Enyingi Polgármesteri Hivatal Jegyzője
01/4615-2/ 2015.

ENYINGI POLGÁRMESTERI HIVATAL

Informatikai Biztonsági Stratégia

.....

dr. Kóródi-Juhász Zsolt
jegyző

Enying, 2015. február

Tartalomjegyzék

I. BEVEZETŐ

Az Enyingi Polgármesteri Hivatal (továbbiakban: a Hivatal) **az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény** (továbbiakban: Ibtv.), valamint annak végrehajtási rendeleteiben **foglalt elektronikus információbiztonsági feladatok elvégzésre irányuló felkészülést, illetve azok végrehajtását megkezdte.**

A felkészülés keretében a Hivatal elkészíttette az **Informatikai Biztonságpolitikáját** továbbiakban: IBP), mely tartalmazza a vezetőség elkötelezettségét és támogatását információbiztonság megteremtése, fenntartása és fejlesztése iránt.

A Hivatal elvégezte továbbá az elektronikus információs **rendszereinek biztonsági osztályba sorolását** és a Hivatal **biztonsági szintbe sorolását**. Ennek keretében elkészültek a Hivatal jelenlegi biztonsági szintjét, illetve az elektronikus információs rendszereinek jelenlegi biztonsági osztályát ismertető dokumentumokat.

Az Ibtv. 11. §-ának (1) bekezdése (e) pontja és 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 (továbbiakban: technológiai vhr) 3.1.1. fejezetében meghatározottak alapján a Hivatalnak az érvényes követelmények szerint dokumentálnia kell, és a szervezeten belül ki kell hirdetnie az informatikai biztonsági stratégiát, amely meghatározza a biztonságpolitikai célok megvalósításának módszerét, eszközrendszerét, ütemezését.

Jelen dokumentum célja, hogy ismertesse a Hivatal Informatikai Biztonsági Stratégiáját (továbbiakban: IBS).

II. AZ INFORMATIKAI BIZTONSÁGI STRATÉGIA CÉLJA

A Hivatal IBS-ének célja meghatározni mindazon, rövid-, közép-, és hosszútávra vonatkozó információbiztonsági stratégiai célokat és ezek teljesítéséhez szükséges főbb feladatokat, amelyek az Informatikai Biztonságpolitika által elvi szinten megfogalmazott, a Hivatal biztonságára vonatkozó fontos, tartós igényű elvárások, iránymutatások, állásfoglalások és alapelvek gyakorlati megvalósulását, érvényesítését, illetve teljesítését szolgálják.

Az IBS célja továbbá meghatározni a Hivatal elektronikus információs rendszereiben előállított, tárolt, használt és továbbított információk elektronikus információbiztonságához szükséges stratégiai célokat, és megteremtéséhez szükséges információbiztonsági intézkedéseket, azok fejlesztéseinek irányait, ütemezését.

III. IBS HATÁLYA

III.1. Szervezeti-, személyi hatály

Az IBS **szervezeti hatálya** a Hivatal valamennyi olyan szervezeti egységére kiterjed, amely a Hivatal elektronikus információs rendszereit használja, üzemelteti, fejleszti, továbbá ilyen tevékenységeket irányít és ellenőriz.

Az IBS **személyi hatálya** kiterjed a Hivatallal munkavégzésre irányuló bármely jogviszonyban álló természetes és jogi személyre, tehát azokra, akik kapcsolatba kerülnek a Hivatal elektronikus információs rendszereivel (használják, fejlesztik, telepítik, üzemeltetik, javítják

stb.). Külső szerződéses felek tekintetében az IBS-ben foglaltakat érvényesíteni kell a velük kötött szerződésekben és titoktartási nyilatkozatokban.

III.2. Tárgyi hatály

Az IBS **tárgyi hatálya** kiterjed a Hivatal adataival és adatainak kezelésével összefüggésben használt bármilyen adatrögzítésre, tárolásra, feldolgozásra vagy továbbításra képes infokommunikációs eszközre és ezek működési környezetére.

