Informatikai Biztonsági Szabályzat

Hatályos: 2023. július 1. napjától

1 Általános rész

1.1. A szabályzat célja

A Nyőgéri Közös Önkormányzati Hivatal (a továbbiakban: Hivatal) Informatikai Biztonsági Szabályzatának (a továbbiakban: szabályzat) célja, hogy a hatálya alá tartozó elektronikus információs rendszerek teljes életciklusában biztosítsa az elektronikus információs rendszerben kezelt adatok és információk bizalmassága, sértetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer és elemeinek sértetlensége és rendelkezésre állása zárt, teljes körű, folytonos és kockázatokkal arányos védelmét. Ennek érdekében meghatározza a szervezetnek a jogszabályban előírt adminisztratív, fizikai és logikai védelmi intézkedéseket, amelyek támogatják:

a) a megelőzést és a korai figyelmeztetést,

b) az észlelést,

c) a reagálást,

d) a biztonsági események kezelését.

A szabályzat céljainak megvalósítását annak figyelembe vételével kell megszervezni, hogy a Hivatal informatikai szakrendszerei az önkormányzati ASP központban üzemelnek, továbbá olyan központi informatikai rendszerekhez csatlakozik, melyek biztonságáért az üzemeltető állami szerv a felelős. Ennek megfelelően:

- Az önkormányzati ASP rendszer szakrendszereinek biztonsági osztályba sorolását a Magyar Államkincstártól kapja meg, azokat nem kell biztonsági osztályba sorolni.
- Az állami központi informatikai rendszereket az azokat üzemeltető szervek sorolják biztonsági osztályba.
- A védelmi intézkedéseket elsősorban a jogszabály alapján kijelölt szolgáltató követelményeinek megfelelően kell meghatározni és alkalmazni.
- A védelmi intézkedések meghatározásánál figyelembe kell venni, hogy a Hivatal saját, helyi informatikai rendszert üzemeltet.
- A Hivatal információbiztonsági tevékenysége elsődlegesen az elektronikus információs rendszerrel kapcsolatba kerülő személyek információbiztonsággal kapcsolatos kötelezettségeinek szabályozására, számonkérésére terjed ki, addig a mértékig, ameddig a szervezet vagy az egyes személyek tevékenysége az elektronikus információs rendszerre hatást tud gyakorolni.

1.2. A szabályzat hatálya

1.2.1. Személyi hatály

A szabályzat személyi hatálya kiterjed a Hivatal informatikai rendszereit használó, valamint azzal egyéb céllal kapcsolatba kerülő természetes és jogi személyekre:

- a választott tisztségviselőkre,

- 187/2015. (VII. 13.) Korm. rendelet az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról
- 257/2016. (VIII. 31.) Korm. rendelet az önkormányzati ASP rendszerről
- 370/2011. (XII.31.) Korm. rendelet a költségvetési szervek belső kontrollrendszeréről és belső ellenőrzéséről
- 451/2016. (XII. 19.) Korm. rendelet az elektronikus ügyintézés részletszabályairól
- 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről

A jelen szabályzatban használt fontosabb fogalmakat a 6.5 Fogalmak jegyzéke ismerteti.

1.5. Az elektronikus információbiztonsággal kapcsolatos szerepkörök és feladatok

Az elektronikus információbiztonsággal kapcsolatos tevékenységek, feladatok és felelősségek az alábbi szerepkörökhöz vannak rendelve:

- A szervezet vezetője, a jegyző
- Az elektronikus információs rendszer biztonságáért felelős személy
- A felhasználó
- Kulcsfelhasználók (önkormányzati ASP adminisztrátor, szakrendszeri ASP adminisztrátor, ASP és helyi kulcsfelhasználó)
- A rendszergazda
- A szolgáltató

Az egyes szerepkörökhöz rendelt feladatok és felelősségek a következők:

1.5.1. Jegyző

Mint a szervezet vezetője az elektronikus információs rendszerek védelméről a következők szerint gondoskodik:

a. biztosítja az elektronikus információs rendszerre irányadó biztonsági osztály tekintetében a jogszabályban meghatározott követelmények teljesülését,
b. biztosítja a szervezetre irányadó biztonsági szint tekintetében a jogszabályban meghatározott követelmények teljesülését,
c. az elektronikus információs rendszer biztonságáért felelős személyt nevez ki vagy bíz meg,
d. meghatározza a szervezet elektronikus információs rendszerei védelmének felelőseire, feladataira és az ehhez szükséges hatáskörökre, felhasználókra vonatkozó szabályokat, illetve kiadja az Informatikai Biztonsági Szabályzatot,
e. gondoskodik az elektronikus információs rendszerek védelmi feladatainak és felelősségi köreinek oktatásáról, saját maga és a szervezet munkatársai információbiztonsági ismereteinek szinten tartásáról,

i. Folyamatosan figyelemmel kíséri a biztonsági osztályba sorolás és a szervezeti szint felülvizsgálatára, módosítására okot adó körülményeket, kezdeményezi és előkészíti a módosított besorolásokat.
j. Három évente, illetve a jogszabály által meghatározott egyéb esetekben kezdeményezi a besorolások felülvizsgálatát, előkészíti a szükséges módosításokat.
k. Véleményezi az elektronikus információs rendszerek biztonsága szempontjából a szervezet e tárgykört érintő szabályzatait és szerződéseit.
l. Kapcsolatot tart a hatósággal és a Kormányzati Eseménykezelő Központtal.

Felelőssége: felelős a jogszabályokban és jelen szabályzatban meghatározott feladatainak végrehajtásáért.

1.5.3. Felhasználó

a. A Hivatal elektronikus informatikai rendszereinek felhasználója munkaköri leírásában szereplő feladatai és az egyedi vezetői munkautasítások alapján használhatja a számára engedélyezett informatikai eszközöket és szolgáltatásokat. Ennek során az információvédelem területén az adott helyzetben általában elvárható magatartást köteles tanúsítani, és tartózkodni minden károkozó tevékenységtől.
b. Felelősséggel tartozik a munkavégzés céljából átvett eszközért, köteles megőrizni annak hardver- és szoftverintegritását. Az integritás sérelmének minősül a rendeltetésellenes használat, hardveres vagy szoftveres módosítás.
c. A részére kiadott azonosítókat és hitelesítő eszközöket bizalmasan kell kezelnie, nem szabad kiadni azokat más személynek, illetve nem szabad felhasználnia másik felhasználó azonosítóját és hitelesítő eszközét, az erre irányuló esetleges kérést vagy utasítást meg kell tagadnia.
d. Köteles azonnal értesíteni munkahelyi vezetőjét, ha az informatikai rendszer rendelkezésre állása, a kezelt adatok bizalmassága és sértetlensége sérült, vagy ennek közvetlen veszélye fennáll.

