Jelen dokumentumot elfogadom és végrehajtását elrendelem:

Puskás Zoltán s.k.,

Igazgató

VIDÉKFEJLESZTÉSI MINISZTÉRIUM

Balaton-felvidéki Nemzeti Park Igazgatóság

NEMZETI PARKI SZINTŰ INFORMATIKAI BIZTONSÁGI SZABÁLYZAT

Balaton-felvidéki Nemzeti Park

Szám: 884-51/2017.

Ügyiratszám: 884/2017.

Kiadmányozó: Puskás Zoltán igazgató

Dátum: 2017.12.06.

Hatályba lépés ideje: 2017.12.08.

Dokumentum leíró adatok

Szervezet neve:	**Balaton-felvidéki Nemzeti Park Igazgatóság - BfNPI**		
Dokumentum címe:	**BfNPI - NEMZETI PARKI SZINTŰ BIZTONSÁGI SZABÁLYZAT**		
Ügyiratszám:	884/2017.		
Kiadványozó:	Puskás Zoltán igazgató		
Készítette:	BfNPI Jogi, Igazgatási és Birtokügyi Osztály: Takács Bódis Attila, Dr. Gabler Júlia	Dátum:	2017.12.06.
Szakmailag jóváhagyta:	Veszelszki Márta Gazdasági igazgató-helyettes	Dátum:	2017.12.06.
Adatvédelmi minősítés:	3-as szintű biztonsági osztály	Verzió:	v1.01.
A dokumentum leírása:	A Balaton-felvidéki Nemzeti Park Igazgatóság szervezetére érvényes informatikai biztonsági szabályok, ill. módszertani útmutatók		
A dokumentum felülvizsgálatának szükségessége:	1. Jogszabályváltozás, szervezeti változás 2. Évente 3. Lényeges informatikai fejlesztés megvalósulása		
A dokumentum karbantartásáért felelős:	Takács Bódis Attila informatikus		

A dokumentum változásai

Verzió:	Dátum:	Készítette:	Jóváhagyta:	A változások leírása:
v1.01	2017.12.06.	BfNPI Jogi, Igazgatási és Birtokügyi Osztály: Takács Bódis Attila, dr. Gabler Júlia	Veszelszki Márta Gazdasági igazgató-helyettes	Első, jóváhagyott változat

Tartalomjegyzék

1. Bevezetés

Jelen dokumentum a Balaton-felvidéki Nemzeti Park Igazgatóság (továbbiakban: **Igazgatóság**) magas szintű Informatikai Biztonsági Szabályzata (a továbbiakban: I**BSZ**), amely támaszkodik az ISO/IEC 27001:2013 nemzetközi szabvány követelményeire, felépítése a szabvány felépítését követi.
A szabályzat tartalmazza az Igazgatóság szervezetére, bemutatóhelyére, telephelyére, irodájára (továbbiakban egységesen: szervezetére) érvényes informatikai biztonsági szabályokat.

2. A dokumentum célja, hatálya

Jelen szabályozás célja, hogy az Igazgatóságon belül a szervezeti sajátosságok meghatározta korlátok között egységes megközelítéssel legyenek rögzítve az informatikai biztonsághoz kapcsolódó szabályozások.

Az Igazgatóság Informatikai Biztonsági Szabályzata az Igazgató jóváhagyásával és aláírásával lép életbe és visszavonásig érvényben marad.

A dokumentum aktualitását, alkalmasságát, hatékonyságát minden nagyobb változáskor, de legalább évente az informatikus felülvizsgálja és az értékelést az Igazgató elé terjeszti.