A tárgyi hatály kiterjed továbbá ezen infokommunikációs eszközök működéséhez alkalmazott szoftverekre, illetve az infokommunikációs eszközökkel rögzített, tárolt, feldolgozott vagy továbbított adatokra és információkra.

III.3. Területi hatály

Az IBSZ területi hatálya kiterjed a Hivatal enyingi székhelyére.

III.4. Időbeli hatály

Jelen IBS a **kiadás napján** lép hatályba.

IV. AZ IBS FELÜLVIZSGÁLATA

Az IBS **eseti módosítására** kerül sor, ha a benne szereplő adatok megváltoztak, illetve ha az IBS olyan kisebb mértékű kiegészítésekre szorul, amelyek nem érintik az aktuális biztonsági elvárásokat.

Az IBS **módosítására** van szükség, ha a Hivatal elektronikus információs rendszereinek működésében, egyéb stratégiai céljaiban (humán, pénzügyi, informatikai, stb.), vagy a Hivatal elektronikus információs rendszereinek működését meghatározó jogszabályi környezetben jelentős változások következnek be.

Az IBS-t **legalább évente egy alkalommal** felül kell vizsgálni.

Az IBS eseti módosításának, felülvizsgálatának kezdeményezése és a felülvizsgálat, valamint a módosítás elvégzése az **elektronikus információs rendszerek biztonságáért felelős személy** (továbbiakban: információbiztonsági felelős, rövidítve IBF) feladata. A módosítások engedélyezése és az újabb változat jóváhagyása a **jegyző** hatásköre.

IV.1. Az IBS kezelése

Az IBS belső használatú dokumentum, azt a következő személyek kezelhetik, azonban illetéktelenek részére nem adhatják tovább:

a) jegyző,

b) információbiztonsági felelős.

V. MEGFELELÉS A JOGSZABÁLYOKNAK

A Hivatal célul tűzi ki a teljekörű megfelelést a mindenkori jogszabályi követelményeknek, mind az elektronikus információbiztonság, mind az adatvédelem területén.

Ennek érdekében a Hivatal információbiztonsági céljainak és stratégiájának megvalósítása során

a) az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény,

b) az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény,

c) 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 NFM rendelet,

d) a Nemzeti Elektronikus Információbiztonsági Hatóság és az információbiztonsági felügyelő feladat- és hatásköréről, valamint a Nemzeti Biztonsági Felügyelet szakhatósági eljárásáról szóló 301/2013. (VII. 29.) Korm. rendelet,

e) az elektronikus információbiztonságról szóló törvény hatálya alá tartozó egyes szervezetek hatósági nyilvántartásba vételének, a biztonsági események jelentésének és közzétételének rendjéről szóló 73/2013. (XII. 4.) NFM rendelet,

f) az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról 26/2013. (X. 21.) KIM rendelet,

g) valamint a MSZ ISO/IEC 27001:2006 szabvány és a Közigazgatási Informatikai Bizottság 25. és 28. számú ajánlásait veszi alapul.

VI. A HELYZETÉRTÉKELÉS

A Hivatal informatikai és információbiztonsági eszközeinek és környezetének felmérését az Ibtv. és a technológiai vhr által előírt feladatok megvalósítása érdekében elvégezte.

A Hivatal jelenlegi informatikai és információbiztonsági helyzetének, információs rendszereinek megismerését segítette elő a Hivatal adminisztratív, fizikai és logikai védelmi intézkedéseinek felmérése a technológiai vhr segédleteként kiadott értékelő táblázat, amelynek eredményeként **megállapításra került a Hivatal jelenlegi biztonsági szintje, illetve információs rendszereinek jelenlegi biztonsági osztálya**. Az Ibtv. által elvárt, illetve a jelenlegi biztonsági osztályok és biztonsági szint közötti hiányosságok megszüntetésére **cselekvési tervek** kerültek kidolgozásra.