Felelőssége: felelős a jelen szabályzatban és a vezetői utasításokban meghatározott szabályok betartásáért, az informatikai rendszerben végzett műveleteiért.

1.5.4. Kulcsfelhasználó

Feladatai:

a. Beállítja, karbantartja, illetve törli a felhasználói fiókokat, jogosultságokat a helyi hozzáférésekre vonatkozóan.
b. Segítséget nyújt a felhasználóknak a jelszavak beállításához és időszakos vagy eseti cseréje során.
c. Az önkormányzati ASP adminisztrátori és/vagy szakrendszer adminisztrátori feladatait az ASP rendszerben meghatározott szabályok szerint végzi.

Felelőssége: felelős azért, hogy a felhasználók kizárólag a jegyző által engedélyezett hozzáférési jogosultságokat kapják meg, a visszavont fiókokat és jogosultságokat pedig haladéktalanul törölje.

1.5.5. Rendszergazda

rendelet) kijelölt szolgáltatót vesz igénybe. A Hivatal szervezeti egységekre nem tagolódik, így szervezeti egységekre vonatkozóan a biztonsági szintbe sorolás nem értelmezhető.

A Hivatal biztonsági szintjét a jogszabályban meghatározottak szerint kell értékelni, és szükség szerint a 4. biztonsági szint elérését szolgáló intézkedéseket cselevési tervben kell meghatározni. Az intézkedések meghatározása során figyelembe kell venni, hogy a hivatal adatkezelése alapvetően központi szolgáltatások igénybevételére alapul.

1.5.9. Védelmi intézkedések

A szabályzat 2.-4. fejezete a 41/2015. (VII. 15.) BM rendelet és a Magyar Államkincstár által kiadott, az önkormányzati ASP rendszerekhez történő csatlakozáshoz megvalósítandó informatikai biztonsági követelmények teljesítését szolgáló védelmi intézkedéseket, eljárásokat és szabályokat rögzíti.

A Hivatal az előírt nyilvántartásokat elektronikusan, az erre kialakított IBF portálon vezeti. A nyilvántartásban a változásokat 5 munkanapon belül át kell vezetni.

2.1.5 Az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárás

Az elektronikus információbiztonsággal kapcsolatos engedélyezés kiterjed minden, a Hivatal hatáskörébe tartozó emberi, fizikai és logikai erőforrásra, eljárási és védelmi követelményszintre és folyamatra. Az ezekkel kapcsolatos engedélyeket – ha jogszabály vagy a Hivatalra vonatkozó utasítás ettől eltérően nem rendelkezik - a jegyző, illetve a helyettesítésével megbízott személy adhatja ki.

Az emberi, fizikai és logikai erőforrásra, eljárási és védelmi követelményszintre és folyamatra vonatkozó engedélyezési eljárások speciális szabályait a szabályzat vonatkozó fizikai és logikai védelmi intézkedéseinek meghatározása tartalmazza.

2.2 Kockázatelemzés

2.2.1 Kockázatelemzési és kockázatkezelési eljárásrend

A Hivatal integrált kockázatkezelési módszertant és eljárásrendet alkalmaz, melyet a Hivatal Kockázatkezelési szabályzata tartalmaz.

2.2.2 Biztonsági osztályba sorolás

Az önkormányzati ASP rendszer szakrendszereinek biztonsági osztályba sorolását a Magyar Államkincstártól kapja meg, azokat nem kell biztonsági osztályba sorolni.

A Hivatal egyéb informatikai szakrendszert nem üzemeltet, ide nem értve a szakrendszernek nem minősülő, a papíralapú szöveges iratok előkészítését, szerkesztését, valamint nyilvántartását támogató irodai és egyéb, jogszabály alapján archiválást nem igénylő alkalmazásokat.

2.2.3 Kockázat elemzés

Kockázatelemzést évente kell végezni. A kockázatelemzés dokumentumai nem nyilvános iratok.

Az IBF a Kockázatkezelési szabályzatban meghatározottak szerint együttműködik a belső ellenőrrel, részt vesz az évente kötelezően elvégzendő kockázatelemzésben. Ennek eredményeképpen meghatározza a következő belső audit szempontjait, melyet a jegyző hagy jóvá.

A kockázatelemzés eredményét, a szükséges intézkedéseket az érintett önkormányzatok polgármesterei, szükség szerint az önkormányzatok képviselő testületei számára, a jegyző a hivatali beszámolóban ismerteti. Amennyiben a kockázatkezelés anyagi ráfordítással járó intézkedéseket tesz szükségessé, a jegyző – az IBF és más kijelölt munkatársak bevonásával – elkészíti az ehhez szükséges előterjesztést, gondoskodik az önkormányzati döntés végrehajtásról.

A kockázatelemzés eredményeképpen megállapított szervezeti szintű intézkedésekről a jegyző munkaértekezleten tájékoztatja az érintett munkatársakat.

- Az önkormányzat veszélyelhárítási tervében meghatározott estekben végrehajtja a Hivatal részére kijelölt feladatokat.
- A Hivatal ügymenetét tartósan akadályozó káresemény, vészhelyzet esetén a jogszabályban meghatározottak szerint igazgatási szünetet rendel el, intézkedik a helyreállítás és az újraindítás érdekében szükséges feladatok végrehajtására.
- A Hivatal ügymenetét részlegesen és/vagy csak munkanapon belüli rövid időre akadályozó káresemény, vészhelyzet esetén intézkedik a helyreállítás és az újraindítás érdekében szükséges feladatok végrehajtására.
- A bekövetkezett káresemény, vészhelyzet jellegétől függően értesíti az illetékes hatóságokat.

2.4.2 Üzletmenet folytonossági terv informatikai erőforrás kiesésekre

Az informatikai erőforrások kiesése esetén a jegyző az IBF bevonásával értékeli a kialakult helyzetet és meghatározza a kisesés miatt végrehajtandó intézkedéseket.

