ENYINGI POLGÁRMESTERI HIVATAL

CSELEKVÉSI TERV

az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény által a Hivatal elvárt biztonsági szintjének, valamint az elektronikus információs rendszereinek elvárt biztonsági osztályainak elérésre

I. számú felülvizsgálat

Jóváhagyom!

2015. december …….

……

Dr. Kóródi-Juhász Zsolt

jegyző

Enying, 2015.

TARTALOMJEGYZÉK

TÁBLÁZATJEGYZÉK

I. BEVEZETÉS

Jelen dokumentum célja, hogy az Enyingi Polgármesteri Hivatal (továbbiakban: a Hivatal) számára rögzítse azokat az intézkedéseket, amelyek az elektronikus információs rendszerei elvárt biztonsági osztályainak eléréséhez szükségesek.

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (továbbiakban: Ibtv.) 7. §-ának (1) bekezdése alapján a szervezet **elektronikus információs rendszereit** (továbbiakban: informatikai rendszer) a kockázatarányos védelem megvalósítása érdekében **biztonsági osztályba kell sorolni.**

Az Ibtv. 9. §-ának (1) bekezdése alapján a szervezet védelmi felkészültsége alapján **a szervezetet biztonsági szintbe kell sorolni.**

Az Ibtv. 9. §-ának (2) bekezdése alapján a szervezet elektronikus információs rendszer

a) fejlesztését végző,

b) üzemeltetését végző,

c) üzemeltetéséért felelős vagy

d) információbiztonságáért felelős

szervezeti egységeit - jogszabályban meghatározott szempontok szerint - az elektronikus információs rendszerek védelmére való felkészültségük alapján a szervezettől elvárt, eltérő **biztonsági szintekbe** kell sorolni.

Az Ibtv. alapján a szervezetnek meg kell vizsgálnia, hogy a vizsgálat időpontjában melyik biztonsági szint, illetve biztonsági osztály előírásainak felel meg és a hiányosságok pótlására 90 napon belül cselekvési tervet kell készítenie.

A Hivatal elektronikus információbiztonsági felelőse (továbbiakban: IBF) – a Hivatal vezetőivel együttműködve – elvégezte a Hivatal elektronikus információs rendszereinek biztonsági osztályba sorolását, melyet a Hivatal jegyzője jóváhagyott.

Az Ibtv. 2015. július 16-i módosítása, illetve az új technológiai végrehatási rendelet, a 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 hatályba lépésével **indokolttá vált a Hivatal biztonsági szintjének felülvizsgálata és a cselekvési tervek módosítása.**

A jelen dokumentum tartalmazza a Hivatal elvárt, illetve jelenlegi biztonsági szintjének a meghatározását, az elektronikus információs rendszerek adminisztratív, fizikai és logikai védelmi intézkedéseinek a vizsgálatát, valamint a Hivatal elvárt biztonsági szintjének és az elektronikus információs rendszereinek elvárt biztonsági osztályainak eléréséhez szükséges, módosított cselekvési terveket.

I.1. Hivatkozott dokumentumok

A jelen dokumentumban a következő dokumentumok kerültek hivatkozásra:

1. *Enyingi Polgármesteri Hivatal elektronikus információs rendszereinek biztonsági osztályba sorolása*
2. *PROFESSIONAL PE alkalmazás logikai védelmi intézkedéseinek vizsgálata*
3. *ÖNKADÓ alkalmazás logikai védelmi intézkedéseinek vizsgálata*

II. A HIVATAL ELVÁRT BIZTONSÁGI SZINTJÉNEK MEGÁLLAPÍTÁSA

Az Ibtv. 9. §-ának (1) és (2) bekezdései alapján a kockázatokkal arányos, költséghatékony védelem kialakítása érdekében a szervezetet, valamint az elektronikus információs rendszer

- fejlesztését végző,
- üzemeltetését végző,
- üzemeltetéséért felelős vagy
- információbiztonságáért felelős

szervezeti egységeket az elektronikus információs rendszerek védelmére való felkészültségük alapján a szervezettől elvárt, eltérő biztonsági szintekbe kell sorolni jogszabályban meghatározott szempontok szerint.

II.1. A Hivatal biztonsági szintbe sorolása

Az Ibtv. 9. §-ának (4) bekezdése alapján a szervezet vagy szervezeti egységek biztonsági szintjének meghatározását az elektronikus információs rendszer felhasználásának módja határozza meg, jogszabályban meghatározott szempontok szerint.

A technológiai vhr alapján **a Hivatal biztonsági szintje 4-es**, mivel

- szakfeladatait támogató elektronikus információs rendszert használ (3-as szint)
- a következő kritikus adatokat[1] kezel (3-as szint)
    - személyes adatok, adótitok
- elektronikus információs rendszert üzemeltet (4-es szint).

II.2. Szervezeti egységek biztonsági szintbe sorolása

A Hivatal hatályban lévő Szervezeti és Működési Szabályzata alapján a Hivatalban nem működnek az elektronikus információs rendszer

- fejlesztését végző,
- üzemeltetését végző,
- üzemeltetéséért felelős vagy
- információbiztonságáért felelős

szervezeti egységek, ezért azok biztonsági szintbe sorolása nem értelmezhető.

[1] *Ibtv. 1. § (1) bekezdés 32.a pontja szerint kritikus adat: az Infotv. szerinti személyes adat, különleges adat vagy valamely jogszabállyal védett adat;*

III. A HIVATAL ELVÁRT BIZTONSÁGI SZINTJÉNEK ELÉRÉSÉHEZ SZÜKSÉGES INTÉZKEDÉSEK VIZSGÁLATA

A Hivatal elvárt biztonsági szintjének eléréséhez szükséges védelmi intézkedések vizsgálatát – a technológiai vhr 2. számú melléklete alapján - a jelen fejezet tartalmazza:

41/2015. BM R.	Biztonsági szintek követelményei	Megfelelt?
1.1.	**Az 1. biztonsági szint követelményei**	**Igen**
1.1.1.	az érintett szervezet az érintett személyi kör részére biztosítja az 1.1.3. pont szerinti szervezeti, vagy feladathoz rendelt működési terület hatályos információbiztonságot érintő munkautasítását, belső rendelkezését, szabályozását, vagy más erre célra szolgáló dokumentumot (a továbbiakban együtt: szabályzat);	Igen
1.1.2.	az informatikai biztonsági szabályzat része a folyamatos kockázatelemzési eljárás, amely tartalmazza a beépített ellenőrzési pontokat;	Igen
1.1.3.	az informatikai biztonsági szabályzat vonatkozhat egész szervezetre és működési területére, vagy meghatározott vagyonelemre, vagy szervezeti egységre;	Igen
1.1.4.	az informatikai biztonsági szabályzatot a szervezetre érvényes rendelkezések szerint az erre jogosult vezetőnek kell jóváhagynia;	Igen
1.1.5.	az informatikai biztonsági szabályzat tartalmazza az információbiztonság felügyeleti rendszerét, az információbiztonsággal kapcsolatos kötelezettségeket és felelősségeket;	Igen
1.1.6.	az informatikai biztonsági szabályzat be nem tartása jogkövetkezményt von maga után.	Igen
2.1.	**A 2. biztonsági szint követelményei**	**Nem**
2.1.1.	az érintett szervezet biztonsági kontrollfolyamatai eljárásrendben szabályozottak;	Nem
2.1.2.	a 2.1.1. pont szerinti eljárásrend tartalmazza a kontrollfolyamatok végrehajtásának menetét, módját, időpontját, végrehajtóját, tárgyát, eszközét;	Nem
2.1.3.	az egyes folyamatok egyértelműen meghatározzák az információbiztonsági felelősségeket és a biztonságtudatos viselkedést az elektronikus információs rendszerrel kapcsolatba kerülő személyek, valamint az információbiztonságért felelős személyek és szervezeti egységek tekintetében;	Nem
2.1.4.	az egyes folyamatokat szervezeti egységek, vagy személyek felügyelete alá kell rendelni, akik az adott folyamat végrehajtása érdekében közvetlen kapcsolatban állnak a folyamatban érintett más személyekkel, vagy	Nem

41/2015. BM R.	Biztonsági szintek követelményei	Megfelelt?
	szervezeti egységekkel;	
2.1.5.	a folyamatokat és végrehajtásukat úgy kell dokumentálni, hogy abból az elvégzett kontroll tevékenység - ideértve annak egyes jellemzőit, így különösen mélységét, érintett személyi és tárgyi körét - megállapítható legyen.	Nem
3.1.	**A 3. biztonsági szint követelményei**	**Nem**
3.1.1.	az érintett szervezet a biztonsági kontroll folyamataiba bevonja, és feladataikról, a velük szemben támasztott elvárásokról tájékoztatja a folyamatokban résztvevő személyeket;	Nem
3.1.2.	a 3.1.1. pont szerinti folyamatokat az érintett szervezet vagy szervezeti egység tekintetében szabályozottan és ellenőrizhető módon kell bevezetni, az érintett személyek számára oktatás tárgyává tenni;	Nem
3.1.3.	a 3.1.1. pont szerinti folyamatok nem alkalmazandók egyéni, vagy eseti eljárásokra;	Nem
3.1.4.	a 3.1.1. pont szerinti folyamatokat a szervezetre érvényes rendelkezések szerint erre jogosult vezetőnek kell jóváhagynia;	Nem
3.1.5.	a 3.1.1. pont szerinti folyamatok előzetes tesztelésével biztosítani kell a folyamatok előre meghatározott követelmények szerinti működését;	Nem
3.1.6.	a szervezetnek rendelkeznie kell információbiztonsági költség- és haszonelemzési módszertannal.	Nem
4.1.	**A 4. biztonsági szint követelményei**	
4.1.1.	az üzemeltetési, vagy fejlesztési tevékenységbe épített rendszeres, előre meghatározott tesztekkel biztosítani kell az üzemeltetés, vagy fejlesztés információbiztonsági intézkedéseinek hatékonyságát és megfelelőségét;	Nem
4.1.2.	tesztelési eljárásban rögzítetten biztosítani kell minden szabályozási folyamat és kontroll működését az elvárt és előre meghatározott információbiztonsági követelmények szerint;	Nem
4.1.3.	azonnali és eredményes, előre meghatározott biztonsági intézkedéseket kell bevezetni a feltárt, vagy bekövetkezett biztonsági események kezelésére, beleértve az eseménykezelő központok, a beszállítók vagy egyéb megbízható forrás jelzése alapján lehetséges, vagy bekövetkezett biztonsági esemény kezelését is;	Nem

41/2015. BM R.	Biztonsági szintek követelményei	Megfelelt?
4.1.4.	folyamatba épített rendszeres belső értékelés alá kell vonni az egyes információ, rendszer, vagy alkalmazás biztonsága érdekében bevezetett intézkedések megfelelőségét és hatékonyságát, mely belső értékelések részben, vagy egészben történhetnek alvállalkozók, vagy más, erre feljogosított, vagy a szerv felett felügyelet gyakorló szerv bevonásával;	Nem
4.1.5.	a szervezet folyamatba épített belső értékelései nem helyettesíthetőek;	Nem
4.1.6.	a 4.1.3. pont szerinti forrásból származó, potenciális vagy a valódi biztonsági eseményekkel és biztonsággal kapcsolatos információk, vagy riasztások alapján tesztelési eljárást, vagy biztonsági ellenőrzést kell végezni;	Nem
4.1.7.	a tesztelés értékelése alapján megállapított követelményeket, - beleértve a tesztelés típusával és gyakoriságával kapcsolatos követelményeket is - dokumentálni kell, az arra jogosulttal jóvá kell hagyatni és be kell vezetni;	Nem
4.1.8.	az egyedi kontroll eljárások tesztelésének gyakoriságát és mélységét ahhoz kell igazítani, hogy milyen biztonsági kockázattal jár a kontrollok nem megfelelő működése.	Nem

1. táblázat - A Hivatal jelenlegi biztonsági szintjének vizsgálata

III.1. A Hivatal jelenlegi biztonsági szintjének megállapítása

A *{III. A Hivatal elvárt biztonsági szintjének eléréséhez szükséges intézkedések vizsgálata}* fejezetben megállapítottak alapján

a Hivatal jelenlegi biztonsági szintje: 1.

IV. A HIVATAL ELEKTRONIKUS INFORMÁCIÓS RENDSZEREINEK JELENLEGI ADMINISZTRATÍV ÉS FIZIKAI VÉDELMI INTÉZKEDÉSEINEK VIZSGÁLATA

A Hivatal valamennyi elektronikus információs rendszere 2-es biztonsági osztályba került besorolásra, ezért a Hivatalra a 2-es biztonsági osztályra vonatkozó adminisztratív és fizikai védelmi intézkedések az irányadók.

IV.1. Adminisztratív védelmi intézkedések vizsgálata

A 2-es biztonsági osztályhoz előírt intézkedésekhez képest a meglévő adminisztratív védelmi intézkedéseinek hiányosságait a következő táblázat tartalmazza:

Adminisztratív védelmi intézkedések		Megfelelt/Nem felelt meg
Sorszám	**Intézkedés típusa**	
3.1.1.	**Szervezeti szintű alapfeladatok**	**Nem felelt meg**
3.1.1.1.	*Informatikai biztonságpolitika*	*Megfelelt*
3.1.1.2.	*Informatikai biztonsági stratégia*	*Nem felelt meg*
3.1.1.3.	*Informatikai biztonsági szabályzat*	*Nem felelt meg*
3.1.1.4.	*Az elektronikus információs rendszerek biztonságáért felelős személy*	*Megfelelt*
3.1.1.5.	*Pénzügyi erőforrások biztosítása*	*Nem felelt meg*
3.1.1.6.	*Az intézkedési terv és mérföldkövei*	*Nem felelt meg*
3.1.1.7.	*Az elektronikus információs rendszerek nyilvántartása*	*Nem felelt meg*
3.1.1.10.	*Kockázatkezelési stratégia*	*Nem felelt meg*
3.1.1.11.	*Az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárás*	*Nem felelt meg*
3.1.2.	**Kockázatelemzés**	**Nem felelt meg**
3.1.2.1.	*Kockázatelemzési eljárásrend*	*Nem felelt meg*
3.1.2.2.	*Biztonsági osztályba sorolás*	*Nem felelt meg*
3.1.2.3.	*Kockázatelemzés*	*Nem felelt meg*
3.1.3.	**Tervezés**	**Nem felelt meg**
3.1.3.1.	*Biztonságtervezési eljárásrend*	*Nem felelt meg*
3.1.3.2.	*Rendszerbiztonsági terv*	*Nem felelt meg*
3.1.3.3.	*Személyi biztonság*	*Nem felelt meg*
3.1.3.3.2.	*Viselkedési szabályok az interneten*	*Nem felelt meg*
3.1.6.	**Emberi tényezőket figyelembe vevő - személy - biztonság**	**Nem felelt meg**
3.1.6.5.	*Eljárás a jogviszony megszűnésekor*	*Nem felelt meg*
3.1.6.8.	*Fegyelmi intézkedések*	*Nem felelt meg*
3.1.7.	**Tudatosság és képzés**	**Nem felelt meg**
3.1.7.1.	*Képzési eljárásrend*	*Nem felelt meg*
3.1.7.2.	*Biztonság tudatosság képzés*	*Nem felelt meg*

2. táblázat – A Hivatal adminisztratív védelmi intézkedéseinek vizsgálata

IV.1.1. A Hivatal jelenlegi adminisztratív védelmi intézkedései szintjének megállapítása

A *{IV.1.* Adminisztratív védelmi intézkedések vizsgálata*}* fejezet alapján a Hivatal jelenlegi adminisztratív védelmi intézkedései nem érik el az 1-es biztonsági osztály követelményeit.

IV.2. Fizikai védelmi intézkedések vizsgálata

A 2-es biztonsági osztályhoz előírt intézkedésekhez képest a meglévő fizikai védelmi intézkedéseinek hiányosságait a következő táblázat tartalmazza:

Fizikai védelmi intézkedések		Megfelelt/Nem felelt meg
Sorszám	**Intézkedés típusa**	
3.2.1.2.	*Fizikai védelmi eljárásrend*	*Nem felelt meg*
3.2.1.3.	*Fizikai belépési engedélyek*	*Nem felelt meg*
3.2.1.4.	*A fizikai belépés ellenőrzése*	*Nem felelt meg*

3. táblázat – A Hivatal fizikai védelmi intézkedéseinek vizsgálata

IV.2.1. A Hivatal jelenlegi fizikai védelmi intézkedései szintjének megállapítása

A *{IV.2.* Fizikai védelmi intézkedések vizsgálata*}* fejezet alapján a Hivatal jelenlegi fizikai védelmi intézkedései nem érik el az 2-es biztonsági osztály követelményeit.

V. A HIVATAL ELEKTRONIKUS INFORMÁCIÓS RENDSZEREINEK JELENLEGI LOGIKAI VÉDELMI INTÉZKEDÉSEINEK VIZSGÁLATA

Jelen fejezetben a Hivatal elektronikus információs rendszerinek meglévő logikai védelmi intézkedéseinek - technológiai vhr alapján történő - vizsgálati eredményei találhatók.

V.1. PROFESSIONAL PE alkalmazás

Jelen fejezet a ***PROFESSIONAL PE alkalmazás*** elvárt biztonsági osztályát, a jelenlegi logikai védelmi intézkedéseit és a jelenlegi biztonsági osztályának megállapítását tartalmazza.

V.1.1. A PROFESSIONAL PE alkalmazás elvárt biztonsági osztálya

A Hivatal ***PROFESSIONAL PE alkalmazásának*** az *{Enyingi Polgármesteri Hivatal elektronikus információs rendszereinek biztonsági osztályba sorolása}* alapján összességében a 2-es biztonsági osztályt szükséges elérni, mivel

Elvárt biztonsági osztály (PROFESSIONAL PE) =

{(Bizalmasság, 2), (Sértetlenség, 2), (Rendelkezésre állás, 2)}.

V.1.2. A PROFESSIONAL PE jelenlegi védelmi intézkedéseinek vizsgálata és a hiányosságok kimutatása

Az ***PROFESSIONAL PE alkalmazás*** jelenlegi védelmi intézkedéseinek részletes értékelését az *{PROFESSIONAL PE alkalmazás logikai védelmi intézkedéseinek vizsgálata}* dokumentum tartalmazza.

A következő táblázat az értékelés során tapasztalt hiányosságokat tartalmazza:

Logikai védelmi intézkedések		Megfelelt/Nem felelt meg		
Sorszám	**Intézkedés típusa**	**Bizalmasság**	**Sértetlenség**	**Rendelkezésre állás**
3.3.1.	**Konfigurációkezelés**	**Nem felelt meg**	**Nem felelt meg**	**Nem felelt meg**
3.3.1.1.	*Konfigurációkezelési eljárásrend*	*Nem felelt meg*	*Nem felelt meg*	*Nem felelt meg*
3.3.1.2.	*Alapkonfiguráció*	*Nem felelt meg*	*Nem felelt meg*	*Nem felelt meg*
3.3.1.8.	*Elektronikus információs rendszerelem leltár*	*Nem felelt meg*	*Nem felelt meg*	*Nem felelt meg*
3.3.1.10.	*A szoftverhasználat korlátozásai*	*Nem felelt meg*	*Nem felelt meg*	*Nem felelt meg*
3.3.1.11.	*A felhasználó által telepített szoftverek*	*Nem felelt meg*	*Nem felelt meg*	*Nem felelt meg*
3.3.2.	**Üzletmenet- (ügymenet-) folytonosság tervezése**	**Megfelelt**	**Nem felelt meg**	**Nem felelt meg**
3.3.2.1.	*Üzletmenet-folytonosságra vonatkozó eljárásrend*	*Nem kötelező*	*Nem kötelező*	*Nem felelt meg*
3.3.2.2.	*Üzletmenet-folytonossági terv informatikai erőforrás kiesésekre*	*Nem kötelező*	*Nem kötelező*	*Nem felelt meg*
3.3.2.8.	*Az elektronikus információs rendszer mentései*	*Nem kötelező*	*Nem felelt meg*	*Nem felelt meg*
3.3.2.9.	*Az elektronikus információs rendszer helyreállítása és újraindítása*	*Nem kötelező*	*Nem felelt meg*	*Nem felelt meg*
3.3.3.	**Karbantartás**	**Megfelelt**	**Nem felelt meg**	**Nem felelt meg**
3.3.3.1.	*Rendszer karbantartási eljárásrend*	*Nem kötelező*	*Nem felelt meg*	*Nem felelt meg*
3.3.3.2.	*Rendszeres karbantartás*	*Nem kötelező*	*Nem felelt meg*	*Nem felelt meg*
3.3.4.	**Adathordozók védelme**	**Nem felelt meg**	**Nem felelt meg**	**Nem felelt meg**
3.3.4.1.	*Adathordozók védelmére vonatkozó eljárásrend*	*Nem felelt meg*	*Nem felelt meg*	*Nem felelt meg*
3.3.4.2.	*Hozzáférés az adathordozókhoz*	*Nem felelt meg*	*Nem felelt meg*	*Nem felelt meg*
3.3.4.6.	*Adathordozók törlése*	*Nem felelt meg*	*Nem kötelező*	*Nem kötelező*
3.3.4.7.	*Adathordozók használata*	*Nem felelt meg*	*Nem felelt meg*	*Nem felelt meg*
3.3.5.	**Azonosítás és hitelesítés**	**Nem felelt meg**	**Nem felelt meg**	**Nem felelt meg**
3.3.5.1.	*Azonosítási és hitelesítési eljárásrend*	*Nem felelt meg*	*Nem felelt meg*	*Nem felelt meg*
3.3.5.2.	*Azonosítás és hitelesítés*	*Nem felelt meg*	*Nem felelt meg*	*Nem felelt meg*
3.3.5.4.	*Azonosító kezelés*	*Nem felelt meg*	*Nem felelt meg*	*Nem felelt meg*
3.3.5.5.	*A hitelesítésre szolgáló eszközök kezelése*	*Nem felelt meg*	*Nem felelt meg*	*Nem felelt meg*
3.3.6.	**Hozzáférés ellenőrzése**	**Nem felelt meg**	**Nem felelt meg**	**Nem felelt meg**
3.3.6.1.	*Hozzáférés ellenőrzési eljárásrend*	*Nem felelt meg*	*Nem felelt meg*	*Nem felelt meg*