Az Ibtv.-ben meghatározott információbiztonsági célok, az elvégzett helyzetértékelések, valamint az elérendő biztonsági szintek és osztályok alapján kerül meghatározásra a Hivatal Informatikai Biztonsági Stratégiája.

VI.1. Elektronikus információs rendszerek biztonsági osztályba sorolása

A Hivatal az Ibtv. és a technológiai vhr rendelkezései alapján elvégezte a Hivatal elektronikus információs rendszereinek **biztonsági osztályba sorolását**, megállapította azok **jelenlegi biztonsági osztályát** és elkészítette az elvárt biztonsági osztályok eléréséhez szükséges **cselekvési terveket**.

Az Ibtv. alapján osztályonként 2 év áll a rendelkezésre ahhoz, hogy felkészítse a Hivatal az elektronikus információs rendszereit a technológiai vhr-ben előírt, az irányadó biztonsági osztályokra vonatkozó logikai védelmi intézkedések bevezetésére.

VI.2. A Hivatal biztonsági szintjének megállapítása

Az Ibtv. alapján a Hivatal minimum biztonsági szintje 2-es és mivel a biztonsági osztályba sorolás alapján nincs 2-esnél magasabb biztonsági osztályba sorolt elektronikus információs rendszere, így az Ibtv. alapján a **Hivatal elvárt biztonsági szintje 2-es**.

A Hivatal elvégezte a jelenlegi adminisztratív és fizikai védelmi intézkedéseinek a vizsgálatát és megállapításra került, hogy a Hivatal jelenlegi biztonsági szintje nem éri el az 1-est.

Az Ibtv. alapján az 1-es biztonsági szint elérésére 1 év, a 2-es biztonsági szint elérésére további 2 év áll a rendelkezésre.

VII. INFORMÁCIÓBIZTONSÁGI VÍZIÓ, JÖVŐKÉP

A Hivatal célul tűzi ki, hogy - az Ibtv. által meghatározott határidőket figyelembe véve - felkészíti elektronikus információs rendszereit a technológiai vhr által előírt logikai védelmi intézkedésekre, illetve felkészíti szervezetét az elvárt biztonsági szint követelményeire.

VIII. ÁLTALÁNOS INFORMÁCIÓBIZTONSÁGI STRATÉGIAI CÉLKITŰZÉSEK

A Hivatal általános információbiztonsági stratégiai céljaként a következőket kívánja foganatosítani:

a) A Hivatal információbiztonságának megteremtésére, megőrzésére, fejlesztésére vonatkozó intézkedések mindenkor feleljenek meg a vonatkozó jogszabályoknak és meghatározásukkor figyelembevételre kerüljenek mindazon legjobb gyakorlatok, hatósági ajánlások, technikai-, műszaki fejlesztések által kínált lehetőségek, információk, amelyek a Hivatal információbiztonsági érdekeinek érvényesülését szolgálhatják.

b) A Hivatal információbiztonságának folyamatos fenntartása, megőrzése és növelése érdekében a szükséges források, eszközök és feltételek biztosítottak legyenek, ezen belül a humán és anyagi erőforrások rendelkezésre álljanak.

c) A Hivatal információbiztonságának megteremtésére, megőrzésére, fejlesztésére vonatkozó intézkedések a biztonsági események megelőzésére koncentráljanak, ezek meghatározásakor a megelőzést szolgáló eszközök, alkalmazások, gyakorlatok alkalmazását kell elsődlegesnek tekinteni.

d) A Hivatal által fel nem vállalható kockázatok kezelésére vonatkozó védelmi intézkedések, a biztonsági rendszerek kialakításakor, üzemeltetésekor alkalmazott eljárások, eszközök és végrehajtási módszerek kockázatarányosak, költségtakarékosak és a különböző forrásokból származó reális fenyegetettségekkel arányosak legyenek.

