következmények
	az érintett szervezet üzlet- vagy ügymenete szempontjából nagy értékű üzleti titkot, vagy kiemelten érzékeny folyamatokat kezelő elektronikus információs rendszer, vagy információt képező adat tömegesen vagy jelentősen sérülhet;
	a közvetlen és közvetett anyagi kár eléri az érintett szervezet költségvetésének 15%-át.

A bekövetkezési valószínűséget a támadási potenciál [Common Criteria Common Evaluation Methodology (CEM)] implicit ismeretének segítségével, szakértői tapasztalatokon alapuló becslés elvégzésének módszerével kell meghatározni. A támadási potenciál a sikeres támadás esélyét fejezi ki, és függ a támadási cél értékétől, a támadáshoz szükséges szakértelemtől, eszköztől és időtől, valamint a védelem erősségétől is.

A bekövetkezési valószínűség lehetséges értékei az alábbiak lehetnek:

Jelölése	Jelentése	Gyakoriság, illetve támadási potenciál
A	alacsony	Bekövetkezhet, de nem valószínű.
K	közepes	Elképzelhető, hogy bekövetkezik a jövőben (előfordulhat visszaélés vagy károkozás).
M	magas	1-2 éven belül bekövetkezhet.
N	nagyon magas	Várhatóan bekövetkezik a közeljövőben (pl.: bárki által kihasználható, ismert sérülékenység).

A kockázatelemzés eredményét az 1. számú melléklet – Kockázatelemzési jelentés adott kockázatra vonatkozó táblázatának 5. és 6. soraiban kell rögzíteni.

6.1.3 Kockázatok értékelése

A kockázatelemzés eredményeinek értékelése során az összevethetőség biztosítása, valamint a kockázati kritérium mátrixban történő megjeleníthetőségük érdekében a bekövetkezési valószínűség értékeit az alábbiak szerint számszerűsítjük:

Jelölése	Jelentése	Értéke
A	alacsony	1
K	közepes	2
M	magas	3
N	nagyon magas	4

A következmények várható hatása (kár mértéke), valamint a bekövetkezési valószínűség értékeiből az alábbiak szerint számítható a kockázati érték:

Hatás (kár) értéke / Bekövetkezési valószínűség	1	2	3	4	5
1	1	2	3	4	5
2	2	4	6	8	10
3	3	6	9	12	15
4	4	8	12	16	20

Fenti kockázati kritériumrendszer (mátrix) alapján a becsült kockázat értéke szolgál a kockázatkezelési intézkedésekre vonatkozó javaslat, illetve döntés alapjául.

A Hivatalnál alkalmazott kockázati szintek:

Kockázat értéke	Kockázati szint
1 – 2	alacsony kockázat
3 – 9	közepes kockázat
10 vagy több (10+)	

A kockázatértékelés eredményét az 1. számú melléklet – Kockázatelemzési jelentés adott kockázatra vonatkozó táblázatának 7. sorában kell rögzíteni.

6.2 Kockázatkezelés

A kockázatkezelés azon tevékenységek összessége, amely az adott EIR, illetve az általa kezelt adatok bizalmasságát, sértetlenségét, illetve rendelkezésre állását veszélyeztető kockázat megszüntetésére vagy elfogadható szintre való csökkentésére irányul. A kockázatkezelés módját a kockázat nagysága, a megvalósítás költsége és várható hatása alapján kell meghatározni.

A kockázatkezelés végrehajtásának lehetőségei:

- kockázat elfogadása, felvállalása,
- kockázat elkerülése,
- kockázat áthárítása,
- kockázat módosítása,
- maradvány kockázatok felvállalása.

6.2.1 A kockázat elfogadása, felvállalása

A Hivatal a kockázat tudatos elfogadását, felvállalását kizárólag abban az esetben alkalmazhatja, amennyiben a kockázat megfelel az alábbi elfogadási kritériumokban foglaltaknak:

- a megállapított kockázati szint alacsony;
- nem történik külső vagy belső normatíva (jogszabály, szabályozó) megsértése;
- a közvetlen, illetve közvetett kár értéke nem haladja meg a Hivatal költségvetésének 1%-át;
- a társadalmi-politikai hatás a Hivatalon belül kezelhető, nem romlik a Hivatal jó hírneve, reputációja;
- a kockázat megszüntetése vagy mérséklése nagyobb költséggel vagy erőforrás igénnyel jár, mint amekkora kár a bekövetkezésekor keletkezik vagy a helyreállításhoz szükséges;
- közvetve vagy közvetlenül testi épséget vagy emberi életet nem veszélyeztet.

