A 37/2015.(III.19.) határozat
melléklete

GKI digital
Kutató és Tanácsadó Kft.

Informatikai szabályzatok felülvizsgálata a Sajószentpéteri Polgármesteri Hivatal számára

2015. március

GKI digital
Kutató és Tanácsadó Kft.

A GKI csoport tagja

H-1092 Budapest Ráday utca 42-44. III. emelet

telefon: +36 1 318 1284 / 128
fax: +36 1 318 4023

Kapcsolat:

Madar Norbert | üzletágvezető
madar@gkidigital.hu
+36 30 541 0905

Timár Szabolcs | ügyvezető
timar@gkidigital.hu
+36 70 331 5843

1 Bevezetés

1.1 Előzmények

A 2013. évi L. törvény részletesen szabályozza az állami és önkormányzati szervek elektronikus információbiztonságát. A törvény részletes leírást tartalmaz az önkormányzatok számára kötelezően megvalósítandó tevékenységekről, szabályzatokról, valamint azok kötelező felülvizsgálatáról.

Az informatikai rendszerek folyamatos változásából kifolyólag az informatikai szabályzatokkal kapcsolatosan általános elvárás, hogy azokat évente egyszer felülvizsgálják, mind a vonatkozó törvényi szabályozásnak való megfelelés, mind annak a valóban használt megoldásokhoz való aktualitása miatt.

A fenti feladat elvégzése céljából a Sajószentpéteri Polgármesteri Hivatal a GKI Digital Kft.-t bízta meg a Hivatal informatikai szabályzatainak éves felülvizsgálatára.

A vizsgálat során az elvégzendő feladatok az alábbiak voltak:

- A Hivatal jelenlegi informatikai szabályzatainak felülvizsgálata, a törvényi megfeleléshez szükséges javítások elvégzése.
- A törvény hatályos változata értelmében feladatlista készítése, mely biztosítja a Hivatal számára a törvényi megfelelést.

1.2 A felülvizsgálat szempontjai

A hivatkozott törvényi előírásnak megfelelően az informatikai szabályzatok vizsgálata az alábbi területekre terjedt ki:

- a biztonsági besorolásnak való megfelelés;
- szabályozott területek köre;
- felelősségi körök meghatározása;
- szükséges informatikai jellegű stratégiák megléte.

Az informatikai szabályzatok felülvizsgálata során kizárólag a fenti szempontok vonatkozásában vizsgáltuk a Hivatal írott szabályzatait, az abban foglalt eljárásrendeknek – pl. megfelelő dokumentáció tényleges vezetése – gyakorlati alkalmazásának ellenőrzése nem képezte jelen vizsgálat tárgyát.

2 Elvárások az informatikai szabályzattal szemben

A polgármesteri hivatalok esetében az informatikai szabályzatokkal szembeni részletes elvárást a 2013. évi L. törvény alapján elkészített informatikai biztonsági besorolás szintje határozza meg. Éppen ezért a következőkben összefoglaljuk, hogy milyen biztonsági besorolása van a Sajószentpéteri Polgármesteri Hivatalnak és ez milyen elvárásokat támaszt az informatikai szabályzatokkal szemben.

2.1 A Hivatal informatikai biztonsági besorolása

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény 7. § (1) bekezdése kimondja, hogy az elektronikus információs rendszereket biztonsági osztályba kell sorolni. A hivatal jelenleg 14 olyan informatikai rendszert használ, melyek vonatkozásában az értékelést el kellett végezni. A hivatal elektronikus információs rendszerei az alábbi biztonsági osztályokba tartoznak.

Rendszer megnevezése	Rendszer biztonsági osztálya
EPER	3
KGR	2
E-kata	1
Bérleti díj	2
Lakbér	2
Wonkadó	3
KIR3	2
WINSZOC	3
Telephely engedély	2
Szabálysértés	2
Működési engedély	1
Szálláshely	1
Complex jogtár	1
ÉTDR	2

A hivatalra vonatkozóan a 2013. évi L. törvény és a vonatkozó végrehajtási rendeleteknek megfelelően az elvárt biztonsági szint: 3.

2.2 Elvárások az informatikai biztonsági besorolás alapján

Az informatikai szabályzatokkal szemben alapvető elvárás a különböző területekre vonatkozóan:

- megfelelő eljárásrendek leírása;
- felelősök, jogkörök meghatározása;
- szabályozott területek pontos meghatározása;
- dokumentálás módjának meghatározása.

Az informatikai szabályzatoknak a megfelelő biztonsági szint elérése szempontjából a hivatkozott törvény szabályozása értelmében három fő területen kell megfelelnie, illetve területenként elérni a szükséges szintet, tartalmat:

- adminisztratív elvárások,
- fizikai védelem szabályozása,
- logikai védelem szabályozása.

Az informatikai szabályzat felülvizsgálata során elsősorban a fentieknek való megfelelést vizsgáltuk. emellett természetesen szem előtt kell tartani, hogy az informatikai rendszerek, hálózat felépítésének megváltozása során igényel-e a szabályzat módosítást, pontosítást.