IX. RÉSZLETES STRATÉGIAI CÉLOK

A jelen fejezetben meghatározott rövid, közép és hosszútávú stratégiai célok a *{VI.1. Elektronikus információs rendszerek biztonsági osztályba sorolása}*és a *{VI.2. A Hivatal biztonsági szintjének megállapítása}* fejezetekben megfogalmazott határidőkkel összhangban kerültek meghatározásra.

IX.1. Rövid távú stratégiai célok

A Hivatal rövidtávon (1 éven belül) a következő stratégiai célokat megvalósítását tervezi:

IX.1.1 Információbiztonsági Irányítási Rendszer szabályozóinak, eljárásrendjeinek kialakítása, bevezetése

Az Információbiztonsági Irányítási Rendszernek (továbbiakban IBIR) egyik legfontosabb alappillére a keretrendszer következő szabályozóinak kidolgozása, és azok kihirdetése és bevezetése a szervezeten belül:

a) Informatikai Biztonsági Politika,

b) Informatikai Biztonsági Stratégia,

c) Informatikai Biztonsági Szabályzat.

A szabályozók biztosítják azokat az információbiztonsági kereteket, elveket, irányokat, és folyamatokat, amelyek elengedhetetlenek a Hivatal információinak bizalmassága, sértetlensége és rendelkezésre állásának biztosítása, valamint a biztonsági követelmények maradéktalan teljesülése érdekében.

A Hivatal az IBIR-hez kapcsolódó szabályozások elkészítését megkezdte, a hiányzó szabályozók, és eljárásrendek kidolgozását a lehető legrövidebb időn belül saját belső erőforrásai, illetve külső információbiztonsági szakértő bevonásával kívánja elérni.

IX.1.2 Információbiztonsági felelős támogatása

Az IBIR fenntartása, folyamatos fejlesztése, szabályozóiban, és eljárásrendjeiben meghatározott teendők érvényre juttatása, megvalósítása érdekében ki kell jelölni a Hivatalinformációbiztonsági felelősét (továbbiakban IBF).

A Hivatal vezetésének teljes körű támogatásával elő kell segítenie az IBF által ellátott feladatok maradéktalan elvégzését, valamint jogköre gyakorlását, hogy a Hivatal a jogszabályi előírásoknak - a meghatározott határidőre - megfeleljen.

IX.1.3 Oktatás, képzés és a biztonságtudatosság fokozása

A biztonsági követelmények maradéktalan teljesülése érdekében minden munkavállalónak, oktatásban kell részesülni és rendszeresen informálni kell őket a biztonsági szabályzatok és elvárások változásairól, különös tekintettel azokra melyek az általuk ellátott munkakörben érvényesek.

A tudatossági oktatás kötelezően tartalmazzon olyan részt, melynek során a felhasználókat megismertetik a rájuk vonatkozó szabályokkal és azok elérhetőségével.

A munkavállalót folyamatosan képezni kell a rá vonatkozó szabályokról, melynek tartalmaznia kell a részletes biztonsági követelményeket, jogi felelősséget, kontrollokat, a fegyelmezés folyamatát, valamint azt, hogy az adatfeldolgozó, információs rendszereket, eszközöket hogyan kell helyesen használni.

A Hivatal gondoskodik arról, hogy az információbiztonság kulcsszereplői részt vegyenek az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról szóló 26/2013. (X. 21.) KIM rendeletben meghatározott képzésen, illetve továbbképzésen.

IX.1.4 Külső felek kezelése, megfelelő szerződések kialakítása

A Hivatal szerződéses partnereinek is megfelelő biztonsági kontrollokat kell alkalmazniuk a felhasznált adatok és dokumentumok bizalmasságának és sértetlenségének megőrzése érdekében, valamint ezek szándékos vagy nem szándékos kompromittálódásának elkerülése érdekében.

Az elektronikus információs rendszerrel kapcsolatba kerülő, vagy az információbiztonságra hatást gyakorló külső személyekkel olyan írásbeli megállapodást – szerződés, titoktartási megállapodást – kell kötni, amely vagy tartalmazza, vagy utal minden olyan információbiztonsági követelményre, amely biztosítja a Hivatalnál bevezetett informatikai és információbiztonsági szabályoknak, elvárásoknak való megfelelést.