Az Informatikai Biztonsági Szabályzat hatálya kiterjed:

- az Igazgatóság valamennyi szervezeti egysége vagy munkavállalója által munkavégzéssel kapcsolatban használt, illetve a szervezeti egység adatait feldolgozó, tároló vagy továbbító mindazon informatikai eszközökre és berendezésekre (számítógépek, nyomtatók, külső adattároló eszközök, aktív hálózati elemek, elektronikus adathordozók stb.) amelyeket a szervezet üzemeltet;

- a szervezeti egység területén bármely okból használt, más személy vagy szervezet tulajdonát képező illetve vagyonkezelésében lévő informatikai eszközökre és berendezésekre, amennyiben ezek a szervezet hálózatával vagy a szervezet által üzemeltetett informatikai eszközeivel adatkapcsolatot létesítenek;

- a fenti kategóriák valamelyikébe tartozó informatikai eszközökön használt vagy tárolt szoftverekre és adatokra (rendszerprogramok, alkalmazások, adatbázisok stb.), ideértve az üzemelő rendszerek adatain kívül az oktatási, teszt és egyéb célra használt adatokat is;

- a fentiekben meghatározott eszközökre és rendszerekre vonatkozó minden dokumentációra (fejlesztési, szervezési, programozási, üzemeltetési stb. dokumentumok), függetlenül azok formátumától (papír vagy elektronikus);

- az Igazgatóság által kezelt és üzemeltett eszközökön tárolt adatok teljes körére, felmerülésüktől, feldolgozási és tárolási helyüktől függetlenül.

Az IBSZ területi hatálya kiterjed az Igazgatóság valamennyi objektumára, telephelyére, illetve működési területére.

A dokumentum aktualitását, alkalmasságát, hatékonyságát minden nagyobb változáskor, jelentős súlyú biztonsági esemény bekövetkezésekor, kritikus biztonsági kockázatok felmerülése esetén, de legalább évente az Igazgatóság Jogi, Igazgatási és Birtokügyi Osztálya felülvizsgálja és az értékelést az igazgató elé terjeszti.

Jelen szabályzat előírásait érvényesíteni kell az Igazgatóság szolgáltatásaival kapcsolatban szerződéses jogviszonyban álló külső partnerek, beszállítók, gazdasági társaságok, egyéni vállalkozók és az általuk, illetve a részükre a fenti területi hatályon belül munkatevékenységet végző munkavállalóikra vonatkozóan is (a továbbiakban: Közreműködők).

Jelen szabályzat hatálybalépésével egyidejűleg a Balaton-felvidéki Nemzeti Park Igazgatóság 3076/2014. szám, nemzeti parki szintű informatikai biztonsági szabályzata hatályát veszti.

3. Rövidítések, meghatározások

Fogalom, rövidítés	Meghatározás
Adatkezelés	Az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (pl. ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítése.
Adatkezelő	Adatkezelőnek minősül az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki, vagy amely önállóan vagy másokkal együtt az adatok kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az általa megbízott adatfeldolgozóval végrehajtatja.

Fogalom, rövidítés	Meghatározás
Beléptető rendszer	Beléptető rendszernek nevezzük azokat az elsődleges intézkedéseket, amelyek a védett létesítménybe történő belépést a belépési jogosultság ellenőrzésével lehetővé teszik. A fizikai védelem tekintetében a beléptető rendszer első lépcsője az elektronikus beléptető rendszer, amely valamilyen jellemző, vagy jellemzők együttes ellenőrzésével a belépési jogosultságot a védett területre lehetővé teszi.
Biztonsági esemény	Nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat, amely az elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, és amelynek hatására az elektronikus információs rendszer által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül.
Emberi erőforrás biztonság	Az információbiztonság azon területe, melynek célja a munkatársak által kezelt információ védelme, megőrzése megfelelő szabályzatok megalkotásával és érvényre juttatásával.
Fizikai biztonság	Az információbiztonság azon területe, melynek célja az információ hordozóinak (pl. papír alapú dokumentumok, adathordozók, számítógépek) védelme, megőrzése.
Ibtv.	Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény.
Információbiztonság	Az információ bizalmasságának, sértetlenségének és rendelkezésre állásának megőrzése.
Információbiztonsági irányítási rendszer (MSZ ISO/IEC 27001:2014 szerint)	Az átfogó irányítási rendszernek az a része, amely – egy, a működési kockázatokat figyelembe vevő megközelítésen alapulva – kialakítja, bevezeti, működteti, figyeli, átvizsgálja, fenntartja és fejleszti az információvédelmet.
Informatikai biztonság	Az információbiztonságnak azon területe, melynek célja az informatikai rendszerekben elektronikusan tárolt információ megőrzése.
Infotv.	Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény.

