52.15/2020.

A Nemzeti Kibervédelmi Intézet Hatósági Főosztályának 420/A-90-2/2016. számon iktatott ellenőrzése kapcsán adott megállapításokról készített intézkedési terv és beszámoló az eddig a BfNPI által elvégzett feladatokról.			
Végzésben szereplő pont száma	Alpont	Az előírt megállapítás (kivastagított betűkkel), alatta a BfNPI intézkedése. A színnel nem jelölt részek az Informatikai Biztonsági Szabályzattal vagy más intézkedés megtételével elvégzésre, teljesítésre kerültek. A még le nem zárt intézkedéseket a jelen táblázatban sárga színnel jelöltük, melyekhez kapcsolódóan a további intézkedések előírásra kerültek.	*A BfNPI beszámolója az elvégzett feladatokról / Az előírt intézkedési terv feladata (felelős, határidő megjelölésével.*
		A hatályos informatikai biztonsági szabályzat (továbbiakban: IBSZ) felülvizsgálata és a kiadása óta történt változások átvezetése. Ennek keretén belül a következők figyelembe vétele:	
1		*A BfNPI rendelkezik az előírt, formailag megfelelő, hiteles és helytálló szakmai tartalommal bíró IBSZ el és mellékleteivel, azonban, bár a felülvizsgálat gyakorisága szabályozva van, a rendszeres felülvizsgálatok elmaradtak. (3.1.1.1.2 pont)*	*Az új IBSZ kiadásra került - éves felülvizsgálatára sor kerül. (IBF kompetencia és felelősségi körébe tartozik)*
	a	**OVI és SZVI kategóriák**	
		Az IBSZ saját biztonsági osztályokat és szinteket definiál. Nem követi a BM rendelet előírásait. (3.1.1.1.4 pont és BM rendelet 1. melléklet)	*A korábbi besorolások a felettes szerv által megbízott szervezet iránymutatása alapján nyert besorolást. Az új IBSZ követi a 41/2015. (VII. 15.) BM rendelet rendelet által meghatározott szinteket és osztályokat.*
	b	**Az informatikai és információbiztonsági tevékenységekhez kapcsolódó szerepkörök, jogosultságok, felelősségek meghatározása, továbbá a szereplők együttműködési rendszerének szabályozása.**	
		Az információbiztonsági szerepkörök nincsenek meghatározva. Az IBF kijelölése formailag megtörtént, de az információbiztonsági feladatok és felelősségi körök nem tisztázottak. A szerepkörökhöz rendelet tevékenységek és a kapcsolódó felelősség nincs meghatározva. Az információbiztonság szervezetrendszerének belső együttműködése az IBSZ-ben nincs meghatározva. (3.1.1.1.2 pont)	*Az új IBSZ már tartalmazza a szerepköröket és az IBF is kinevezésre került. A szerepkörökhöz rendelt felelősségi körök meghatározását az új IBSZ szintén tartalmazza.*
	c	**Biztonsági helyzet- és eseményértékelési eljárásrend kialakítása.**	
		Az IBSZ-ből hiányzik a biztonsági helyzet-, és eseményértékeli eljárási rendje. (3.1.1.1.3.2 pont)	*IBSZ mellékleteként bevezetésre került: B50 -s dokumentum.*
	d	**Az intézkedési tervek felülvizsgálata és karbantartása a kockázatkezelési stratégia és a kockázatokra adott válasz tevékenységek prioritásai alapján.**	
		Az IBSZ-ből hiányzik az intézkedési tervek felülvizsgálata és karbantartása a kockázatkezelési stratégia és a kockázatokra adott válasz tevékenységek prioritása alapján. (3.1.1.3.1.2 pont)	*Az IBSZ mellékleteként került bevezetésre az éves belső audit ok lefolytatásának dokumentuma, amely az eltérésekre adott válaszokat intézkedési tervben rögzíti - B11 -s dokumentum.*
	e	**A munkakörök biztonsági besorolása, az ehhez kapcsolódó ellenőrzésének szabályozása (lehetséges más belső szabályozóban is).**	
		A BfNPI IBSZ-ének 10. fejezete tartalmazza a személybiztonsági előírásokat, azonban a fejezetben leírtak nem minden esetben felelnek meg a BM rendelet 3.1.6 pontban és alpontjaiban meghatározott követelményeknek. Hiányzik a munkakörök biztonsági szintű besorolása, a személyek ellenőrzéseinek szabályozása, továbbá az interneten köbvetendő viselkedési szabályok leírása.	***AZ új IBSZ -ben meghatározott a munkakörökhöz kapcsolódó képzés (és ezek időarányosan megtörténtek), a biztonsági besorolást a munkaköri leírások fogják tartalmazni - azok átvizsgálása folyamatban van. <u>A szükséges intézkedés:</u> a BfNPI munkatársainak munkaköréhez tartozó informatikai biztonsági kategóriába történő besorolása (1-5 kategória) . Határidő: 2021. január 31. Felelős: Jogi és Birtokügyi Osztály vezetője, közreműködik az IBF***
	f	**Az interneten követendő viselkedési szabályok meghatározása.**	*Minisztériumi utasítás bekerült az IBSZ -be - az általános részt konkrét eljárásrenddel egészült ki.*
		ugyanazon intézkedések végrehajtása., mint az 1/ e.) pontnál találhatóak.	