3 Az informatikai szabályzat felülvizsgálata

A Hivatal által használt informatikai rendszerek biztonsági besorolását követően az elvárt biztonsági szintnek megfelelő szabályozáshoz szükséges kiegészítések a 2014.09.15-én elfogadott informatikai szabályzatban kerületek érvényesítésre.

A szabályzat által előírt rendszer-felülvizsgálat értelmében, 2015 márciusában a GKI Digital Kft. elvégezte az informatikai szabályzatok felülvizsgálatát annak ellenőrzése céljából, hogy az abban foglaltak ténylegesen igazodjanak a Hivatalnál található informatikai rendszerek működéséhez. A szabályzatok felülvizsgálata során a Hivatal részéről az informatikai biztonsági felelős támogatta munkánkat, rendelkezésünkre bocsátotta a szükséges dokumentumokat.

A felülvizsgálat eredményeképp összességében megállapítható, hogy **a Hivatal informatikai szabályzatai megfelelnek az elvárásoknak**, jelen formájában azok nem igényelnek kiegészítéseket.

A következőkben részletesen bemutatjuk, hogy a szabályzatok ellenőrzése során milyen tartalmi szempontok meglétét, teljesülését ellenőriztük.

3.1 Adminisztratív védelmi intézkedések

Szervezeti szintű alapfeladatok

A Hivatal rendelkezik a szükséges szabályzatokkal és informatikai biztonsági stratégiával. A szabályzatok és stratégiák tartalmazzák az elvárt területeknek, a biztonsági besorolásnak megfelelő részletezettségű szabályozását. Az informatikai stratégia részletesen foglalkozik a felmerülő fejlesztési feladatokkal, azok megvalósíthatóságával, illetve kitér az informatikai biztonságot érintő területekre is.

Kockázatelemzés

Az informatikai szabályzat külön fejezetben foglalkozik a kockázatelemzéssel, a sérülékenység ellenőrzésével és a frissítések szabályozásával. A Hivatal informatikai rendszerei rendelkeznek az előírt informatikai biztonsági besorolással.

Tervezés

Az informatikai szabályzat részletesen foglalkozik a rendszerek felhasználóihoz kötődő folyamatok biztonsági szempontból való szabályozásával. Rendelkezik a jogosultságkezelés szabályozásáról és elvárt viselkedési formákat fogalmaz meg az internetes tevékenységek kapcsán. A szabályzat külön fejezetben foglalkozik az informatikai rendszerek biztonságának szabályozásával és a megfelelő működési környezet leírásával.

Biztonsági elemzés

A szabályzat részletesen foglalkozik az informatikai rendszerek biztonsági ellenőrzésével, meghatározza az ellenőrzési folyamatokat, felelősöket és jogköröket.

Emberi tényezőket figyelembe vevő – személy – biztonság

Az informatikai szabályzat részletesen foglalkozik a humán erőforráshoz kapcsolódó védelmi, biztonsági kérdések szabályozásával. Kitér az új, illetve a kilépő dolgozók kapcsán felmerülő szabályokra, valamint az érintett szervezettel szerződéses jogviszonyban álló (külső) szervezetre vonatkozó kérdésekre. Szabályozza a felhasználók jogköreit, azok nyilvántartási igényét.

Tudatosság és képzés

Az informatikai szabályzat rendelkezik a hivatali dolgozók informatika-biztonsági oktatásáról, és szabályozza az oktatásért felelős személyt.

3.2 Fizikai védelmi intézkedések

A Hivatal informatikai szabályzata részletesen foglalkozik az informatikai rendszerek, – köztük a szerverek tárolását biztosító terem – fizikai védelmével. A szabályzat előírja a szükséges fizikai intézkedéseket és a felülvizsgálati gyakoriságokat. Rendelkezik a vagyonvédelmi, tűzvédelmi előírásokkal és részletesen szabályozza a fizikai és környezeti biztonság területeit.

3.3 Logikai védelmi intézkedések

A törvényi szabályozásban meghatározott. a logikai védelmi intézkedések köré épülő szabályozások tekintetében a 3-as biztonsági besorolású informatikai rendszerrel rendelkező Hivatalok számára az alábbi területekre vonatkozóan kell megfelelő szabályozással és eljárásrendekkel rendelkeznie:

- Konfigurációkezelés
- Üzletmenet-(ügymenet-) folytonosság tervezése
- Karbantartás
- Adathordozók védelme
- Azonosítás és hitelesítés
- Hozzáférés ellenőrzése
- Rendszer- és információsértetlenség
- Naplózás és elszámoltathatóság
- Rendszer- és kommunikációvédelem
- Reagálás a biztonsági eseményekre

A jelenleg hatályos informatikai szabályzat a fenti területek mindegyikével külön fejezetben foglalkozik. Részletesen szabályozásra kerül a területek működési környezete, annak felelőse, az alkalmazandó eljárásrendek, valamint a felülvizsgálati időszakok. A szabályozás részletezettsége és kiterjedtsége megfelel a hivatkozott törvény által, a 3-as biztonsági besorolású hivatalokkal szemben támasztott követelményeknek.

4 Melléklet

4.1 A Hivatal informatikai hálózatának felépítése