Fogalom, rövidítés	Meghatározás
Mobil eszköz	Minden olyan mobil informatikai eszköz, amely központilag ellenőrizhető, azaz érvényesíthetők rajta az informatikai rendszer központilag meghatározott működési és konfigurációs beállításai (laptop/notebook, netbook, tablet, stb.).
NEIH	Nemzeti Elektronikus Információbiztonsági Hatóság.
PAD	Projekt Alapító Dokumentum.
Személyes adat	Az Infotv. 3. § 2. pontja alapján személyes adat az érintettel kapcsolatba hozható adat - különösen az érintett neve, azonosító jele, valamint egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző ismeret -, valamint az adatból levonható, az érintettre vonatkozó következtetés. Az emberi hang, amennyiben az természetes személlyel összefüggésbe hozható, az Infó törvény által védett személyes adat.

4. Az informatikai biztonsági szabályozáshoz kapcsolódó dokumentumok

Az Igazgatóságnak rendelkeznie kell Informatikai Biztonsági Szabályzattal, és ehhez szorosan kapcsolódó szabályozási dokumentum rendszerrel. Ennek megfelelően az Igazgatóságnak rendelkeznie kell az alábbi szabályzatokkal, vagy az adott kérdéskört szerepeltetni kell, jelen dokumentumban. A szabályzatok, amelyekre az Informatikai Biztonsági Szabályzata hivatkozik, vagy tartalmazza azt:

#	Szabályozási terület	Szabályozás célja
1.	Adathordozó kezelési szabályzat	Formális eljárás biztosítása a cserélhető adathordozók kezelésére a teljes életciklusukra vonatkozóan.
2.	Az információbiztonsággal kapcsolatos intézkedések a projektvezetési szabályzatban	Az információbiztonsággal foglalkozni kell a projektvezetésben - tekintet nélkül a projektek típusára.
3.	Beszerzési szabályzat	Biztosítani kell, hogy az információbiztonság szerves része legyen az információs rendszereknek a teljes életciklus során, beleértve a rendszerek **beszerzését** is.

#	Szabályozási terület	Szabályozás célja
4.	Biztonsági szabályzat (fizikai biztonságra vonatkozóan)	Megelőzni a jogosulatlan fizikai hozzáférést, károkozást és zavarást a szervezet információi és információ feldolgozó eszközei vonatkozásában.
5.	Eszközhasználati szabályzat	Biztosítani az információ feldolgozó eszközök helyes és biztonságos üzemelését.
6.	Fejlesztési szabályzat	Biztosítani kell, hogy az információbiztonság szerves része legyen az információs rendszereknek a teljes életciklus során, beleértve a rendszerek **fejlesztését** is.
7.	Felhasználói informatikai biztonsági útmutató	A felhasználók tájékoztatása a mindennapi munkájuk során betartandó szabályokról. Az IBSZ kivonata.
8.	Hálózathasználati szabályzat	Minden hálózati szolgáltatásra meg kell határozni a biztonsági mechanizmusokat, a szolgáltatási szinteket és a kezelési követelményeket, és be kell építeni a hálózati szolgáltatási megállapodásokba.
9.	Hozzáférés-felügyeleti szabályzat	Biztosítani a hozzáférést az arra jogosult felhasználók számára, és megelőzni a jogosulatlan hozzáférést a rendszerekhez és szolgáltatásokhoz.
10.	IBSZ (Informatikai Biztonsági Szabályzat) az Igazgatóságra vonatkozóan	Az ágazati szintű biztonsági szabályozáshoz (jelen dokumentum) kapcsolódva a szervezeti szintű szabályozás megvalósítása.
11.	Incidenskezelési szabályzat (biztonsági incidensre vonatkozóan)	Biztosítani egy következetes és hatásos módot az információbiztonsági incidensek kezelésére, beleértve a biztonsági események és gyengeségek kommunikációját is.
12.	IT Üzemeltetési szabályzat	- Biztosítani az információ feldolgozó eszközök helyes és biztonságos üzemelését; - Biztosítani, hogy az információk és az információ feldolgozó eszközök védettek legyenek a rosszindulatú szoftverek ellen