2		**Az elektronikus információs rendszerek mentési eljárásrendjében (BFNPI Mentési Rend) rögzíteni az egyes rendszerekre vonatkozó RPO és RTO értékeket, amelyek szükségesek a mentések gyakoriságának megállapításához.**	

A Nemzeti Kibervédelmi Intézet Hatósági Főosztályának 420/A-90-2/2016. számon iktatott ellenőrzése kapcsán adott megállapításokról készített intézkedési terv és beszámoló az eddig a BfNPI által elvégzett feladatokról.			
Végzésben szereplő pont száma	Alpont	Az előírt megállapítás (kivastagított betűkkel), alatta a BfNPI intézkedése. A színnel nem jelölt részek az Informatikai Biztonsági Szabályzattal vagy más intézkedés megtételével elvégzésre, teljesítésre kerültek. A még le nem zárt intézkedéseket a jelen táblázatban sárga színnel jelöltük, melyekhez kapcsolódóan a további intézkedések előírásra kerültek.	*A BfNPI beszámolója az elvégzett feladatokról / Az előírt intézkedési terv feladata (felelős, határidő megjelölésével.*
		A mentési eljárásrendet a BfNPI Mentési rend szabályzata tartalmazza. Sem a mentési rend, sem a más szabályozó dokumentum nem tartalmaz információt az egyes EIR-ekhez tartozóan a szervezet által elfogadható RPO értékekről, és a szervezet által elvárt RTO értékekről. A fenti információk ismerete nélkül nem lehet megítélni, hogy az alkalmazott mentési rendszerek képesek-e biztostani a szervezet álal elvárt üzemeltetési célok megvalósulását.	***Az egyes EIR -ek besorolása már folyamatban van. Egyes szakrendszerek besorolását az azt üzemeltető szervezet hatóköre - más szakrendszerek esetében a fejlesztővel még egyeztetések folynak . <u>A szükséges intézkedés:</u> RPO és RTO értékek teljes körű meghatározása. Határidő: 2021. február 28. Felelős: Takács Bódis Attila informatikus***
3		**Az üzletmenet folytonosságra vonatkozó eljárásrend (BfNPI Katasztrófaelhárítási terve) aktualizálása a BM rendelet 3.1.4.2 pontban és alpontjaiban meghatározott követelményeknek megfelelően.**	
		A BfNPI Katasztrófa elhárítási terve rögzíti a működésfolytonosságra vonatkozó elvárásokat és alapelveket, azonban a dokumentumban leírtak nem mindenben felelnek meg a 3.1.4.2 pontban és alpontjaiban meghatározott követelménykenek.	*Az új IBSZ mellékleteként került bevezetésre a B36 Informatikai működésfolytonossági- és katasztrófaterv, amely a hvatkozott pontokat kielégíti*
4		**Incidenskezelési szabályzat aktualizálása a 3.1.5.8 pont szerint**	
		A BfNPI az IBSZ 15. fejezetében is az Incidenskezelési szabályzatában szabályozza a biztonsági események kezelését, azonban a leírtak nem mindenben felelnek meg a a BM rendelet 3.1.5.8 pontban és alpontjaibnan meghatározott követelményeknek.	*Az új IBSZ mellékleteként került bevezetésre a B10 -s nyomtatvány, amely a B42 -s nyomtatvánnyal együtt már kielégíti a hivatkozott pontok követelményeit.*
5		**A távozó munkavállalók esetében a jogosultságok visszavonásának dokumentálása és ellenőrzése.**	