Logikai védelmi intézkedések		Megfelelt/Nem felelt meg		
Sorszám	**Intézkedés típusa**	**Bizalmasság**	**Sértetlenség**	**Rendelkezésre állás**
3.3.6.2.	*Felhasználói fiókok kezelése*	*Nem felelt meg*	*Nem felelt meg*	*Nem felelt meg*
3.3.6.3.	*Hozzáférés ellenőrzés érvényesítése*	*Nem felelt meg*	*Nem felelt meg*	*Nem felelt meg*
3.3.7.	**Rendszer- és információsértetlenség**	**Nem felelt meg**	**Nem felelt meg**	**Nem felelt meg**
3.3.7.2.	*Rendszer- és információsértetlenségre vonatkozó eljárásrend*	*Nem kötelező*	*Nem felelt meg*	*Nem kötelező*
3.3.7.3.	*Hibajavítás*	*Nem kötelező*	*Nem felelt meg*	*Nem kötelező*
3.3.7.4.	*Kártékony kódok elleni védelem*	*Nem felelt meg*	*Nem felelt meg*	*Nem felelt meg*
3.3.7.5.	*Az elektronikus információs rendszer felügyelete*	*Nem felelt meg*	*Nem felelt meg*	*Nem felelt meg*
3.3.7.12.	*A kimeneti információ kezelése és megőrzése*	*Nem felelt meg*	*Nem felelt meg*	*Nem kötelező*
3.3.8.	**Naplózás és elszámoltathatóság**	**Nem felelt meg**	**Nem felelt meg**	**Nem felelt meg**
3.3.8.1.	*Naplózási eljárásrend*	*Nem felelt meg*	*Nem felelt meg*	*Nem felelt meg*
3.3.8.2.	*Naplózható események*	*Nem felelt meg*	*Nem felelt meg*	*Nem felelt meg*
3.3.8.3.	*Naplóbejegyzések tartalma*	*Nem felelt meg*	*Nem felelt meg*	*Nem felelt meg*
3.3.8.8.	*Időbélyegek*	*Nem felelt meg*	*Nem felelt meg*	*Nem felelt meg*
3.3.8.9.	*A naplóinformációk védelme*	*Nem felelt meg*	*Nem felelt meg*	*Nem felelt meg*
3.3.8.11.	*A naplóbejegyzések megőrzése*	*Nem felelt meg*	*Nem felelt meg*	*Nem felelt meg*
3.3.8.12.	*Naplógenerálás*	*Nem felelt meg*	*Nem felelt meg*	*Nem felelt meg*
3.3.9.	**Rendszer- és kommunikációvédelem**	**Nem felelt meg**	**Nem felelt meg**	**Nem felelt meg**
3.3.9.1.	*Rendszer- és kommunikációvédelmi eljárásrend*	*Nem felelt meg*	*Nem felelt meg*	*Nem felelt meg*
3.3.9.6.	*A határok védelme*	*Nem felelt meg*	*Nem felelt meg*	*Nem felelt meg*

4. táblázat – A PROFESSIONAL PE alkalmazás logikai védelmi intézkedéseinek hiányosságai

V.1.3. A PROFESSIONAL PE alkalmazás jelenlegi biztonsági osztályának megállapítása

A meglévő adminisztratív, fizikai és logikai védelmi intézkedések vizsgálata alapján

- nem teljesülnek az 1-es biztonsági osztályra előírt adminisztratív védelmi intézkedések,
- nem teljesülnek a 2-es biztonsági osztályra előírt logikai védelmi intézkedések, valamint
- nem teljesülnek a 2-es biztonsági osztályra előírt fizikai védelmi intézkedések,

ezért összességében **a PROFESSIONAL PE alkalmazás jelenlegi biztonsági osztálya: 0.**

V.2. ÖNKADÓ alkalmazás

Jelen fejezet az ***ÖNKADÓ alkalmazás*** elvárt biztonsági osztályát, a jelenlegi logikai védelmi intézkedéseit és a jelenlegi biztonsági osztályának megállapítását tartalmazza.

V.2.1. Az ÖNKADÓ alkalmazás elvárt biztonsági osztálya

A Hivatal ***ÖNKADÓ alkalmazásának*** *az {Enyingi Polgármesteri Hivatal elektronikus információs rendszereinek biztonsági osztályba sorolása}* alapján összességében a 2-es biztonsági osztályt szükséges elérni, mivel

Elvárt biztonsági osztály (ÖNKADÓ) =

{(Bizalmasság, 2), (Sértetlenség, 2), (Rendelkezésre állás, 1)}.

V.2.2. AZ ÖNKADÓ alkalmazás jelenlegi logikai védelmi intézkedéseinek vizsgálata és a hiányosságok kimutatása

Az ***ÖNKADÓ alkalmazás*** jelenlegi védelmi intézkedéseinek részletes értékelését az *{ÖNKADÓ alkalmazás logikai védelmi intézkedéseinek vizsgálata}* dokumentum tartalmazza.