- Az internet szolgáltatás hivatali épületre, kirendeltségre kiterjedő kiesése esetén a halaszthatatlan adatfeldolgozást igénylő ügyek (banki utalások, határidős jelentések) tekintetében a jegyző intézkedik, hogy az érintett dolgozók átmenetileg a kieséssel nem érintett intézményben vagy kirendeltségen folytassák a munkát.
- A belső hálózatot és egyedi számítógépeket érintő átmeneti és korlátozott kiesés esetén a jegyző értesíti a javítást végző szolgáltatót a hiba elhárítása érdekében, szükség szerint az előző pontban leírtak szerint gondoskodik a halaszthatatlan feladatok végrehajtásáról.
- Ha az erőforrás kiesés visszavezethető kártékony kódra vagy illetéktelen külső beavatkozásra, a kárelhárítással egyidejűleg az IBF értesíti az illetékes hatóságot.

Az üzletmenet folytonosságának sérülését okozó káresemények helyreállítását követően az IBF soron kívül ellenőrzést végez, és javaslatot tesz a hasonló jellegű veszélyhelyzetek megelőzésére, a kiesések következményeinek hatékony felszámolását biztosító feladatok tervezésére.

2.4.3 Kritikus rendszerelemek meghatározása

A Hivatal informatikai rendszereinek kritikus elemei:

- Az önkormányzati ASP rendszer, mint szolgáltatás.
- Az önkormányzati ASP rendszer elérését biztosító hálózat (WAN/LAN, internet szolgáltatás, NTG hálózat) és az ehhez kapcsolódó számítógépek (kliensek).

Nem kritikus rendszerelemek: az irodai munkát támogató egyéb elektronikus berendezések, nyomtatók, szkennerek stb.

2.4.4 A folyamatos működésre felkészítő képzés

A felhasználók a szokásos informatikai biztonsági oktatás keretében kapnak felkészítést az ügymenet folyamatosságának fenntartását biztosító feladataikról.

Az IBF soron kívüli oktatást tart az üzletmenet folytonosságot érintő káreseményt követően, ha az visszavezethető felhasználói mulasztásra, illetve, ha megfelelő felhasználói magatartással megelőzhető lett volna.

A munkakörök és feladatok biztonsági szempontú besorolását az IBSZ módosításának szükségessége esetén felül kell vizsgálni.

2.5.3 A személyek ellenőrzése

A jegyző a köztisztviselőt a kinevezés előtt a vonatkozó jogszabályok alapján ellenőrzi. Az elektronikus információs rendszerhez való hozzáférés jogosságát - az alkalmazási feltételeknek való megfelelés és a köztisztviselő kinevezése esetén - a betöltött munkakörnek megfelelő mértékben igazoltnak kell tekinteni.

Az egyes rendszerelemek karbantartásával, javításával és a rendszergazda feladatok ellátásával megbízott személytől, ha nem köztisztviselő, a büntetlen előélet igazolására vonatkozóan a megbízáskor (szerződéskötéskor) 3 hónapnál nem régebbi erkölcsi bizonyítványt, illetve szakmai életútját bemutató referenciaigazolást kell kérni.

2.5.4 Eljárás a jogviszony megszűnésekor

A Hivatal munkavégzésre irányuló jogviszony megszűnésekor az alábbi feladatokat végzi el:

- legkésőbb a jogviszony fennállásának utolsó napján megszünteti a hozzáférési jogosultságot az elektronikus információs rendszerhez, és – ha volt ilyen – a riasztó rendszerhez;
- megszünteti vagy visszaveszi a személy egyéni hitelesítő eszközeit;
- visszaveszi a fizikai belépéshez használt kulcsokat;
- tájékoztatja a kilépőt az esetleg reá vonatkozó, jogi úton is kikényszeríthető, a jogviszony megszűnése után is fennálló kötelezettségekről;
- visszaveszi az érintett szervezet elektronikus információs rendszerével kapcsolatos, tulajdonát képező összes eszközt;
- megtartja magának a hozzáférés lehetőségét a kilépő személy által korábban használt, kezelt elektronikus információs rendszerekhez és szervezeti információkhoz;
- e-mailben értesíti az IBF-t és a rendszergazdát a jogviszony megszűnéséről;
- a jogviszonyt megszüntető személy elektronikus információs rendszerrel, vagy annak biztonságával kapcsolatos esetleges feladatainak ellátásáról a jogviszony megszűnését megelőzően gondoskodik;
- a jogviszony megszűnésekor a jogviszonyt megszüntető személy esetleges elektronikus információs rendszert, illetve abban tárolt adatokat érintő, elektronikus információbiztonsági szabályokat sértő magatartását megelőzi.

2.5.5 Az áthelyezések, átirányítások és kirendelések kezelése

A Hivatalban nem különülnek el a szervezeti egységek, ezért az áthelyezések, átirányítások és kirendelések kezelése nem igényel szabályozást.

A munkakör megváltozása, pl. helyettesítés esetén a jegyző, vagy az általa megbízott önkormányzati ASP adminisztrátor gondoskodik az elektronikus információs rendszerhez való hozzáférési jogosultságok beállításáról az új munkakörnek megfelelően, vagy intézkedik, hogy a szakrendszeri adminisztrátor ezeket állítsa be. Egyidejűleg a már szükségtelenné váló jogosultságokat vissza kell vonni.

A Hivatal az önkormányzati ASP rendszert elérő számítógépeken az interneten elérhető tartalmakat indokolt esetben szűri, erről az érintett munkatársakat tájékoztatja.

2.6 Tudatosság és képzés

2.6.1 Kapcsolattartás az elektronikus információbiztonság jogszabályban meghatározott szervezetrendszerével, és az e célt szolgáló ágazati szervezetekkel

A jegyző és az IBF a jogszabályokban meghatározottak szerint kapcsolatot tart a Nemzeti Elektronikus Információbiztonsági Hatósággal, a Magyar Államkincstárral, a NISZ Zrt.-vel, a Kormányhivatallal, valamint a jogszabályokban kijelölt más illetékes szervezetekkel, ennek során kölcsönösen tájékoztatják egymást a hatáskörükbe tartozóan megtett intézkedésekről.

2.6.2 Képzési eljárásrend

Az elektronikus információs rendszerek biztonságával összefüggő oktatásra az IBF évente készít tervet, melyet a jegyző hagy jóvá.