		A helyszíni ellenőrzés során bemutatásra került egy távozó kolléga kilépőlapja. Ezen jogosultság visszavonására vonatkozó adatok nem szerepelnek. A jogosultságok időben történő visszavonásának ellenőrzése miatt szükséges szerepeltetni ezeket az adatokat a kilépő lapon. (3.1.6.4. pont)	*Az új IBSZ tartalmazza - jogviszony megszűnése fejezet (3.2.5)*
6		**A rendszerelem leltár kiegészítése, további rendszerek és eszközök közötti logikai kapcsolatok feltüntetése.**	
		A BfNPI elektronikus nyilvántartást vezet az információs rendszerelemekről, ez azonban nem tartalmazza teljeskörűen a hardver- és szoftver elemeket. (3.3.6.8. pont)	***Az új IBSZ egyik melléklete - a B12 bevezetésre került és inventory management rendszer bevezetése is folymatban van (OCS, ESET). <u>A szükséges intézkedések:</u> 1. BfNPI központi épületén belül található informatikai eszközök pilotként történő elemzése, az Inventorry rendszerek közül az intézményre alkalmas kiválasztása. Határidő: 2021. március 31. felelős: Takács Bódis Attila informatikus, az IBF közreműködéésvel. 2. A pilot projekt kiterjesztése az Igazgatóság többi ingatlanában található informatikai elemekre. Határidő: 2021. augusztus 31. (a leltárt megelőző időszak vége) Felelős: Takács Bódis Attila informatikus az IBF közreműködésével.***
7		**Az adathordozók újrafelhasználásának, selejtezésének, illetve ehhez kapcsolódóan a visszaállíthatatlan törlésüknek a szabályozása.**	
		A BfNPI az IBSZ -ben nem szabályozza az adathordozók újrafelhasználását és ehhez kapcsolódóan az adathordozók visszaállíthatatlan törlését. (3.3.8.6. és 3.3.8.7 pontok)	*Az új IBSZ tartalmazza az előírt feladatot. (4.4.2 fejezet)*

A Nemzeti Kibervédelmi Intézet Hatósági Főosztályának 420/A-90-2/2016. számon iktatott ellenőrzése kapcsán adott megállapításokról készített intézkedési terv és beszámoló az eddig a BfNPI által elvégzett feladatokról.			
Végzésben szereplő pont száma	Alpont	Az előírt megállapítás (kivastagított betűkkel), alatta a BfNPI intézkedése. A színnel nem jelölt részek az Informatikai Biztonsági Szabályzattal vagy más intézkedés megtételével elvégzésre, teljesítésre kerültek. A még le nem zárt intézkedéseket a jelen táblázatban sárga színnel jelöltük, melyekhez kapcsolódóan a további intézkedések előírásra kerültek.	*A BfNPI beszámolója az elvégzett feladatokról / Az előírt intézkedési terv feladata (felelős, határidő megjelölésével.*
8		**Kizárási házirend alkalmazása a sikertelen bejelentkezési kísérletek meghatározott száma fölött (AD) esetében**	
		Csak a szakrendszerekre vonatkozóan van kizárási házirend kialakítva, míg az AD-ba való belépés esetén korlátlan számban fordulhat elő sikertelen belépési kísérlet. (3.3.10.7.1.1. pont)	*Az IT a feltárt hiányosságot a csoportházirend módosításával oldotta meg.*
9		**OVI űrlap/ok kitöltése**	