A következő táblázat az értékelés során tapasztalt hiányosságokat tartalmazza:

Logikai védelmi intézkedések		Megfelelt/Nem felelt meg		
Sorszám	**Intézkedés típusa**	**Bizalmasság**	**Sértetlenség**	**Rendelkezésre állás**
3.3.1.	**Konfigurációkezelés**	**Nem felelt meg**	**Nem felelt meg**	**Megfelelt**
3.3.1.1.	*Konfigurációkezelési eljárásrend*	*Nem felelt meg*	*Nem felelt meg*	*Nem kötelező*
3.3.1.2.	*Alapkonfiguráció*	*Nem felelt meg*	*Nem felelt meg*	*Nem kötelező*
3.3.1.8.	*Elektronikus információs rendszerelem leltár*	*Nem felelt meg*	*Nem felelt meg*	*Nem kötelező*
3.3.1.10.	*A szoftverhasználat korlátozásai*	*Nem felelt meg*	*Nem felelt meg*	*Nem kötelező*
3.3.1.11.	*A felhasználó által telepített szoftverek*	*Nem felelt meg*	*Nem felelt meg*	*Nem kötelező*
3.3.2.	**Üzletmenet- (ügymenet-) folytonosság tervezése**	**Megfelelt**	**Nem felelt meg**	**Megfelelt**
3.3.2.8.	*Az elektronikus információs rendszer mentései*	*Nem kötelező*	*Nem felelt meg*	*Nem kötelező*
3.3.2.9.	*Az elektronikus információs rendszer helyreállítása és újraindítása*	*Nem kötelező*	*Nem felelt meg*	*Nem kötelező*
3.3.3.	**Karbantartás**	**Megfelelt**	**Nem felelt meg**	**Megfelelt**
3.3.3.1.	*Rendszer karbantartási eljárásrend*	*Nem kötelező*	*Nem felelt meg*	*Nem kötelező*
3.3.3.2.	*Rendszeres karbantartás*	*Nem kötelező*	*Nem felelt meg*	*Nem kötelező*
3.3.4.	**Adathordozók védelme**	**Nem felelt meg**	**Nem felelt meg**	**Megfelelt**
3.3.4.1.	*Adathordozók védelmére vonatkozó eljárásrend*	*Nem felelt meg*	*Nem felelt meg*	*Nem kötelező*
3.3.4.2.	*Hozzáférés az adathordozókhoz*	*Nem felelt meg*	*Nem felelt meg*	*Nem kötelező*
3.3.4.6.	*Adathordozók törlése*	*Nem felelt meg*	*Nem kötelező*	*Nem kötelező*
3.3.4.7.	*Adathordozók használata*	*Nem felelt meg*	*Nem felelt meg*	*Nem kötelező*
3.3.5.	**Azonosítás és hitelesítés**	**Nem felelt meg**	**Nem felelt meg**	**Megfelelt**

Logikai védelmi intézkedések		Megfelelt/Nem felelt meg		
Sorszám	**Intézkedés típusa**	**Bizalmasság**	**Sértetlenség**	**Rendelkezésre állás**
3.3.5.1.	*Azonosítási és hitelesítési eljárás-rend*	*Nem felelt meg*	*Nem felelt meg*	*Nem kötelező*
3.3.5.2.	*Azonosítás és hitelesítés*	*Nem felelt meg*	*Nem felelt meg*	*Nem kötelező*
3.3.5.4.	*Azonosító kezelés*	*Nem felelt meg*	*Nem felelt meg*	*Nem kötelező*
3.3.5.5.	*A hitelesítésre szolgáló eszközök kezelése*	*Nem felelt meg*	*Nem felelt meg*	*Nem kötelező*
3.3.6.	**Hozzáférés ellenőrzése**	**Nem felelt meg**	**Nem felelt meg**	**Megfelelt**
3.3.6.1.	*Hozzáférés ellenőrzési eljárásrend*	*Nem felelt meg*	*Nem felelt meg*	*Nem kötelező*
3.3.6.2.	*Felhasználói fiókok kezelése*	*Nem felelt meg*	*Nem felelt meg*	*Nem kötelező*
3.3.6.3.	*Hozzáférés ellenőrzés érvényesítése*	*Nem felelt meg*	*Nem felelt meg*	*Nem kötelező*
3.3.7.	**Rendszer- és információsértetlenség**	**Nem felelt meg**	**Nem felelt meg**	**Megfelelt**
3.3.7.2.	*Rendszer- és információsértetlenségre vonatkozó eljárásrend*	*Nem kötelező*	*Nem felelt meg*	*Nem kötelező*
3.3.7.3.	*Hibajavítás*	*Nem kötelező*	*Nem felelt meg*	*Nem kötelező*
3.3.7.4.	*Kártékony kódok elleni védelem*	*Nem felelt meg*	*Nem felelt meg*	*Nem kötelező*
3.3.7.5.	*Az elektronikus információs rendszer felügyelete*	*Nem felelt meg*	*Nem felelt meg*	*Nem kötelező*
3.3.7.12.	*A kimeneti információ kezelése és megőrzése*	*Nem felelt meg*	*Nem felelt meg*	*Nem kötelező*
3.3.8.	**Naplózás és elszámoltathatóság**	**Nem felelt meg**	**Nem felelt meg**	**Megfelelt**
3.3.8.1.	*Naplózási eljárásrend*	*Nem felelt meg*	*Nem felelt meg*	*Nem kötelező*
3.3.8.2.	*Naplózható események*	*Nem felelt meg*	*Nem felelt meg*	*Nem kötelező*
3.3.8.3.	*Naplóbejegyzések tartalma*	*Nem felelt meg*	*Nem felelt meg*	*Nem kötelező*
3.3.8.9.	*A naplóinformációk védelme*	*Nem felelt meg*	*Nem felelt meg*	*Nem kötelező*
3.3.8.11.	*A naplóbejegyzések megőrzése*	*Nem felelt meg*	*Nem felelt meg*	*Nem kötelező*
3.3.8.12.	*Naplógenerálás*	*Nem felelt meg*	*Nem felelt meg*	*Nem kötelező*
3.3.9.	**Rendszer- és kommunikációvédelem**	**Nem felelt meg**	**Nem felelt meg**	**Megfelelt**
3.3.9.1.	*Rendszer- és kommunikációvédelmi eljárásrend*	*Nem felelt meg*	*Nem felelt meg*	*Nem kötelező*
3.3.9.6.	*A határok védelme*	*Nem felelt meg*	*Nem felelt meg*	*Nem kötelező*

5. táblázat – Az ÖNKADÓalkalmazás logikai védelmi intézkedéseinek hiányosságai

V.2.3. Az ÖNKADÓ alkalmazás jelenlegi biztonsági osztályának megállapítása

A meglévő adminisztratív, fizikai és logikai védelmi intézkedések vizsgálata alapján

- nem teljesülnek az 1-es biztonsági osztályra előírt adminisztratív védelmi intézkedések,
- nem teljesülnek a 2-es biztonsági osztályra előírt logikai védelmi intézkedések, valamint
- nem teljesülnek a 2-es biztonsági osztályra előírt fizikai védelmi intézkedések,

ezért összességében **az Önkadó alkalmazás jelenlegi biztonsági osztálya: 0.**

VI. CSELEKVÉSI TERVEK

VI.1. A Hivatal elvárt biztonsági szintjének elérésére készített cselekvési terv

Az Ibtv. 10. § (2) bekezdése alapján a szervezetnek a szervezet biztonsági szintjének megállapítása után 90 napon belül cselekvési tervet kell készítenie az elvárt biztonsági szintre előírt intézkedések megvalósítására. Az egyes biztonsági szintek teljesítésére - 2014. július 1-től számítva - szintenként 2-2 év (Ibtv. 10. § (4) bekezdése) áll a rendelkezésre.