Az oktatást lehetőség szerint úgy kell megtartani, hogy minden munkatárs részt tudjon venni rajta, pl. online videoelőadás formájában. Az oktatás során kapott ismeretekről kérdőív kitöltetésével vagy más megfelelő formában meg kell győződni.

Az új belépő dolgozóknak meg kell ismerni jelen szabályzatot, illetve annak a felhasználói ismereteket tartalmazó kivonatát, és erről a munkatársat nyilatkoztatni szükséges.

A képzés helyzetét az IBF az éves jelentés keretében felülvizsgálja, és javaslatot tesz a szükséges intézkedésekre.

2.6.3 Biztonság tudatosság képzés

A lehetséges belső fenyegetések felismerése érdekében az IBF gondoskodik a felhasználók biztonsággal kapcsolatos rendszeres tájékoztatásáról, felkészítéséről. Ennek keretében:

- Felhívja a figyelmet az informatikai rendszereket fenyegető aktuális veszélyekre, a megelőzés, az észlelés és a szükséges jelzés érdekében teendő felhasználói feladatokra.
- Az új belépő munkatársak részére évente aktualizálja a jelen szabályzatból a felhasználók oktatásához készített kivonatot.
- Az elektronikus rendszerben bekövetkezett változásokhoz kapcsolódóan tájékoztatja a felhasználókat a megváltozott követelményekről, intézkedésekről.

2.6.4 Belső fenyegetés

Minden felhasználónak kötelessége jelenteni a jegyzőnek, ha az informatikai rendszert érintő belső fenyegetést észlel. A munkahelyi értekezletek keretében fel kell a felhasználók figyelmét hívni arra, hogy az informatikai rendszer biztonsága a Hivatal működésének előfeltétele, ezért minden olyan körülményt, magatartást (mulasztást) időben fel kell tárni, ami a rendszer rendelkezésre állását, az adatok bizalmasságát és sértetlenségét veszélyezteti.

3 Fizikai védelmi intézkedések

3.1 Fizikai védelmi eljárásrend

A Hivatal elektronikus információs rendszereinek fizikai védelmét a tűzvédelmi, vagyonvédelmi, munkavédelmi és más kapcsolódó jogszabályok, önkormányzati és hivatali szabályzatok figyelembe vételével kell megszervezni.

A fizikai védelmi szabályok kialakítása, módosítása és ellenőrzése során az egyes szakterületek felelőseinek (IBF, tűzvédelmi felelős stb.) együttműködését a jegyző koordinálja.

A Hivatalban végrehajtandó, a fizikai védelmet érintő felújítás, karbantartás előkészítésébe az IBF-t a szükséges mértékben be kell vonni.

A fizikai védelem helyzetét az IBF évente ellenőrzi, értékeli és javaslatot tesz a szükséges intézkedésekre.

3.2 Fizikai belépési engedélyek

A Hivatal épületeibe a belépést és ott tartózkodást a jegyző engedélyezi.

A Hivatal épületeiben, hivatali időben külön engedély nélkül tartózkodhatnak:

- a polgármester;
- a választott tisztségviselők;
- a hivatal köztisztviselő jogállású munkatársai;
- egyéb munkavégzésre irányuló jogviszony alapján munkát végző személyek, akiknek kijelölt munkahelyük a Hivatalban van;
- a szolgáltatók a szerződésben meghatározott feltételeknek (kísérő, előzetes bejelentés stb.) megfelelően.

A hivatali időn kívül belépésre jogosultakról, a belépés esetleges külön feltételeiről (riasztó, kulcs használat) a jegyző nyilvántartást vezet.

3.3 A fizikai belépés ellenőrzése

A hivatali épületbe munkavégzés céljából belépő munkatársak jelenléti ívet vezetnek. A munkaidőn kívüli belépést, illetve az épületnyitást a riasztórendszer is naplózza ott, ahol telepítve van.

A Hivatalba ügyintézés céljából belépő ügyfelek szabad mozgását az ügyfélvárónak kijelölt területre kell korlátozni. A Hivatal ügyintézésre kijelölt irodáiba az ügyfél csak az illetékes munkatárs engedélyével és felügyelete mellett léphet be, és tartózkodhat ott.

Az ügyfelet vagy más látogatót nem szabad felügyelet nélkül hagyni olyan helyiségben, ahol aktív informatikai eszközök működnek, illetve ahol az informatikai infrastruktúra kritikus elemei hozzáférhetők (pl. kapcsoló szekrény, kábelelosztó, szünetmentes táp).

A Hivatal minden munkatársának kötelessége jelenteni a jegyzőnek, ha az épületben vagy annak valamely helyiségében illetéktelen személy tartózkodik, vagy a belépési rendet veszélyeztető egyéb körülményt (riasztó, zár meghibásodás, kulcs elvesztése stb.) észlelt.

3.9 Áramellátó berendezések és kábelezés

Az informatikai infrastruktúra elektromos ellátását biztosító technikai eszközöket (kapcsoló- és biztosíték tábla, szünetmentes táp, hosszabbítók stb.) védeni kell az illetéktelen hozzáféréstől, sérüléstől és rongálástól. Ennek során figyelembe kell venni a vonatkozó műszaki, tűzvédelmi, érintésvédelmi és egyéb előírásokat. Az áramellátó berendezések és kábelek telepítését, karbantartását és javítását csak megfelelő szakképesítéssel és engedéllyel rendelkező személy végezheti.

A munkatársak figyelmét fel kell hívni arra, hogy az irodai elosztók, csatlakozók, hosszabbítók épségére ügyeljenek, a meghibásodott, sérült eszközöket ne használják tovább.

3.10 Tűzvédelem

A Hivatalban a tűzvédelmi feladatokat az ezzel megbízott külső személy látja el. A Hivatalnak az informatikai rendszerek tekintetében is meg kell felelni a hatályos tűzvédelmi előírásoknak.

3.11 Víz-, és más, csővezetéken szállított anyag okozta kár elleni védelem

Az elektronikus információs rendszer elemeit meg kell védeni a víz-, és más, csővezetéken szállított anyag okozta károkkal szemben. Ennek érdekében nem szabad csővezeték, víztározó, vízmelegítő és hasonló funkciójú, folyadékot, gázt vagy gőzt tartalmazó berendezés közelében aktív informatikai eszközöket elhelyezni.