		A BfNPI az IBSZ -ben kilenc elektronikus információs rendszert azonosított, azonban ezekről nem küldött be NEIH-OVI űrlapokat a hatósághoz. Cselekvési terv nem készült a hiányosságok felszámolására. Egy követhető és és számonkérhető cselekvési terv elkészítése szükséges, amiben a feladatok mellett a felelősök és a határidők is szerepelnek. Az előrehaladás vezetői szintű követése javasolt. (3.1.2.2 és 3.3.2.3 pontok)	***Az egyes EIR -ek besorolása folyamatban van. Egyes szakrendszerek besorolását az azt üzemeltető szervezet hatóköre - más szakrendszerek esetében a fejlesztővel még folynak az egyeztetések. A szükséges intézkedés : OVI űrlapok kitöltése. Határidő: 2021. szeptember 30. (a leltárt megelőző időszak vége) Felelős: IBF A feladatat vezetői követése: előrehaladási jelentés készítése és megküldése az IBF részéről a BfNPI Üzemeletetési Osztály vezetője számára.***
10		**SZVI űrlap/ok kitöltése**	
		A BfNPI az IBSZ-e tartalmazza a szervezet biztonsági szintbe sorolásának eredményét, azonban nem készült el a felmérésre és a követelményeknek történő megfelelésre vonatkozó NEIH-SZVI táblázat. Ennek megfelelően a hiányosságok felszámolására vonatkozó cselekvési terv is hiányzik.. (BM rendelet 2. melléklet és 3.3.2.3 pont)	***Besorolás alatt - a szervezet különböző szervezeti egységei külön kerülnek besorolásra - folyamatban van a vezetői egyeztetés. A szükséges intézkedés: NEIH SZVI táblázat kitöltése kitöltése. Határidő: 2021. május 31. Felelős: IBF A feladatat vezetői követése: előrehaladási jelentés készítése és megküldése az IBF részéről a BfNPI Üzemeletetési Osztály vezetője számára.***
11		**Rendszeres karbantartásokra vonatkozó dokumentáció bevezetése.**	
		A BfNPI-nél rendszeres karbantartásra vonatkozódokumentáció nem áll rendelkezésre. A rendszeres tervezett karbantartás elvégzése és ellenőrzése céljából szükséges lenne ennek megléte. (3.3.7.2 pont)	*Az új IBSZ mellékleteiben került kialakításra - B39 és B40*
12		**Külső rendszerekkel kapcsolódás esetében a szolgáltatási szerződésekben minden esetben szerepeltetni kell az információbiztonsági előírásokat.**	
		Külső elektronikus rendszerekhez kapcsolódós esetén a szolgáltatói szerződésekben nem minden esetben szerepelnek az információbiztonsági előírások. (3.3.10.16 pont)	*Az új IBSZ 3.4.1 -s fejezete szabályozza - ellenőrzése folyamatos*
13		**Kockázatelemzés alapján meghatározni azon adathordozók körét, amelyek titkosítása szükséges, az eredmény függvényében a használt adathordozók titkosítása.**	
		A használt adathordozók titkosítása jelenleg nem megoldott, jelenleg kockázatelemzés hiányában nem ismeretes, hogy indokolt-e ennek bevezetése, és mely adathordozók esetében. (3.3.8 pont)	*Az új IBSZ -ben a 4.4 -s fejezetben szabályozott*
14		**Hozzáférési jogosultságok felülvizsgálatának szabályozása és dokumentálása.**	
		A hozzáférési jogosultságok rendszeres felülvizsgálata nem történik meg. Erre vonatkozó előírás sem az IBSZ -ben sem más szabályozóban nincs. (3.3.10.2.1.9 pont)	*Az új IBSZ 2.5 -s fejezetében szabályozott és a B15 -s nyomtatvány segítségével igényelhető hozzáférés.*
15		**Biztonsági értékelés módszerének kidolgozása és bevezetése.**	

A Nemzeti Kibervédelmi Intézet Hatósági Főosztályának 420/A-90-2/2016. számon iktatott ellenőrzése kapcsán adott megállapításokról készített intézkedési terv és beszámoló az eddig a BfNPI által elvégzett feladatokról.			