41/2015. BM R.	BIZTONSÁGI SZINTEK KÖVETELMÉNYEI	INTÉZKEDÉS	FELELŐS	HATÁRIDŐ
2.1.	**2. biztonsági szint**			
2.1.1.	az érintett szervezet biztonsági kontrollfolyamatai eljárásrendben szabályozottak;	Technológiai vhr-ben előírt eljárásrendek kidolgozása	IBF	2017. december 1.
2.1.2.	a 2.1.1. pont szerinti eljárásrend tartalmazza a kontrollfolyamatok végrehajtásának menetét, módját, időpontját, végrehajtóját, tárgyát, eszközét;	Az IBSZ-ben és a kapcsolódó eljárásrendekben kell előírni az adminisztratív, a fizikai és a logikai védelmi intézkedések végrehajtásának módját.	IBF	2017. december 1.
2.1.3.	az egyes folyamatok egyértelműen meghatározzák az információbiztonsági felelősségeket és a biztonságtudatos viselkedést az elektronikus információs rendszerrel kapcsolatba kerülő személyek, valamint az információbiztonságért felelős személyek és szervezeti egységek tekintetében;	Az IBSZ-en kívül (mely az elektronikus információs rendszerek üzemeltetésében, fejlesztésében, karbantartásában részt vevők, a vezetők, az adatgazdák, a felhasználók és az IBF feladatait, felelősségét tartalmazza) Felhasználói Informatikai Biztonsági Házi-rendet kell készíteni, mely kifejezetten a felhasználók jogait és kötelezettségeit tartalmazza az elektronikus információs rendszerek biztonságával kapcsolatban. A felhasználók részére biztonságtudatosság fokozó tréningeket kell szervezni. A Hivatal valamennyi munkatársa részére havonta-kéthavonta információbiztonsági hírlevelet kell kiküldeni, mely egy-egy - felhasználói szemszögből releváns – témát (pl.: jelszavak, socialengineering, mobil eszközök stb.) dolgoz fel felhasználó számára érthető formában.	IBF	2017. december 1.
2.1.4.	az egyes folyamatokat szervezeti egységek, vagy személyek felügyelete alá kell rendelni, akik az adott folyamat végrehajtása érdekében közvetlen kapcsolatban állnak a folyamatban érintett más személyekkel, vagy szervezeti egységekkel;	Az IBSZ-t úgy kell elkészíteni, hogy az egyértelműen határozza meg az egyes feladatok elvégzéséhez rendelt szerepköröket. A szerepkörökhöz jól beazonosíthatóan személyek kerültek kijelölésre.	IBF	2017. december 1.
2.1.5.	a folyamatokat és végrehajtásukat úgy kell dokumentálni, hogy abból az elvégzett kontroll tevékenység - ideértve annak egyes jellemzőit, így különösen mélységét, érintett személyi és tárgyi körét - megállapítható legyen.	Az IBSZ-ben meghatározott dokumentálások végrehajtása.	Az IBSZ-ben meghatározott szerepkör	2017. december 1.
3.1.	**3. biztonsági szint**			
3.1.1.	az érintett szervezet a biztonsági kontroll folyamataiba bevonja, és feladataikról, a velük szemben támasztott elvárásokról tájékoztatja a folyamatokban résztvevő személyeket;	A Hivatal a biztonsági kontrollfolyamatairól e-learning alapú biztonságtudatosság fokozó tréningen, illetve havi-kéthavi rendszerességgel kiadott hírlevelekben tervezi tájékoztatni az érintetteket. Az érintetteknek az aláírásukkal igazolják, hogy megismerték a rájuk vonatkozó szabályokat.	IBF	2019. december 1.
3.1.2.	a 3.1.1. pont szerinti folyamatokat az érintett szervezet vagy szervezeti egység tekintetében szabályozottan és ellenőrizhető módon kell bevezetni, az érintett személyek számára oktatás tárgyává tenni;	A Hivatal a biztonsági kontrollfolyamatairól e-learning alapú biztonságtudatosság fokozó tréningen, illetve havi-kéthavi rendszerességgel kiadott hírlevelekben tervezi tájékoztatni az érintetteket. Az érintetteknek az aláírásukkal igazolják, hogy megismerték a rájuk vonatkozó szabályokat.	IBF	2019. december 1.
3.1.3.	a 3.1.1. pont szerinti folyamatok nem alkalmazandók egyéni, vagy eseti eljárásokra;	A biztonsági kontrollfolyamatokat egységesen kell alkalmazni.	Valamennyi érintett szerepkör	2019. december 1.
3.1.4.	a 3.1.1. pont szerinti folyamatokat a szervezetre érvényes rendelkezések szerint erre jogosult vezetőnek kell jóváhagynia;	Az információbiztonsági eljárásrend gyűjteményt a jegyzőnek kell jóváhagynia.	Jegyző	2019. december 1.
3.1.5.	a 3.1.1. pont szerinti folyamatok előzetes tesztelésével biztosítani kell a folyamatok előre meghatározott követelmények szerinti működését;	A biztonsági kontrollfolyamatokat előzetesen tesztelni kell.	IBF	2019. december 1.