#	Szabályozási terület	Szabályozás célja
		(**vírusvédelem**); - Védekezni az adatvesztés ellen (**mentés szabályozása**); - Nyilvántartani az eseményeket, és létrehozni bizonyítékokat (**naplózás szabályozása**); - Biztosítani az üzemelő rendszerek sértetlenségét (**telepítés szabályozása**); - Megelőzni a műszaki sebezhetőségek kihasználását; - Ágazat specifikus szakrendszerek üzemeltetési szabályozása (**üzemeltetési szabályozás**).
13.	IT változáskezelési szabályzat	Biztosítani kell, hogy az információbiztonság szerves része legyen az információs rendszereknek a teljes életciklus során, beleértve a rendszerek **fejlesztését** is.
14.	Kockázatkezelési szabályzat	Az Igazgatóságnak fel kell mérnie azokat a kockázatokat, melyekkel foglalkozni kell ahhoz, hogy: ▪ biztosítsák az információbiztonság-irányítási rendszertől elvárt eredmények elérhetőségét; ▪ megelőzzék vagy csökkentsék a nem kívánt hatásokat. Az Igazgatóságnak szabályoznia kell az ezen kockázatokkal kapcsolatos tevékenységeket.
15.	Mobil és távmunka biztonsági szabályzat	Biztosítani a távmunka és a mobil eszközök használatának biztonságát.
16.	Munkaköri leírások	Az egyes munkakörökben elvárt információbiztonsági felelősségek, feladatok.
17.	Kinevezések/Munkaszerződések kiegészítése informatikai biztonsági követelményekkel	Az munkavállalókkal kötendő szerződéses megállapodásoknak meg kell adniuk az információbiztonságra vonatkozó felelősségeket mind a munkavállalók, mind a munkáltató oldaláról.
18.	Működésfolytonossági terv (BCP)	Az Igazgatóságnak olyan folyamatokat,

#	Szabályozási terület	Szabályozás célja
		eljárásokat és intézkedéseket kell létrehoznia, dokumentálnia, bevezetnie és fenntartania, amelyek biztosítják a működés folytonosságának elvárt szintjét egy kedvezőtlen helyzetben.
19.	Selejtezési szabályzat	Biztosítani kell, hogy az információ feldolgozó eszközök selejtezése során, az azokon tárolt adatok megsemmisítésre kerüljenek.
20.	Szerződések kiegészítése informatikai biztonsági pontokkal	A szerződéses vállalkozókkal kötendő megállapodásoknak tartalmazniuk kell az információbiztonságra vonatkozó felelősségeket mind az Igazgatóság, mind a vállalkozók oldaláról.
21.	Titkosítási szabályzat	Alkalmas és hatásos titkosítást biztosítani, hogy védeni lehessen az információk bizalmasságát, hitelességét és/vagy sértetlenségét.
22.	Tűzvédelmi szabályzat	A szabályzat célja, hogy rögzítse a vezetők, a munkatársak tűzvédelmi feladatait, a munkavégzésre, használatra vonatkozó általános követelményeket, valamint meghatározza a tűzvédelmi eljárások szabályait.
23.	Vagyonelem kezelési szabályzat	Azonosítani a szervezeti vagyonelemeket és meghatározni a megfelelő védelmi felelősségeket.
24.	Vagyonleltár	Az információs vagyonelemeket és az információ feldolgozó eszközöket azonosítani kell, ezeknek a vagyonelemeknek egy leltárát kell kialakítani, és azt karban kell tartani.