Végzésben szereplő pont száma	Alpont	Az előírt megállapítás (kivastagított betűkkel), alatta a BfNPI intézkedése. A színnel nem jelölt részek az Informatikai Biztonsági Szabályzattal vagy más intézkedés megtételével elvégzésre, teljesítésre kerültek. A még le nem zárt intézkedéseket a jelen táblázatban sárga színnel jelöltük, melyekhez kapcsolódóan a további intézkedések előírásra kerültek.	*A BfNPI beszámolója az elvégzett feladatokról / Az előírt intézkedési terv feladata (felelős, határidő megjelölésével.*
		A biztonsági értékelés a BfNPI-nél nem valósul meg. Az elektronikus információs rendszerek és működési környezetük védelmi intézkedéseinek kontrollja hiányzik. A bevezetett védelmi intézkedések működőképességének, valamint a tervezettnek megfelelő működés értékelése dokumentált módon nem valósul meg. (3.3.4.2 pont)	*Az új IBSZ 2.10 -s fejezetében szabályozott és a B50 -s mellékletben is fellehető az eljárásrend*
16		**Publikálási szabályok kidolgozása**	
		A nyilvánosan elérhető tartalom (a BfNPI hivatalos honlapján és Facebook oldalán) publikálásának szabályai nem kellően kidolgozottak. A szabályozás célja: gondoskodni arról, hogy kizárólag pontos, szakszerű és odaillő tartalom jelenhessen meg a szervezettel kapcsolatban a fent felsorolt helyeken. (3.3.10.118 pont)	***Az új honlap kidolgozása folyamatban van; az új IBSZ pedig az 1.4.4 -s fejezetben szabályozza. <u>A szükséges intézkedések:</u> 1. Honlapfelelős és felelősségi rend, publikálási rend kialakítása a "bfnp.hu" honlapon és a BfNPI közösségi média felületein. Határidő: 2021. január 31. Felelős: Dr Kopek Annamária az Ökoturisztikai és Környezeti Nevelési osztály osztályvezetője. 2. Az informatikai biztonsági szabályzat kiegészítése. Határidő: 2021. május 31. felelős: IBF***
17		**Tesztelés eseteire, menetére vonatkozó szabályok kialakítása**	
		A tesztelés menete sem az IBSZ-ben sem más szabályzatban nem kellően szabályozott, így nincs meghatározva, hogy milyen folyamatoknál, milyen módon kell elvégezni. (3.3.5 pont)	***Az új IBSZ 2.11 -s fejezetében szabályozott - részletes eljárásrend kialakítása folyamatban van. <u>A szükséges intézkedések:</u> 1. részletes eljárásrend kialakítása a tesztelés menetéről kapcsolódva az inventory management kiválasztásához. Határidő: 2021. január 31. Felelős: Takács Bódis Attila informatikus az IBF közreműködésével. 2. Az eljárásrend alapján a tesztelés végrehajtása. Határidő: 2021. március 31. felelős Takács Bódis Attila informatikus az IBF közreműködésével.***
18		**Konfigurációkezelési eljárásrend**	
		Konfigurációkezelési eljárásrend nem állrendelkezésre. A konfigurációváltozások nem dokumentáltan történnek, az alapkonfiguráció nincs definiálva. (3.3.6.pont)	*Az új IBSZ 4.2.1 -s fejezete szabályozza, illetve a B32 -s mellékletben rögzített*
19		**Admin jogok felülvizsgálata, szoftvertelepítési lehetőségek szabályozása, ellenőrzése**	
		A felhasználók adminisztrátori jogosultsággal használják a munkaállomásaikat. A felhasználók kontroll nélkül telepíthetnek fel szoftvereket munkaállomásaikra és egy esetleges vírusfertőzés vagy ransomware támadás esetén az ártó kód továbbterjedésének nincs gátja. (3.3.6.11 pont)	*Az IT a feltárt hiányosságot a csoportházirend módosításával oldotta meg.*
20		**Inaktivitási idő - felhasználói fiókok felfüggesztése**	
		Felhasználói fiókok inaktivitása esetén nincs szabályozva annak automatikus tiltása vagy felfüggesztése. A rendszerekben nincs beállítva automatikus zárolás. A tartósan távol lévő munkatársak felhasználói fiókja esetileg sem kerül felfüggesztésre. (3.3.9.4.1.4 pont)	***Az IT a feltárt hiányosságot a csoportházirend módosításával oldotta meg. Határidő: 2020.12.31., mely időpontra a feladat elvégzésre került.***
21		**Privilegizált fiókok - kétfaktoros autentikáció**	
		A privilegizált felhasználók szükség esetén a Teamviewer alkalmazáson keresztül érik el távolról a munkaállomásokat és a szervereket. A két faktoros autentikáció csak részben került megvalósításra. (3.3.9.2 pont)	***Az IT a feltárt hiányosságot csoportházirend módosításával oldja meg. <u>A szükséges intézkedés:</u> Többtényezős hitelesítés kialakítása. Felelős: Takács Bódis attila informatikus, Gál Róbert az üzemeltetési osztály osztályvezetője***

A Nemzeti Kibervédelmi Intézet Hatósági Főosztályának 420/A-90-2/2016. számon iktatott ellenőrzése kapcsán adott megállapításokról készített intézkedési terv és beszámoló az eddig a BfNPI által elvégzett feladatokról.			