41/2015. BM R.	BIZTONSÁGI SZINTEK KÖVETELMÉNYEI	INTÉZKEDÉS
3.1.6.	a szervezetnek rendelkeznie kell információbiztonsági költség- és haszonelemzési módszertannal.	Költség- és haszonelemzési módszertan kidolgozása az információ kockázatelemzési eljárásrend részeként.
4.1.	**4. biztonsági szint**	
4.1.1.	az üzemeltetési, vagy fejlesztési tevékenységbe épített rendszeres, előre meghatározott tesztekkel biztosítani kell az üzemeltetés, vagy fejlesztés információbiztonsági intézkedéseinek hatékonyságát és megfelelőségét;	Az információbiztonsági irányítási rendszer hatékonysága mérési nak kidolgozása.
4.1.2.	tesztelési eljárásban rögzítetten biztosítani kell minden szabályozási folyamat és kontroll működését az elvárt és előre meghatározott információbiztonsági követel-mények szerint;	Az információbiztonsági irányítási rendszer hatékonysága mérési nak kidolgozása.
4.1.3.	azonnali és eredményes, előre meghatározott biztonsági intézkedéseket kell bevezetni a feltárt, vagy bekövetkezett biztonsági események kezelésére, beleértve az eseménykezelő központok, a beszállítók vagy egyéb megbízható forrás jelzése alapján lehetséges, vagy bekövetkezett biztonsági esemény kezelését is;	Biztonságkezelési eljárásrendet és eseménykezelési tervet kell kid feltárt, vagy bekövetkezett biztonsági események kezelésére, bel eseménykezelő központok, a beszállítók vagy egyéb megbízható fo se alapján lehetséges, vagy bekövetkezett biztonsági esemény keze
4.1.4.	folyamatba épített rendszeres belső értékelés alá kell vonni az egyes információ, rendszer, vagy alkalmazás biztonsága érdekében bevezetett intézkedések megfelelőségét és hatékonyságát, mely belső értékelések részben, vagy egészben történhetnek alvállalkozók, vagy más, erre feljogosított, vagy a szerv felett felügyelet gyakorló szerv bevonásával;	Éves információbiztonsági ellenőrzési tervet kell kidolgozni és vég az eredményekről tájékoztatni kell a jegyzőt.
4.1.5.	a szervezet folyamatba épített belső értékelései nem helyettesíthetőek;	Éves információbiztonsági ellenőrzési tervet kell kidolgozni és vég az eredményekről tájékoztatni kell a jegyzőt.
4.1.6.	a 4.1.3. pont szerinti forrásból származó, potenciális vagy a valódi biztonsági eseményekkel és biztonsággal kapcsolatos információk, vagy riasztások alapján tesztelési eljárást, vagy biztonsági ellenőrzést kell végezni;	Sebezhetőség vizsgálati eszköz beszerzése, sebezhetőség vizsgálat tatása
4.1.7.	a tesztelés értékelése alapján megállapított követelményeket, - beleértve a teszte-lés típusával és gyakoriságával kapcsolatos követelményeket is - dokumentálni kell, az arra jogosulttal jóvá kell hagyatni és be kell vezetni;	A sebezhetőségi vizsgálatok eredményéről jegyzőkönyvet kell felve dolgozni a sebezhetőségek elhárításának a módját. A jegyzőkönyve részére jóváhagyás céljából meg kell küldeni.
4.1.8.	az egyedi kontroll eljárások tesztelésének gyakoriságát és mélységét ahhoz kell igazítani, hogy milyen biztonsági kockázattal jár a kontrollok nem megfelelő műkö-dése.	Az információbiztonsági irányítási rendszer mérését, információbiztonsági ellenőrzési tervet és a sebezhetőségi vi tesztek mélységét és gyakoriságát úgy kell megállapítani, hog kontrollok nem megfelelő működéséből fakadó kockázatok m egyenesen arányban álljanak.

6. táblázat - A Hivatal elvárt biztonsági szintjének cselekvési terve

VI.2. Cselekvési terv a Hivatal elektronikus információs rendszerei elvárt biztonsági osztályai elérésére

Az Ibtv. 8. § (3) bekezdésében foglaltak szerint az elektronikus információs rendszerre vonatkozó védelem elvárt erősségének eléréséhez a szervezetnek lehetősége van a biz

VI.2.1. Cselekvési terv az elvárt adminisztratív védelmi intézkedések megvalósítására

A következő táblázat az elvárt adminisztratív védelmi intézkedések megvalósítására készített cselekvési tervet tartalmazza:

KÖVETELMÉNYEK			INTÉZKEDÉSEK			
77/2013. NFM R.	I. biztonsági osztály	II. biztonsági osztály	I. biztonsági osztály	Felelős	Határidő	II. bizto
3.1.1.	**Szervezeti szintű alapfeladatok**					
3.1.1.2.	Informatikai biztonsági stratégia		Információbiztonsági projekt részeként kidolgozandó.	IBF	2014. november 30.	
3.1.1.3.	Informatikai biztonsági szabályzat		Információbiztonsági projekt részeként kidolgozandó.	IBF	2014. október 31.	
3.1.1.5.		Pénzügyi erőforrások biztosítása				SzMSz módo A 2017. tervezés sc fedezet bizto információbi kiadásokra
3.1.1.6.		Az intézkedési terv és mérföldkövei				Jelen inf projekt keret
3.1.1.7.	Az elektronikus információs rendszerek nyilvántartása		A nyilvántartás elkészítése.	IT	2016. július 1.	
3.1.1.10.		Kockázatkezelési stratégia				IBSZ részek kerül.
3.1.1.11.	Az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárás		IBSZ részeként szabályozásra kerül.	IBF	2014. október 31.	
3.1.2.	**Kockázatelemzés**					
3.1.2.1.	Kockázatelemzési eljárásrend		IBSZ részeként szabályozásra kerül.	IBF	2014. október	

KÖVETELMÉNYEK			INTÉZKEDÉSEK			
77/2013. NFM R.	I. biztonsági osztály	II. biztonsági osztály	I. biztonsági osztály	Felelős	Határidő	II. bizto
3.1.3.2.		Rendszerbiztonsági terv				Valamennyi rendszer tervének elk
3.1.3.3.		Személyi biztonság				IBSZ részek kerül.
3.1.3.3.2.		Viselkedési szabályok az interneten				IBSZ részek kerül.
3.1.6.	**Emberi tényezőket figyelembe vevő - személy - biztonság**					
3.1.6.5.	Eljárás a jogviszony megszűnésekor		IBSZ-ben rögzítésre kerül.	IBF	2014. október 31.	
3.1.6.8.	Fegyelmi intézkedések		IBSZ-ben rögzítésre kerül.	IBF	2014. október 31.	
3.1.7.	**Tudatosság és képzés**					
3.1.7.1.	Képzési eljárásrend		IBSZ-ben rögzítésre kerül.	IBF	2014. október 31.	
3.1.7.2.	Biztonság tudatosság képzés		Információbiztonsági projekt részeként végrehajtásra kerül.	IBF	2014. október 31.	