Fenti kritériumok alapján a Hivatal jelen eljárásrend tárgyában – az általa használt EIR-ek kockázataival kapcsolatban – megállapított ***kockázati tűréshatára az alacsony kockázati szint*** besorolásnál került kijelölésre.

A jogszabályi nem megfelelés automatikusan magas kockázati szintnek minősül, amelynek elfogadása, felvállalása kizárólag az arra jogosult Jegyző felelőssége, melyet írásban köteles rögzíteni.

A kockázat elfogadásáról, felvállalásáról a kockázatkezelési javaslat alapján a Jegyző dönt.

6.2.2 A kockázat elkerülése

Amennyiben a kockázat költségarányos kezelésére, csökkentésére nincs reális lehetőség, akkor a kockázat előfordulásának elkerülését biztosítandó javasolható a kockázatos tevékenység, az érintett EIR vagy rendszerelem használatának megszüntetése, illetve korlátozása, amennyiben az hatékonyan kivitelezhető és megfelelő védelmet garantál.

A kockázat elkerülése kizárólag az alacsony és közepes kockázatok esetén alkalmazható kockázatkezelési eljárás.

A kockázat elkerüléséről a kockázatkezelési javaslat alapján a Jegyző dönt.

6.2.3 A kockázat áthárítása

A kockázat csökkenthető a következmények, a bekövetkezett kár vagy a felelősség áthárításával, megosztásával. A Hivatal a számára kockázatos szolgáltatással, eszközzel vagy körülménnyel kapcsolatos kockázatokat átháríthatja harmadik félre, külső partnerre (pl.: szolgáltató, beszállító, biztosító, stb.). Ebben az esetben szerződésben kell meghatározni a felelősségeket, azok elhatárolását, valamint a kockázat átvállalás mértékét (pl.: felelősségbiztosítás összege).

A kockázat áthárítása, megosztása esetén új kockázati tényezők jelenhetnek meg, meglévő kockázatok módosulhatnak. Az új kockázatokat be kell vonni a kockázatmenedzsment folyamatba, a módosult kockázatokat ismételten elemezni és kezelni szükséges.

A kockázat áthárítása az alacsony és közepes kockázatok esetén alkalmazható kockázatkezelési eljárás, amennyiben a kockázat áthárítását, megosztását követően a fennmaradó kockázat teljesíti a 6.2.1 A kockázat elfogadása, felvállalása pontban meghatározott elfogadási kritériumokat.

A kockázat áthárításáról a kockázatkezelési javaslat alapján a Jegyző dönt.

6.2.4 A kockázat módosítása

A kockázatmódosítás célja meghatározni mindazon intézkedéseket, amelyekkel a kockázat megszüntethető, megelőzhető, csökkenthető, hatása az elfogadható szintre mérsékelhető, felismerhető, illetve az azzal kapcsolatos tudatosság növelhető.

A javasolt intézkedés lehet már meglévő védelmi intézkedés módosítása vagy új kontroll bevezetése (pl.: EIR vagy rendszerelem konfigurációjának, biztonsági beállításainak módosítása; új, szigorúbb szabályozó elem előírása, stb.).

A nem vagy csak részben hatékony védelmi intézkedések esetében meg kell vizsgálni azok kivezetésének lehetőségét vagy más, esetleg már meglévő, működő kontrollokkal való helyettesíthetőségét.

A kockázat módosítása bármely kockázati szint esetén alkalmazható és preferált kockázatkezelési eljárás.

A kockázat módosításáról a kockázatkezelési javaslat alapján a Jegyző dönt.

6.2.5 Maradvány kockázat felvállalása

Amennyiben a kockázat kezelésével a kockázat szintjének a 6.2.1 A kockázat elfogadása, felvállalása pontban meghatározott elfogadási kritériumok alá csökkentése sikertelen, maradvány kockázat keletkezik.

Maradvány kockázat kizárólag abban az esetben vállalható fel, ha az a Hivatal szervezeti biztonsági szint besorolásával, illetve az érintett EIR biztonsági osztályba sorolásával kapcsolatban az Ibtv.-ben, illetve a Vhr.-ben meghatározott biztonsági követelménnyel vagy egyéb vonatkozó jogszabályi előírással nem ütközik.

A maradvány kockázat felvállalásáról a Jegyző dönt, melyet minden esetben írásban köteles rögzíteni.

6.2.6 A kockázatkezelési javaslat és végrehajtása

A kockázatkezelési javaslat tartalmazza a kockázatfelmérés eredménye alapján kiválasztott kockázatkezelési módot, valamint a megvalósításához szükséges intézkedéseket, amelyekkel az adott kockázat megszüntethető, illetve a kockázati szint a 6.2.1 A kockázat elfogadása, felvállalása pontban meghatározott elfogadási kritériumok alá csökkenthető.