5. A biztonsági irányítás

A biztonsági irányítási folyamatok szervezése során a teljes körű védelem elvét kell szem előtt tartani. Ez azt jelenti, hogy a védelem szervezése kiterjed minden folyamatra, minden erőforrásra és azok valamennyi életciklusára.

Az információ-feldogozó rendszerek használatba vétele során a használhatósági és a biztonsági elveket egyensúlyban kell tartani. Ennek egyik következménye, hogy az információ-feldolgozó rendszerek használói csak a munkájukhoz szükséges mértékben férhessenek hozzá a szervezet információs vagyonához. A másik következmény az, hogy a védelmi intézkedéseket úgy kell tervezni, hogy a kockázatok mértékével arányosan a szervezet folyamatai hatékonyságát és minőségének javítását szolgálja.

A biztonsági irányítás feladatai:

- **Tervezés** - kiemelt eleme a biztonsági politika kialakítása és kommunikálása a munkatársak számára (7. fejezet).
- **A biztonsági feladatok megvalósulásának ellenőrzése** - eszköze a belső biztonsági ellenőrzések, auditok rendszere. A tervezett biztonsági ellenőrzéseket az informatikai biztonságért felelős vezető az éves biztonsági programterv részeként elfogadott biztonsági ellenőrzési tervben irányozza elő. A biztonsági ellenőrzések mindhárom (információbiztonsági, fizikai biztonsági és vagyonvédelmi, humánbiztonsági) funkcionális területre kiterjednek. Az eseti biztonsági ellenőrzéseket az informatikai biztonságért felelős vezető többnyire a szakterületekről beérkezett információk alapján, biztonsági incidensek bekövetkezésekor rendeli el.
- **A biztonság fejlesztése** - magában foglalja:
    - új biztonsági célkitűzések kijelölését,
    - a biztonsági követelmények felülvizsgálatát, új biztonsági követelmények bevezetését,
    - a biztonsági folyamatok, eljárásrendek felülvizsgálatát, fejlesztését, új biztonsági folyamatok bevezetését,
    - a biztonsági technológiák felülvizsgálatát, fejlesztését, új biztonsági technológiák bevezetését,
    - a humánerőforrások biztonságtudatossági szintjének fejlesztését,
    - egyéb erőforrások (pl.: létesítmény) biztonságszempontú átalakítását, fejlesztését.

6. Kockázatkezelés

Az Ibtv. 9. § (1) bekezdés d) pontja alapján a Szolgáltató szervezeti biztonsági szint besorolása: 3.

Az Igazgatóság biztonsági szintjére vonatkozóan az Ibtv. végrehajtási rendelete 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 szóló 41/2015. (VII.15.) BM rendelet (továbbiakban: 41/2015. (VII.15.) BM rendelet) meghatározott védelmi követelményeknek való megfelelés, valamint az Igazgatóság szolgáltatásaival összefüggésben kezelt adatok és információk bizalmasságának, sértetlenségének és rendelkezésre állásának, továbbá a szolgáltatásokat kiszolgáló elektronikus információs rendszer, illetve elemei sértetlenségének és rendelkezésre állásának zárt, teljes körű, folytonos és kockázatokkal arányos védelmének biztosítása érdekében az Igazgatóság az alábbi kockázatmenedzsment eljárásokat működteti:

 Az informatikai biztonsági kockázatok csökkentése érdekében az Igazgatóságnál kockázatkezelési eljárásokat kell végrehajtania, amelynek ki kell terjednie a kockázatok felmérésére, értékelésére, valamint a kockázatokat csökkentő intézkedések meghatározására.

 Az azonosított kockázatokat elemezni szükséges, meg kell határozni, hogy az azonosított kockázatok valamilyen kockázatcsökkentő intézkedést igényelnek-e, vagy döntés alapján felvállalható kockázatoknak minősülnek. Szükség esetén a kockázatok csökkentése érdekében intézkedéseket kell hozni és végrehajtani azokat.

 A kockázatok kezelését dokumentálni szükséges, az aktualitásról rendszeresen gondoskodni kell.