Végzésben szereplő pont száma	Alpont	Az előírt megállapítás (kivastagított betűkkel), alatta a BfNPI intézkedése. A színnel nem jelölt részek az Informatikai Biztonsági Szabályzattal vagy más intézkedés megtételével elvégzésre, teljesítésre kerültek. A még le nem zárt intézkedéseket a jelen táblázatban sárga színnel jelöltük, melyekhez kapcsolódóan a további intézkedések előírásra kerültek.	*A BfNPI beszámolója az elvégzett feladatokról / Az előírt intézkedési terv feladata (felelős, határidő megjelölésével.*
22		**Távoli hozzáférések**	
		A távoli hozzáférés szabályai nem kellően kidolgozattak. Az engedélyezési eljárás nincs dokumentálva. (3.3.10.13 pont)	*Az új IBSZ 3.4 -s fejezete szabályozza, illetve a B15 -s nyomtatvány segítségével igényelhető hozzáférés*
23		**Mobileszközök használata**	
		(A céges mobilon be van állítva a céges levelezés, viszont a mobil eszközök kötelező zárolása nincs kikényszerítve. Nincs beállítva a többszöri sikertelen feloldási kísérletet követő kikényszerített adattörlés sem. (3.3.10.15 pont)	***MDM opció beveztésével a kért intézkedés kielégíthető. Az IBSZ 3.11 pontjában a fizikai eljárásrend szabályozásra került. <u>A szükséges intézkedések</u> : 1. az 6. pontban írt inventory management kiválasztása után pilot vizsgálat leltározás utáni végrehajtása Csopakon az Igazgatóság központi épületében. Határidő: 2021. március 31. Felelős: Takács Bódis Attila informatikus. 2. A pilot projekt kiterjeésztése a BfNPI összes informatikai eszközére. Határidő: 2021. augusztus 31. Felelős: Takács Bódis Attila informatikus. 3. Mobileszközökre az MDM felhasználásval távoli törlés opció teljeskörű kiterjesztése. Határidő 2022. március 31. Felelős: Takács Bódis attila informatikus.***
24		**Naplózási eljárásrend kidolgozása, melyben ki kell térni legalább a naplózandó események meghatározására, a naplóellenőrzés folyamatára, a riasztások kezelésére.**	
		Jelenleg a naplókat csak eseti jelleggel vizsgálják felül. A naplózási eljárásrend nem dokumentált. Ennek elkészítésekor szabályozni kell, hogy mi kerül naplózásra, ki és hogyan ellenőrzi a naplókat, milyen intézkedéseket vált ki a rendellenes tevékenység észlelése. (3.3.12 pont)	*Az új IBSZ 5.4 -s fejezete rendelkezik a naplók eljárásrendjéről, illetve a B43 -s és a B45 -s mellékletek rendszeresítettek*

Csopak, 2020. november 9.

Puskás Zoltán igazgató
Balaton-felvidéki Nemzeti Park igazgatóság

Balaton-felvidéki Nemzeti Park Igazgatóság
Csopak
1.