A munkatársakat munkavédelmi, tűzvédelmi és egyéb oktatás keretében tájékoztatni kell az elzárószelepek helyéről, vészhelyzetben történő használatának szabályairól, a vészhelyzetben teendő halaszthatatlan intézkedésekről.

3.12 Be- és kiszállítás

Az informatikai eszközök javítására, karbantartására a jegyző által kijelölt szakszervíz, vállalkozó jogosult a szerződésben, megrendelésben rögzített feltételeknek megfelelően.

A Hivatal épületéből személyes adatokat tároló eszközt kivételesen, csak a jegyző vagy kijelölt munkatársának felügyelete mellett szabad kivinni. Egyéb esetben az adattároló eszközt a javítandó berendezésből, annak kiszállítása előtt el kell távolítani, és illetéktelen hozzáféréstől védett, biztonságos helyen kell tárolni.

A kiszállított eszközökről a jegyző nyilvántartást vezet.

3.13 Az elektronikus információs rendszer elemeinek elhelyezése

A Hivatalban az informatikai eszközöket – a helyi adottságok keretein belül – úgy kell elhelyezni, hogy a lehető legnagyobb mértékben védve legyenek a jogosulatlan fizikai hozzáféréstől és az üzemi működési feltételeket veszélyeztető fizikai hatásoktól (hő-, nap-, elektromágneses sugárzás, rezgés stb.).

Az informatikai eszközök elhelyezése, az irodák berendezése során figyelembe kell venni az alapvető ergonómiai és munkavédelmi követelményeket annak érdekében, hogy napi munkavégzést, ügyintézést az irodában elhelyezett eszközök, kábelek ne akadályozzák.

4 Logikai védelmi intézkedések

4.1 Általános védelmi intézkedések

A jegyző megfogalmazza, dokumentálja, és kihirdeti az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárási folyamatokat, amelyek kiterjednek minden emberi, fizikai és logikai erőforrásra. Felügyeli az elektronikus biztonsági rendszer és környezet biztonsági állapotát, meghatározza az információbiztonsággal összefüggő szerepköröket és felelősségi köröket.

Az információbiztonsággal összefüggő szerepköröket jelen szabályzat Általános része ismerteti. Az egyes szerepköröket betöltő személyeket a jegyző a munkaköri leírásokban, illetve az IBF, a szolgáltatók és a rendszergazda szerepkört illetően a szerződéskötéssel jelöli ki.

4.1.1 Az elektronikus információs rendszer kapcsolódásai

A Hivatalban nem engedélyezett az információs rendszerek összekapcsolása más elektronikus információs rendszerekkel, ide nem értve az önkormányzati ASP rendszer használatával összefüggő, jogszabályban meghatározott központi szolgáltatóhoz történő kapcsolódást.

Azokon az eszközökön, amelyeken önkormányzati ASP rendszer van használatban vagy adattovábbítás történik rá, tilos olyan alkalmazást használni, amely az eszközt az ASP Központon kívüli harmadik féllel köti össze, és amellyel lehetőség van távoli támogatásra, vezérlésre, távoli hozzáférésre, képernyő átvételére stb.

4.1.2 Belső rendszer kapcsolatok

A Hivatal belső információs rendszereinek összekapcsolását a jegyző engedélyezheti.

Nem minősül rendszerösszekapcsolásnak az általános célú irodai szoftverekkel előállított fájlok megosztása a helyi operációs rendszer és/vagy helyi hálózati kiszolgáló szolgáltatásain keresztül.

4.1.3 Külső kapcsolódásokra vonatkozó korlátozások

A Hivatalban engedélyezett a kapcsolódás a jogszabályban meghatározott központi szolgáltatásokhoz, illetve a munkakör ellátásához szükséges adatbázisokhoz és információs forrásokhoz. Nem engedélyezett a munkakör ellátásával közvetlenül össze nem függő hálózatokhoz és szolgáltatásokhoz történő kapcsolódás.

4.1.4 Személybiztonság

Minden, a személybiztonsággal kapcsolatos eljárás vagy elvárás kiterjed a Hivatal teljes személyi állományára, valamint minden olyan természetes személyre, aki a Hivatal elektronikus információs rendszereivel kapcsolatba kerül vagy kerülhet. Jelen szabályzat személyi hatálya ennek megfelelően került meghatározásra. A szabályzat felülvizsgálata során figyelembe kell venni azokat a körülményeket, melyek a személyi hatály módosítását indokolhatják.

Azokban az esetekben, amikor a Hivatal elektronikus információs rendszereivel tényleges, vagy feltételezhető kapcsolatba kerülő személy nem az érintett szervezet tagja, a tevékenység alapját képező jogviszonyt megalapozó szerződés, megállapodás megkötése során kell, mint kötelezettséget érvényesíteni (ideértve a szabályzatok, eljárásrendek megismerésére és betartására irányuló

A Hivatalban csak az önkormányzati ASP rendszerhez előírt hardver és szoftver konfigurációnak megfelelő számítógépeket és egyéb eszközöket szabad használni. Az ezen követelményeket nem sértő konfigurációs eltéréseket a jegyző engedélyezi.

A Hivatal helyi rendszereinek hardver és szoftver konfigurációját a szállítói alapbeállításoknak megfelelően kell üzembe állítani. Az alapkonfigurációk dokumentációit, telepítő készleteit a jegyző által kijelölt tárolási helyen kell tartani úgy, hogy egy esetleges biztonsági incidens után a helyreállítást a lehető legrövidebb időn belül el lehessen végezni.

4.3.2 Legszűkebb funkcionalitás

A Hivatal informatikai eszközeinek meg kell felelni a munkakör ellátásához szükséges funkcionális követelményeknek, ezen túl azonban további szolgáltatásokat az informatikai rendszerben nem szabad engedélyezni. Tilos olyan programtermékek telepítése, melyek a munkakör ellátásához nem szükségesek. A nem használt protokollokat, portokat a rendszergazdának kell letiltani.

4.3.3 Duplikálás elleni védelem

A Hivatal nem veszi nyilvántartásba azokat az informatikai eszközöket, melyek más, jellemzően központi szerv nyilvántartásában szerepelnek.

4.3.4 A szoftver használat korlátozásai

A Hivatalban tilos olyan szoftvereket, digitális szellemi termékeket telepíteni és használni, melyek felhasználási jogával a Hivatal nem rendelkezik.