A Hivatalnak gondoskodnia kell arról, hogy informatikát, információbiztonságot érintő szerződései átvilágításra kerüljenek, és amelyekben az információbiztonsági követelmények nem kerültek megfelelően rögzítésre, ott törekedni kell arra, hogy a lehető legrövidebb időn belül ezek a szempontok valamilyen hivatalos formában rögzítésre kerüljenek, valamint a külső feleket nyilatkoztatni kell arról, hogy a rájuk vonatkozó információbiztonsági előírásokat megismerték, megértették, és hogy annak betartásával végzik munkájukat.

A jövőbeni szerződéskötéseknél gondoskodni kell arról, hogy az információbiztonsági érdekek már a szerződéskötés megkötése előtti fázisban bevonásra kerüljenek a folyamatba, annak érdekében, hogy a szükséges kontrollok beépítésre kerüljenek a szerződésbe.

IX.1.5 Kockázatelemzés, kockázatok kezelése

A kockázatarányos védelem kialakításához rendszeres és tervszerű információbiztonsági kockázatelemzésre és kezelésre van szükség.

Annak érdekében, hogy a kockázatkezelési folyamata a Hivatal számára jól követhető, megismételhető és ellenőrizhető legyen, írásos kockázatkezelési módszertanra van szükség, mely mind a kockázatelemzés, mind a kockázatkezelés területén lefekteti az alapvető végrehajtási módszereket.

A Hivatal elkészítette kockázatelemzési és kezelési eljárásrendjét, mely alapján rendszeresen, évente kockázatelemzést kíván végre hajtani, az elektronikus információs rendszerek és az azokban kezelt adatok sérülékenységeinek minimalizálása érdekében.

IX.1.6 Windows XP operációs rendszerek cseréje

A Hivatal célul tűzi ki, hogy a lehető leghamarabbi időpontban lecseréli valamennyi Windows XP operációs rendszerét olyan operációs rendszerre, melynek támogatása hosszú távon biztosított.

A Microsoft Windows XP operációs rendszerek gyártói támogatása 2014. áprilisában lejárt, ezután a gyártó nem ad ki biztonsági frissítéseket a termékhez, ezért ezen operációs rendszert futtató munkaállomások a biztonsági réseken keresztül sebezhetőkké válnak.

IX.2. Középtávú stratégiai célok

A Hivatal közép távon (2 éven belül) a következő stratégiai célokat megvalósítását tervezi:

IX.2.1 Logikai védelmi intézkedésekhez kapcsolódó eljárásrendek kidolgozása

A Hivatal kidolgozza és bevezeti az elvárt biztonsági osztályokhoz kapcsolódó eljárásrendeket.

IX.2.2 Logikai védelmi intézkedések megvalósítása az elektronikus információs rendszerekben

A Hivatal elektronikus információs rendszereit fel kell készíteni a technológiai vhr által előírt logikai védelmi intézkedések megvalósítására.

IX.2.3 Információbiztonsági események észlelésének és kezelésének bevezetése, hatékony működtetése

A Hivatalnak az IBSZ-ében, vagy más eljárásrendjében részletesen meg kell határoznia az információbiztonsági események, incidensek észlelésének, és kezelésének folyamatát, felelőseit, illetve a folyamathoz tartozó jelentési kötelezettségeket. A szabályozóban meghatározott folyamatot a Hivatalnak be kell vezetni, és eredményessége érdekében maradéktalanul működtetnie is kell.

A Hivatal célja, hogy az információbiztonságért felelősök és közreműködők a lehető leghamarabb értesüljenek a bekövetkezett incidensekről és ezáltal a lehető leggyorsabban tudjanak reagálni és kockázatarányos védelmi intézkedést foganatosítani.