7. táblázat – Cselekvési terv az elvárt adminisztratív védelmi intézkedések megvalósítására

VI.2.2. Cselekvési terv az elvárt fizikai védelmi intézkedések megvalósítására

A következő táblázat az elvárt fizikai védelmi intézkedések megvalósítására készített cselekvési tervet tartalmazza:

KÖVETELMÉNYEK			INTÉZKEDÉSEK			
77/2013. NFM R.	I. biztonsági osztály	II. biztonsági osztály	I. biztonsági osztály	Felelős	Határidő	II. biztonsági osztály
3.2.1.	**Fizikai és környezeti védelem**					

VI.2.3. Cselekvési terv az elektronikus információs rendszerek elvárt logikai védelmi intézkedéseinek megvalósítására

A következő táblázat az elektronikus információs rendszerek elvárt logikai védelmi intézkedéseinek megvalósítására készített cselekvési tervet tartalmazza:

II. BIZTONSÁGI OSZTÁLY KÖVETELMÉNYEI		INTÉZKEDÉSEK	
Sorszám	**Intézkedés típusa**	**Intézkedés**	**Érintett rendszer**
3.3.1.		**Konfigurációkezelés**	
3.3.1.1.	Konfigurációkezelési eljárásrend	IBSZ-ben kidolgozandó.	Valamennyi rendsz
3.3.1.2.	Alapkonfiguráció	Informatikai rendszerek alapkonfigurációinak dokumentálása és karbantartása.	Valamennyi rendsz
3.3.1.8.	Elektronikus információs rendszerelem leltár	Leltár elkészítése valamennyi szoftver- és hardverelem nyilvántartásba vételével.	Valamennyi rendsz
3.3.1.10.	A szoftverhasználat korlátozásai	IBSZ-ben kidolgozandó.	Valamennyi rendsz
3.3.1.11.	A felhasználó által telepített szoftverek	IBSZ-ben kidolgozandó.	Valamennyi rendsz
3.3.2.		**Üzletmenet- (ügymenet-) folytonosság tervezése**	
3.3.2.1.	Üzletmenet-folytonosságra vonatkozó eljárásrend	Ügymenet folytonosságra vonatkozó eljárásrend kidolgozása az IBSZ részeként.	Professional PE
3.3.2.2.	Üzletmenet-folytonossági terv informatikai erőforrás kiesésekre	Üzletmenet-folytonossági terv kidolgozása.	Professional PE
3.3.2.8.	Az elektronikus információs rendszer mentései	Mentési eljárási rend kidolgozása, és bevezetése a helyreállítási követelmények figyelembe vételével.	Valamennyi rendsz
3.3.2.9.	Az elektronikus információs rendszer helyreállítása és újraindítása	Informatikai rendszer összeomlása esetén a helyreállítási idők figyelembe vételével, a mentési eljárásrend alapján az érintett informatikai rendszer helyreállítása.	Valamennyi rendsz
3.3.3.		**Karbantartás**	
3.3.3.1.	Rendszer karbantartási eljárásrend	Karbantartási tervet kell készíteni, melyben rögzíteni kell a karbantartásra vonatkozó elvárásokat, feladatokat, határidőket, felelősöket, döntési folyamatokat és jogköröket.	Valamennyi rendsz

II. BIZTONSÁGI OSZTÁLY KÖVETELMÉNYEI		INTÉZKEDÉSEK	
Sorszám	**Intézkedés típusa**	**Intézkedés**	**Érintett rendszer**
		zését, korlátozását, vagy tiltását.	
3.3.5.		**Azonosítás és hitelesítés**	
3.3.5.1.	Azonosítási és hitelesítési eljárásrend	IBSZ-ben kell rögzíteni az azonosítási és hitelesítésre vonatkozó előírásokat.	Valamennyi rendsz
3.3.5.2.	Azonosítás és hitelesítés	Egyedi azonosítók létrehozása valamennyi felhasználó részére.	Valamennyi rendsz
3.3.5.4.	Azonosító kezelés	IBSZ-ben kell meghatározni az azonosító kezelést és annak megfelelően kell megvalósítani az adott informatikai rendszerben.	Valamennyi rendsz
3.3.5.5.	A hitelesítésre szolgáló eszközök kezelése	Az IBSZ-ben kell meghatározni a hitelesítési eljárásrendet és annak megfelelő-en kell kezelni a hitelesítésre szolgáló eszközöket.	Valamennyi rendsz
3.3.6.		**Hozzáférés ellenőrzése**	
3.3.6.1.	Hozzáférés ellenőrzési eljárásrend	Hozzáférés ellenőrzési eljárások kidolgozása az IBSZ részeként.	Valamennyi rendsz
3.3.6.2.	Felhasználói fiókok kezelése	Az IBSZ-ben előírt módon a felhasználói fiókok kezelésének megvalósítása.	Valamennyi rendsz
3.3.6.3.	Hozzáférés ellenőrzés érvényesítése	Az elektronikus információs rendszereknek a hozzáférés ellenőrzési eljárás-renddel összhangban érvényesíteniük kell a jóváhagyott jogosultságokat az információkhoz és a rendszer erőforrásaihoz való logikai hozzáféréshez.	Valamennyi rendsz
3.3.7.		**Rendszer- és információsértetlenség**	
3.3.7.2.	Rendszer- és információsértetlenségre vonatkozó eljárás-rend	Az IBSZ-ben kell rögzíteni a rendszer-és információsértetlenségre vonatkozó eljárásrendet.	Valamennyi rendsz
3.3.7.3.	Hibajavítás	Az IBSZ-ben kell szabályozni a hibajavítás módját, a frissítések és a biztonsági frissítések telepítését, illetve azok előzetes tesztelését.	Valamennyi rendsz
3.3.7.4.	Kártékony kódok elleni védelem	Az IBSZ-ben kell kidolgozni a vírusvédelmi eljárásokat és annak megfelelően kell megvalósítani a kártékony kódok elleni védelmet.	Valamennyi rendsz
3.3.7.5.	Az elektronikus információs rendszer felügyelete	Az IBSZ-ben kell meghatározni és annak megfelelően kell megvalósítani az	Valamennyi rendsz

II. BIZTONSÁGI OSZTÁLY KÖVETELMÉNYEI		INTÉZKEDÉSEK	
Sorszám	**Intézkedés típusa**	**Intézkedés**	**Érintett rendszer**
3.3.8.2.	Naplózható események	A naplózás IBSZ-ben foglalt követelményeinek megfelelően az informatikai rendszerekben a naplózás megvalósítása.	Valamennyi rendsz
3.3.8.3.	Naplóbejegyzések tartalma	A naplóbejegyzésekhez belső rendszeróra használata és a bejegyzések hitelesítése az IBSZ-ben meghatározott pontossághoz.	Valamennyi rendsz
3.3.8.9.	A naplóinformációk védelme	A naplózás IBSZ-ben foglalt követelményeinek megfelelően kell az informatikai rendszerekben a naplóinformációk védelmét megvalósítani.	Valamennyi rendsz
3.3.8.11.	A naplóbejegyzések megőrzése	A naplózás IBSZ-ben foglalt követelményeinek megfelelően az informatikai rendszerekben a naplózás megvalósítása.	Valamennyi rendsz
3.3.8.12.	Naplógenerálás	A naplózás IBSZ-ben foglalt követelményeinek megfelelően az informatikai rendszerekben a naplózás megvalósítása.	Valamennyi rendsz
3.3.9.	**Rendszer- és kommunikációvédelem**		
3.3.9.1.	Rendszer- és kommunikációvédelmi eljárásrend	Az IBSZ-ben kell kidolgozni a rendszer- és kommunikációvédelmi eljárásokat.	Valamennyi rendsz
3.3.9.6.	A határok védelme	IBSZ-ben kell meghatározni és annak megfelelően kell megvalósítani a határok védelmét, azok felügyeletét és ellenőrzését.	Valamennyi rendsz

9. táblázat – Cselekvési terv a logikai védelmi intézkedésekre