A kockázatkezelés módszertanára vonatkozóan az Igazgatóságra vonatkozóan kötelező előírás nincs, azt az Igazgatóság saját maga választja meg.

A biztonsági osztályba sorolást legalább háromévenként vagy szükség esetén soron kívül, dokumentált módon felül kell vizsgálni. A soron kívüli biztonsági osztályba sorolást az elektronikus információs rendszer biztonságát érintő jogszabályban meghatározott változás vagy új elektronikus információs rendszer bevezetése esetén szükséges elvégezni. A soron kívüli felülvizsgálatot akkor is el kell végezni, ha az Igazgatóság státuszában, illetve az általa kezelt vagy feldolgozott adatok vonatkozásában változás következik be.

6.1. Kockázatok felmérése

A védelmi intézkedések kockázatarányos kialakítása érdekében az Igazgatóság rendszeresen, legalább évente egyszer hajt végre kockázatelemzési tevékenységet.

A kockázatelemzési folyamat kiterjed:

- Az információ-feldolgozó rendszer erőforrásainak (technológia, humán, adat, stb. minden elemére,
- Az információ-feldolgozó rendszer erőforrásainak minden életciklus folyamatára (tervezés, bevezetés, működtetés, kivonás folyamatára).

A kockázatelemzést a 41/2015. (VII.15.) BM rendelet alapján kell elvégezni.

Az Igazgatóságnál működő szolgáltatásokat kiszolgáló elektronikus információs rendszer biztonsági osztály besorolásáról a 41/2015. (VII.15.) BM rendelet 1. melléklet Az elektronikus információs rendszer biztonsági osztályba sorolása meghatározott szempontok szerint, következetesen végrehajtott kockázatelemzés alapján az igazgató, mint az Igazgatóság informatikai biztonságért felelős vezetője gondoskodik.

A kockázatelemzés során biztosítani kell, hogy a kockázatelemzés eredményei reprodukálhatóak legyenek. Ennek érdekében a kockázatelemzési módszertan dokumentálása szükséges (a 2. Táblázat, 14 dokumentum).

6.2. Kockázatcsökkentő intézkedések tervezése

A feltárt kockázatok kezelésére javasolt védelmi intézkedéseket nyilván kell tartani, illetve azok bevezetését a kockázatok mértékével arányos időtávon tervezni szükséges.
A védelmi intézkedéseket úgy kell kialakítani, hogy azok védelmi költsége arányos legyen az általuk védett vagyon értékével.

A védelmi intézkedéseknek ki kell terjednie:

- az információ-feldolgozó és információbiztonsági folyamatok fejlesztésére:
- folyamatfejlesztési feladatokra (szabályozási feladatok),
- szervezetfejlesztési feladatokra.
- az erőforrások információbiztonsági fejlesztésére:
- a humán erőforrásrendszer fejlesztésére (információbiztonsági oktatás, tudatosítás, stb.),
- a technológiai rendszer fejlesztésére (védelmi rendszerek bevezetése, fejlesztése, stb.), cseréjére, működtetésére, kivonására,
- egyéb erőforrások (pl.: létesítmény) fejlesztésére, cseréjére, működtetésére, kivonására. A kockázatkezelés módszertanára vonatkozóan az Igazgatóság részéről kötelező előírás nincs, arról az Igazgató dönt.

7. Informatikai biztonsági politika

Az Igazgatóság működésnek szükséges feltétele, hogy a munkatársak számára folyamatosan és megbízhatóan, elfogadható szinten álljon rendelkezésre a munkájuk végzéséhez szükséges elegendő számú és megfelelő minőségű erőforrás mind hardver, mind jogtiszta szoftver, mind pedig kommunikációs lehetőség vonatkozásban. Szükséges feltétel továbbá, hogy ezen erőforrások feleljenek meg az adott időponthoz illeszkedő hardver és szoftver technológiai fejlettségi szintnek.