A kereskedelmi forgalomban beszerzett szoftverek licenceit nyilván kell tartani, és kizárólag a licencfeltételekben meghatározott terjedelemben és feltételekkel szabad a terméket használni.

A szerzői joggal védett állományok megosztását a jegyző engedélyezi, ennek során vizsgálja, hogy a megosztást nem használják-e fel a szerzői joggal védett munka jogosulatlan megosztására, megjelenítésére, végrehajtására vagy reprodukálására.

4.3.5 A felhasználó által telepített szoftverek

A Hivatalban nem engedélyezett a felhasználók számára a szoftverek telepítése.

Szoftver telepítését a jegyző utasítására, illetve engedélye alapján a rendszergazda, vagy más, a jegyző által kijelölt munkatárs végzi el.

4.4 Karbantartás

4.4.1 Rendszer karbantartási eljárásrend

Az információs rendszereket, aktív rendszerelemeket legalább félévente ellenőrizni és szükség szerint karbantartani szükséges. A karbantartás diagnosztikai programok futtatásával, szoftverkomponensek frissítésével, indokolt esetben az operációs rendszer és más komponensek újratelepítésével, a konfigurációs beállítások ellenőrzésével és a szükséges módosítások elvégzésével kell végrehajtani.

A rendszerkarbantartás rendjét az erre vonatkozó szolgáltatási szerződésnek kell tartalmazni.

A Hivatal szokásos működése során nincs adathordozó szállításával összefüggő feladat.

Rendkívüli esetben, ha személyes adatokat tartalmazó adathordozó szállítására lenne szükség, az eseti részletszabályokat a jegyző határozza meg. Ennek során dokumentálni kell a szállítás célját és körülményeit, az adathordozón tárolt adatbázis megnevezését, terjedelmét, a szükséges kriptográfiai eljárást, ki kell jelölni a szállításért felelős személyt. A feladat végrehajtásába be kell vonni az IBF-t.

4.5.5 Kriptográfiai védelem

Kriptográfiai védelmet a Hivatal saját hatáskörében nem alkalmaz.

Jogszabályban előírt, kriptográfiai védelemmel összefüggő hivatali feladatok végrehajtása során maradéktalanul be kell tartani a kijelölt központi szolgáltató által előírt eljárásokat és szabályokat.

4.5.6 Adathordozók törlése

A Hivatal kijelölt munkatársai vagy szerződött műszaki partnerei támogatásával gondoskodik arról, hogy helyreállíthatatlanságot biztosító törlési technikákkal és eljárásokkal törölje az elektronikus információs rendszer adathordozóit a leselejtezés, a használatból történő kivonás vagy újrafelhasználásra való kibocsátás előtt.

A törlési eljárások megválasztása során figyelembe kell venni, hogy az adott adathordozón milyen adatok tárolása történt.

4.5.7 Adathordozók használata

A Hivatalban kizárólag a jegyző által engedélyezett, a Hivatal által beszerzett alábbi adathordozókat szabad használni:

- USB kulcs,
- memóriakártya,
- külső HDD.

Adathordozókat csak a jegyző által engedélyezett célra, pl. mentések készítésére és általános célú irodai alkalmazásokkal készült állományok átmeneti tárolására szabad használni.

A Hivatal adathordozón tesz eleget adatszolgáltatási kötelezettségének, ha ezt jogszabály előírja.

Tilos magán, illetve idegen tulajdonban lévő bármilyen adathordozó és adathordozóként használható eszköz (pl. mobil eszköz) csatlakoztatása a Hivatal informatikai eszközeihez, kivéve, ha ez szerződésben vállalt kötelezettség teljesítésének a részét képezi (pl. rendszergazda, karbantartó, IBF feladatok ellátása során).

4.5.8 Ismeretlen tulajdonos

Tilos bármilyen adathordozó és adathordozóként használható eszköz csatlakoztatása a Hivatal informatikai eszközeihez, ha tulajdonos nem azonosítható.

4.6 Azonosítás és hitelesítés

4.6.1 Azonosítási és hitelesítési eljárásrend

Az ASP Központtól kapott szoftveres tanúsítványt és annak jelszavát tilos átadni az ASP Központ által nem feljogosított személynek.

4.7.2 Felhasználói fiókok kezelése

A Hivatalban – a jogszabály alapján kijelölt központi szolgáltatóknál létrehozott felhasználói fiókokon kívül – az alábbi fióktípusok vannak rendszeresítve:

- a munkakör ellátásához biztosított számítógépen normál (nem rendszergazda) fiók,
- a Hivatal (önkormányzat) internetes tartományába bejegyzett e-mail fiók,
- a hivatali számítógépekhez és más aktív eszközök adminisztrációjához szükséges rendszergazda fiók.

A fiókokok kezelését a jegyző, illetve kijelölt munkatársa szolgáltatói támogatással végzi.

A helyi felhasználói fiókok csoport, illetve szerepköri alapon nincsenek elkülönítve.

A felhasználói fiókok létrehozására, módosítására, tiltására, törlésére a munkáltatói intézkedésekhez kapcsolódóan a jegyző ad utasítást.

A felhasználói fiókok rendeltetésszerű használatát a jegyző a szolgáltatók bevonásával is ellenőrizheti.

4.7.3 A felelősségek szétválasztása

A Hivatal minden felhasználója felelős a felhasználói fiókja jelen szabályzatban meghatározott követelményeknek megfelelő használatáért.

A rendszergazda feladatokkal megbízott személy köteles a felhasználói fiókok használatával kapcsolatosan visszaélésre utaló naplóbejegyzések, rendszeresemények észlelése esetén a jegyzőnek a tapasztaltakról soron kívül jelentést tenni.

4.7.4 Legkisebb jogosultság elve

A Hivatal az elektronikus információs rendszerhez történő hozzáférés engedélyezése során a legkisebb jogosultság elvét alkalmazza, azaz a felhasználók - vagy a felhasználók tevékenysége - számára csak a számukra kijelölt munkaköri feladatok végrehajtásához feltétlenül szükséges jogosultságokat engedélyezi.

4.7.5 Jogosult hozzáférés a biztonsági funkciókhoz

A Hivatal a jegyző által kijelölt munkatársaknak és szolgáltatóknak hozzáférési jogosultságot biztosít azon rendszerelemekhez és biztonsági funkciókhoz, melyek feladataik ellátásához szükségesek.