Az informatikai és információbiztonsági események észlelését technológiai oldalról az elektronikus információs rendszerek megfelelő naplózási eljárásainak kidolgozásával, és bevezetésével kívánja a Hivatal elérni. A kialakított naplózási eljárásoknak támogatnia kell a visszamenőleges felderítés lehetőségét.

IX.3. Hosszú távú stratégiai célok

A Hivatal hosszútávon (3 éven belül) a következő stratégiai célokat megvalósítását tervezi.

IX.3.1 A Fizikai védelmi intézkedések továbbfejlesztése

A Hivatal a meglévő fizikai védelmi intézkedéseit továbbfejleszti a fizikai védelmi eljárásrend kidolgozásával.

Ennek érdekében a Hivatal a fizikai biztonságának kialakításakor kiemelt figyelmet fordít az elektronikus információs rendszereinek koncentráltan helyet adó helyiségeinek védelmére, ezért olyan védelmi megoldások bevezetését tűzi ki célul, melyek megfelelő védelmet biztosítanak a természeti károk, illetve az illetéktelen személyek károkozása ellen.

IX.3.2 Az IBIR folyamatos fejlesztése

A Hivatal hosszú távú, folyamatos információbiztonsági célként tűzte ki az IBIR folyamatos fejlesztését.

Az IBIR folyamatos fejlesztését a fenti stratégiai célok, és az elkészített vonatkozó cselekvési tervekben meghatározott feladatok megvalósítása által elért, a törvényben és rendeletben elvárt biztonsági osztály fenntartásával tervezi megvalósítani.

Ezentúl az IBIR folyamatos fejlesztését rendszeres informatikai és információbiztonsági továbbképzésekkel, trendelemzésekkel, külső információbiztonsági szakértő bevonásával kívánja véghezvinni, hogy folyamatosan megvédje az általa kezelt, tárolt adatok, információk bi-

zalmasságát, sértetlenségét, és rendelkezésre állását a korszerűbb technológiai környezetekben, illetve a legújabb, elektronikus információs rendszerek ellen irányuló támadásokkal szemben is.

X. STRATÉGIAI CÉLOK MEGVALÓSÍTÁSA, STRATÉGIAI TERV

A Hivatal által meghatározott rövid-, közép-, és hosszú távú információbiztonsági stratégiai céljainak megvalósítását, a részletes stratégiai tervet a Hivatal által elkészített cselekvési tervekben (kockázatkezelő intézkedések, az elektronikus információs rendszerek biztonsági osztályainakés a Hivatal biztonsági szintjének értékelése során keletkezett cselekvési tervek) meghatározott feladatok, felelősök és határidők alapján kívánja elvégezni, így ezen cselekvési tervek egyben a Hivatal stratégiai terve is.

XI. MELLÉKLET

Stratégiai célok összefoglaló táblázata

Sorszám	Stratégiai cél	Megvalósítás időtartama		
		Rövid távon (1 éven belül)	Közép távon (2 éven belül)	Hosszú távon (3 éven belül)
1.	Információbiztonsági Irányítási Rendszer szabályozóinak, eljárásrendjeinek kialakítása, bevezetése	X		
2.	Információbiztonsági felelős támogatása	X		
3.	Oktatás, képzés és a biztonságtudatosság fokozása	X		
4.	Külső felek kezelése, megfelelő szerződések kialakítása	X		
5.	Kockázatelemzés, kockázatok kezelése	X		
6.	Windows XP operációs rendszerek cseréje	X		
7.	Logikai védelmi intézkedésekhez kapcsolódó eljárásrendek kidolgozása		X	
8.	Logikai védelmi intézkedések megvalósítása az elektronikus információs rendszerekben		X	
9.	Információbiztonsági események észlelésének és kezelésének bevezetése, hatékony működtetése		X	
10.	A Fizikai védelmi intézkedések továbbfejlesztése			X

Sorszám	Stratégiai cél	Megvalósítás időtartama		
		Rövid távon (1 éven belül)	Közép távon (2 éven belül)	Hosszú távon (3 éven belül)
11.	Az IBIR folyamatos fejlesztése			X