A kockázat kezelésére vonatkozó javaslatot az 1. számú melléklet - Kockázatelemzési jelentés adott kockázatra vonatkozó táblázatának 8. sorában kell rögzíteni.

A kockázatkezelési javaslat végrehajtásáról a Jegyző dönt, a javaslatban meghatározott intézkedések végrehajtása – a feladatok kiosztása, intézkedés elrendelése – a Jegyző feladata és felelőssége, amelyet írásos formában az 1. számú melléklet – Kockázatelemzési jelentés adott kockázatra vonatkozó táblázatának 9. és 10. soraiban az adott intézkedés, feladat végrehajtásáért felelős és határidő megjelölésével kell rögzíteni.

Amennyiben a kockázatfelmérés új EIR bevezetését megelőzően a vonatkozó biztonsági osztály meghatározásánál hiányosságokat állapít meg, illetve abban az esetben, ha a feltárt kockázatok számossága miatt indokolt, a kockázatkezelési javaslat a kockázatkezelés elvégzésére Cselekvési Terv elkészítését írja elő.

A Cselekvési Terv tartalmazza a javasolt intézkedések konkrét megvalósítására vonatkozó részletes előírásokat, a feladatokat, határidőket és a végrehajtásukért felelős szerepköröket.

A Cselekvési Terv jóváhagyása, végrehajtásának elrendelése a Jegyző feladata és felelőssége. A tervben foglalt feladatok végrehajtásában köteles minden jelen eljárásrend személyi hatálya alá tartozó személy (hivatali munkavállaló, IT üzemeltető, stb.) közreműködni.

Új EIR bevezetése során a megállapított biztonsági osztályhoz tartozó követelményeket a rendszer használatba vételéig kötelező teljesíteni.

6.3 Kockázatmenedzsment kommunikáció

A kockázatkezelés sikeres megvalósítása érdekében a kockázatmenedzsment folyamattal kapcsolatos információk cseréje és megosztása kiemelten fontos, mely által

- az érintettek információt kapnak a Hivatal kockázatmenedzsment eredményeiről;
- megismerik a kockázatkezelés lehetséges módjait, hatékony eljárásait;
- biztonsági tudatosságuk szintje növelhető;
- felelősen lesznek képesek részt venni a kockázatkezelés végrehajtásában;
- az információk hiánya miatt bekövetkező vétlen károkozás megelőzhető, elkerülhető vagy csökkenthető.

Fentiek biztosítása céljából az 1. számú melléklet – Kockázatelemzési jelentés alapján elkészített kockázatelemzési jelentés megőrzéséről, valamint tartalmának a kockázatkezelésben érintettekkel történő megismertetéséről a Jegyző köteles a 4. Dokumentumvédelem fejezetben előírtak szerint gondoskodni.

7 ZÁRÓ RENDELKEZÉSEK

Jelen kockázatelemzési és kockázatkezelési eljárásrend a kiadása napján lép hatályba és visszavonásig érvényes.

1. SZÁMÚ MELLÉKLET – KOCKÁZATELEMZÉSI JELENTÉS

Hivatal megnevezése:	Nagyszentjánosi Közös Önkormányzati Hivatal

Azonosított kockázatonként külön táblázat kitöltése szükséges!

I. Adminisztratív védelmi intézkedésekkel kapcsolatos kockázatok

1	**Sorszám / Azonosító** (pl.: sorfolytonos számozással, pl.: K01, K02, K03, stb.)	K01
2	**Kockázat megnevezése, leírása** (az azonosított kockázat megnevezése, leírása: a fenyegetés és forrása, esetlegesen hiányzó kontrollok meghatározása)	
3	**Érintett adatok** (az adatkör típusa: személyes / különleges / minősített / közérdekű vagy közérdekből nyilvános adatok / egyéb és mennyisége, nagyságrendje)	
4	**Fenyegetés típusa** (az azonosított kockázat az EIR-ben kezelt adatok mely tulajdonságát – vagy többet is – fenyegeti: B: bizalmasság, S: sértetlenség, R: rendelkezésre állás)	
5	**Hatás (kár) értéke** (a következmény kockázati szint besorolása: 1 – 5)	
6	**Bekövetkezés valószínűsége** (A: alacsony / 1, K: közepes / 2, M: magas / 3, N: nagyon magas / 4)	
7	**Kockázat értéke** (A kockázat értékelésének eredménye: A: alacsony / 1-2; K: közepes / 3-9; M: magas / 10+)	
8	**Kockázatkezelési javaslat** (A kockázat kezelésére vonatkozó szakértői javaslat, pl.: új védelmi intézkedés bevezetése, az adott EIR vagy rendszerelem kivezetése, cseréje, stb.)	
9	**A kockázat kezelésével kapcsolatos döntés** (A kockázat kezelését célzó vezetői döntés, amely lehet: a kockázat elfogadása, felvállalása; a kockázat elkerülése; a kockázat áthárítása; a kockázat módosítása; a maradvány kockázatok felvállalása.	
10	**A kockázat kezeléséhez szükséges intézkedések, feladatok** (Az adott intézkedés, feladat végrehajtásáért felelős és határidő megjelölésével. / Nem igényel intézkedést.)	
202__._____._____		aláírás