4.7.6 Nem privilegizált hozzáférés a biztonsági funkciókhoz

A Hivatal meghatározott biztonsági funkciókhoz vagy biztonságkritikus információkhoz hozzáférési jogosultsággal rendelkező felhasználói a nem biztonsági funkciók használatához nem használhatják a különleges jogosultsághoz kötött - úgynevezett privilegizált - fiókjukat vagy szerepkörüket.

Ennek biztosítása érdekében azon felhasználók részére, akik meghatározott biztonsági funkciókhoz privilegizált fiókkal rendelkeznek, létre kell hozni a munkakörük, feladataik ellátása során egyébként használandó, nem privilegizált fiókot.

Az önkormányzati ASP rendszerhez használt számítógépeket nem szabad vezeték nélküli hálózathoz csatlakoztatni. Ez alól a jegyző engedélyével olyan esetekben szabad csak átmenetileg kivételt tenni, amikor a vezetékes kapcsolatra technikai lehetőség nincs, és a munkaköri feladatok ellátását más módon nem lehet biztosítani.

A vezeték nélküli hálózathoz történő hozzáférést úgy kell korlátozni a hálózati eszközök megfelelő konfigurálásával, hogy illetéktelen személy a hálózaton üzemelő hivatali számítógépekhez ne férhessen hozzá.

Külső személyeknek, illetve magáncélú eszközöknek a Hivatalban vezeték nélküli kapcsolatot biztosító hálózati eszközökhöz csak úgy szabad hozzáférést engedélyezni, ha a hálózat külső személyek által látható szegmense a hivatali számítógépek által használt szegmenstől biztonságosan el van választva.

4.7.12 Mobil eszközök hozzáférés ellenőrzése

A Hivatal hálózatához – a Hivatal (önkormányzat) tulajdonában lévő laptop számítógépek kivételével - mobil eszközökkel nem szabad csatlakozni, ennek lehetőségét a hálózati eszközök megfelelő konfigurálásával ki kell zárni.

4.7.13 Titkosítás

A Hivatalban eszköztitkosítást biztosító eljárások nincsenek rendszeresítve, ezért a Hivatal mobil eszközein védett információt nem szabad tárolni.

4.7.14 Külső elektronikus információs rendszerek használata

A Hivatalban kizárólag a jogszabályban meghatározott és központi szolgáltatók által üzemeltett külső információs rendszerek használata engedélyezett.

Nem minősül külső információs rendszer használatnak a munkaköri feladatok ellátása érdekében igénybe vett, azonosítást nem igénylő, nyilvános, böngésző alapú információs szolgáltatások (keresők, portálok) használata.

4.7.15 Korlátozott használat

A jogszabályban meghatározott és központi szolgáltatók által üzemeltett külső információs rendszerek használata során maradéktalanul be kell tartani a szolgáltató által előírt és megkövetelt biztonsági szabályokat, korlátozásokat.

A külső elektronikus információs rendszerek eléréséhez nem szabad olyan hálózati kapcsolatot, eszközt felhasználni, melyet az üzemeltető szervezet nem hagyott jóvá, vagy amelyet megállapodás, szolgáltatási szerződés nem rögzített.

4.7.16 Hordozható adattároló eszközök

A jogszabályban meghatározott és központi szolgáltatók által üzemeltett külső információs rendszerek használata során nem szabad a munkaállomáshoz hordozható tároló eszközt csatlakoztatni, a rendszerből adatokat kimásolni, vagy oda betölteni. Ez alól csak a központi szolgáltató által jóváhagyott, kifejezetten hordozható adattároló használatát igénylő műveletek lehetnek kivételek (pl. adatmigrálás).

Defender), ott más vírusvédelmi programot nem kötelező alkalmazni. Az operációs rendszer védelmi funkcióit ebben az esetben teljes körűen engedélyezni kell.

A védelmi funkciókat úgy kell konfigurálni, hogy:

- rendszeres ellenőrzéseket hajtson végre az elektronikus információs rendszeren, és hajtsa végre a külső forrásokból származó fájlok valós idejű ellenőrzését amikor a fájlokat letöltik, megnyitják vagy elindítják,
- kártékony kód észlelése esetén blokkolja vagy helyezze karanténba azt, és erről értesítse a felhasználót, aki köteles ezt biztonsági incidensként kezelni és jelenteni.

A téves riasztásokról, ennek várható megismétlődéséről és a szükséges teendőkről a rendszergazda és az IBF szükség szerint tájékoztatja a felhasználókat.

4.8.4 Automatikus frissítés

A kártékony kódok elleni védelmi szoftvereket úgy kell konfigurálni, hogy az elektronikus információs rendszer automatikusan frissítse azokat.

4.8.5 Az elektronikus információs rendszer felügyelete

Az elektronikus információs rendszer felügyeletében a biztonságért felelős minden szereplőnek meghatározott felelőssége és feladata van:

- a felhasználók kötelesek minden olyan jelenséget, szokatlan rendszerviselkedést jelenteni a jegyzőnek, ami a rendszer jogosulatlan használatára, a kezelt adatok sértetlenségének, bizalmasságának sérülésére utal;
- a jegyző intézkedik minden észlelt rendellenesség dokumentálásáról, az érintett rendszertől függően a jelzés kivizsgálásának kezdeményezéséről az ASP Központ, a rendszergazda és az IBF felé;
- a rendszergazda a szerződésben meghatározott módon rendszeresen ellenőrzi az elektronikus információs rendszer naplózásait, kivizsgálja a felhasználók jelzéseit, elvégzi a felügyeleti eszközök konfigurálását;
- az IBF legalább évente ellenőrzi a felügyeleti eszközök beállításait, szükség esetén szakmai támogatást nyújt a bejelentett rendellenességek kivizsgálásához.

4.8.6 Biztonsági riasztások és tájékoztatások

A Nemzeti Kibervédelmi Intézettől (NKI) érkező hálózatbiztonsági eseményekről és sérülékenységekről közzétett figyelmeztetéseket az IBF értékeli, meghatározza az ezzel összefüggésben javasolt vezetői intézkedéseket, felhasználói magatartási szabályokat, rendszergazda feladatokat, és erről az érintetteket haladéktalanul tájékoztatja.

Az NKI által az internetes szolgáltatásokkal kapcsolatban elvégzett sérülékenységvizsgálatok eredményeit az IBF haladéktalanul megküldi a jegyzőnek, aki továbbítja az érintett szerződéses szolgáltatóknak.

A jegyző és az IBF kialakítja és működteti a jogszabályban meghatározott esemény bejelentési kötelezettség rendszerét, kapcsolatot tart a jogszabályban meghatározott szervekkel.

4.8.7 Bemeneti információ ellenőrzés

5 Záró rendelkezések

1. Jelen Szabályzat 2023. július 1. napján lép hatályba.

2. Jelen Szabályzat hatálybalépésével a Hivatal által alkalmazott Informatikai Biztonsági Szabályzat hatályát veszti.

Nyőgér, 2023. június 30.

jegyző

NYŐGÉRI KÖZÖS ÖNKORMÁNYZATI HIVATAL * 1 *

6.2 Az elektronikus információs rendszerek biztonságáért felelős személy adatai

Neve: Balatoni Péter (Személyes adatait a megbízási okmány tartalmazza.)

Címe: 8900 Zalaegerszeg, Béke ligeti utca 1. 219.

Telefon: +36 30 309 7787

e-mail: ibf@okosonkormanyzat.hu

Web: https://portal.okosonkormanyzat.hu

6.3 A Közös Önkormányzati Hivatal informatikai rendszereinek nyilvántartása

1. Hivatali informatikai rendszer
   - 1.1. alapfeladatai: a hivatali irodai -ügyviteli munka támogatása
   - 1.2. szolgáltatásai:
     - 1.2.1. hálózati fájlmegosztás
     - 1.2.2. internetelérés, tartalom megjelenítés
     - 1.2.3. szövegszerkesztés
     - 1.2.4. táblázatkezelés
     - 1.2.5. elektronikus levelezés
     - 1.2.6. prezentáció készítés
     - 1.2.7. nyomtatás
     - 1.2.8. képfeldolgozás
   - 1.3. Licencszámok: a gazdálkodási rendszerben nyilvántartva
   - 1.4. A rendszer felügyeletét a jegyző látja el.
   - 1.5. Szállító és karbantartó szervezetek: a hatályos vállalkozási (szolgáltatási) szerződések szerint.

7. Az ügyfélfogadás során ügyelni kell arra, hogy az ügyfél a számítógép képernyőjét ne láthassa, a nyomtatóban az adott ügyfélnek szánt iraton kívül más dokumentum ne készüljön, illetve a nyomtatóban ne maradjon.

8. A számítógépen minden alkalmazásból ki kell jelentkezni és az alkalmazásokat be kell zárni a munkaidő végén vagy hosszabb munkaközi szünet esetén. Karbantartást megelőzően a számítógépet le kell állítani, illetve újra kell indítani, a karbantartó a számítógépet csak a saját azonosítójával használhatja.

9. A Felhasználó köteles a számítástechnikai eszközökkel végzett munkája során a tűz— és munkavédelmi szabályokat maradéktalanul betartani. Ügyelni kell az elektromos berendezések, irodai elosztók, csatlakozók, hosszabbítók épségére, a meghibásodott, sérült eszközöket tovább használni tilos.

10. Minden felhasználó köteles az informatikai biztonsági oktatáson részt venni, az ott megismert ismereteket mindennapi munkájában hasznosítani.

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

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

észlelés: a biztonsági esemény bekövetkezésének felismerése;

felhasználó: egy adott elektronikus információs rendszert igénybe vevők köre;

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

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

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

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

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

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

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

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

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

központi szolgáltató: a jogszabály által kijelölt központosított informatikai és elektronikus hírközlési szolgáltató;

kritikus adat: a személyes adat, vagy valamely jogszabállyal védett adat;

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

6.6 Nyilatkozat a szabályzat megismeréséről

A jelen szabályzatban foglaltakat megismertem, tudomásul veszem, hogy az abban foglaltakat a munkavégzésem során köteles vagyok betartani.

Név	Beosztás	Kelt	Aláírás
TAKÁCS FERENCNÉ	IGAZGATÁSI ÜGYINTÉZŐ	2023.06.30.	Takács Ferencné
SINKÁNÉ KOSZTOLÁNYI BEÁTA	ÜGYKEZELŐ	2023.06.30.	Sinkáné Kosztolányi Beáta
BÁNDOLINÉ HÁTÉ JUDIT MÁRIA ANITA	PÉNZÜGYI ÜGYINTÉZŐ	2023.06.30.	Bándolinéné
SIMONNÉ GREFFER	PÉNZÜGYI ÜGYINTÉZŐ	2023.06.30.	Simonné
PREICZER ANITA	HIVATALSEGÉD	2023.06.30	Preiczer Anita
TAKÁCSNÉ NAGY GABRIELLA	IGAZGATÁSI ÜGYINTÉZŐ	2023.06.30.	Takácsné Nagy Gabriella
VAJDA KRISZTINA	PÉNZÜGYI ÜI.	2023.06.30	Vajda
KOVÁCSNÉ KLOKK DIANKA	PÉNZÜGYI-ADÓÜGYI ÜGYINTÉZŐ	2023.06.30	Kovácsné Klokk Dianka
KOMÁROMI LAURA	PÉNZÜGYI-ADÓÜGYI ÜGYINTÉZŐ	2023.06.30.	Komáromi Laura
LENGYEL ÁRPÁD GÁBORNÉ	IGAZGATÁSI ÜGYINTÉZŐ	2023.06.30	Lengyel Árpádné
PINTÉR KATALIN ILONA	PÜI és ADÓÜ ÜGYINTÉZŐ	2023.06.30	Pintér
TÁMÁS SÁNDORNÉ	IG. SEGÉD	2023.06.30.	Tám
PALLÓSI CSABÁNÉ	ALJEGYZŐ	2023.06.30.	Pallósi
STELCZERNÉ KÁLMÁN ANIKÓ	IGAZGATÁSI ÜGYINTÉZŐ	2023.06.30	Stelczerné Kálmán Anikó
KOVÁCS ANNAMÁRIA	PÉNZÜGYI-ADÓÜGYI ÜI.	2023.06.30	Kovács
KÁLMÁN VILMOSNÉ	HIVATALSEGÉD	2023.06.30.	Kálmán Vilmosné

A jelen szabályzatban foglaltakat megismertem, tudomásul veszem, hogy az abban foglaltakat a munkavégzésem során köteles vagyok betartani.

Név	Beosztás	Kelt	Aláírás