II. Fizikai védelmi intézkedésekkel kapcsolatos kockázatok

1	**Sorszám / Azonosító** (pl.: sorfolytonos számozással, pl.: K01, K02, K03, stb.)	K02
2	**Kockázat megnevezése, leírása** (az azonosított kockázat megnevezése, leírása: a fenyegetés és forrása, esetlegesen hiányzó kontrollok meghatározása)	
3	**Érintett adatok** (az adatkör típusa: személyes / különleges / minősített / közérdekű vagy közérdekből nyilvános adatok / egyéb és mennyisége, nagyságrendje)	
4	**Fenyegetés típusa** (az azonosított kockázat az EIR-ben kezelt adatok mely tulajdonságát – vagy többet is – fenyegeti: B: bizalmasság, S: sértetlenség, R: rendelkezésre állás)	
5	**Hatás (kár) értéke** (a következmény kockázati szint besorolása: 1 – 5)	
6	**Bekövetkezés valószínűsége** (A: alacsony / 1, K: közepes / 2, M: magas / 3, N: nagyon magas / 4)	
7	**Kockázat értéke** (A kockázat értékelésének eredménye: A: alacsony / 1-2; K: közepes / 3-9; M: magas / 10+)	
8	**Kockázatkezelési javaslat** (A kockázat kezelésére vonatkozó szakértői javaslat, pl.: új védelmi intézkedés bevezetése, az adott EIR vagy rendszerelem kivezetése, cseréje, stb.)	
9	**A kockázat kezelésével kapcsolatos döntés** (A kockázat kezelését célzó vezetői döntés, amely lehet: a kockázat elfogadása, felvállalása; a kockázat elkerülése; a kockázat áthárítása; a kockázat módosítása; a maradvány kockázatok felvállalása.	
10	**A kockázat kezeléséhez szükséges intézkedések, feladatok** (Az adott intézkedés, feladat végrehajtásáért felelős és határidő megjelölésével. / Nem igényel intézkedést.)	
202__._____.____		aláírás

III. Logikai védelmi intézkedésekkel kapcsolatos kockázatok

1	**Sorszám / Azonosító** (pl.: sorfolytonos számozással, pl.: K01, K02, K03, stb.)	K03
2	**Kockázat megnevezése, leírása** (az azonosított kockázat megnevezése, leírása: a fenyegetés és forrása, esetlegesen hiányzó kontrollok meghatározása)	
3	**Érintett adatok** (az adatkör típusa: személyes / különleges / minősített / közérdekű vagy közérdekből nyilvános adatok / egyéb és mennyisége, nagyságrendje)	
4	**Fenyegetés típusa** (az azonosított kockázat az EIR-ben kezelt adatok mely tulajdonságát – vagy többet is – fenyegeti: B: bizalmasság, S: sértetlenség, R: rendelkezésre állás)	
5	**Hatás (kár) értéke** (a következmény kockázati szint besorolása: 1 – 5)	
6	**Bekövetkezés valószínűsége** (A: alacsony / 1, K: közepes / 2, M: magas / 3, N: nagyon magas / 4)	
7	**Kockázat értéke** (A kockázat értékelésének eredménye: A: alacsony / 1-2; K: közepes / 3-9; M: magas / 10+)	
8	**Kockázatkezelési javaslat** (A kockázat kezelésére vonatkozó szakértői javaslat, pl.: új védelmi intézkedés bevezetése, az adott EIR vagy rendszerelem kivezetése, cseréje, stb.)	
9	**A kockázat kezelésével kapcsolatos döntés** (A kockázat kezelését célzó vezetői döntés, amely lehet: a kockázat elfogadása, felvállalása; a kockázat elkerülése; a kockázat áthárítása; a kockázat módosítása; a maradvány kockázatok felvállalása.	
10	**A kockázat kezeléséhez szükséges intézkedések, feladatok** (Az adott intézkedés, feladat végrehajtásáért felelős és határidő megjelölésével. / Nem igényel intézkedést.)	
202__._____.____		
		aláírás