Annak érdekében, hogy az ágazat szervezetei zavartalanul és hatékonyan végezhessék tevékenységüket, a rendelkezésre álló informatikai erőforrások biztonságos működtetése, az erőforrások optimális kihasználhatóságának biztosítása elengedhetetlen. Szükséges, hogy az állam és az ügyfelek érdekei maximálisan

figyelembe legyenek véve és a releváns jogszabályok be legyenek tartva.

Az Igazgatóság tevékenysége során hozzáfér, létrehoz, felhasznál, kezel bizalmas adatokat, adatbázisokat. Az Igazgatóság tevékenységét információs eszközök, adatbázisok, tudásbázisok támogatják, ill. teszik lehetővé. Ennélfogva az Igazgatóság számára kiemelt követelmény az információk és a kezelésükhöz szükséges eszközök biztonságának (bizalmasság, sértetlenség, rendelkezésre állás) folyamatos fenntartása, a szolgáltatások megbízható, működő infrastruktúrával támogatása.

A fentiek betartásához az Igazgatóságnak a következőket kell szem előtt tartania:

- Az Igazgatóság dolgozói azonosítják és betartják a kezelt információkra, információs eszközökre vonatkozó szervezeti, jogszabályi és az ügyfelek által megkövetelt előírásokat, a szükséges intézkedéseket beépítik dokumentációs rendszereikbe.
- Gondoskodik a szolgáltatási tevékenységek támogatására, követésére, felügyeletéhez használt megbízható informatikai rendszerekről, szolgáltatásokról, folyamatos rendelkezésre állásukról, megfelelő működésükről, az igényekkel, változásokkal és a rendelkező erőforrásokkal összhangban fejlesztésükről.
- Biztosítja a biztonságos kommunikációs eszközöket a partnerekkel történő együttműködéshez.
- Az Igazgatóság vezetői időszakonként azonosítják, értékelik az információbiztonságot veszélyeztető kockázatokat, döntést hoznak az elfogadható és a kezelendő kockázatokról és a kezelendő kockázatok esetén a kockázatokkal arányban meghatározzák a kockázatok kezeléséhez szükséges kockázatjavítási intézkedéseket, kontrollokat. Csak olyan kockázatok tekinthetők elfogadhatónak, amelyek az információk és a kezelésükhöz szükséges eszközök biztonságának (bizalmasság, sértetlenség, rendelkezésre állás) folyamatos fenntartását nem veszélyeztetik.
- Biztosítja, hogy a munkatársak és minden érintett szerződéses partner megismerje a rá vonatkozó biztonsági előírásokat, ezek megtartásának fontosságát.
- Gondoskodik az informatikai rendszer biztonságának fenntartásáról, az esetleges incidensek kezeléséről, a folyamatos működés megszakadása esetén ennek helyreállításáról.
- Követi a biztonság növelése érdekében tett intézkedések megvalósulását, eredményességét, a kockázatok változásait, szükség esetén további intézkedéseket tesznek a kockázatok csökkentésére.

Az Ágazati Szintű Informatikai Biztonsági Politika aktualitását, alkalmasságát, hatékonyságát minden nagyobb változáskor, de legalább kétévente a VM IPF vezetője felülvizsgálja és az értékelést a vidékfejlesztési miniszter elé terjeszti.

8. Az informatikai biztonság szervezete

Az informatikai biztonság megfelelő szintű biztosítása érdekében a szabályozás kiterjed szervezeti kérdésekre, mind az Igazgatóság szervezetén belüli, mind a külső ügyfelekkel, partnerekkel fenntartott kapcsolatok kezelésére vonatkozóan.

Az informatikai biztonsági szervezet meghatározásánál figyelembe kell venni azt, hogy a Földművelésügyi Minisztérium Projektkoordinációs és IT Biztonságfelügyeleti Főosztálynak ágazati informatikai felügyeleti joga és kötelezettsége is van az informatikai biztonsággal kapcsolatban.

Az Ibtv. elvárásaival összhangban a Földművelésügyi Minisztérium Projektkoordinációs és IT Biztonságfelügyeleti Főosztály vezetője köteles gondoskodni az elektronikus információs rendszerek védelméről a fenti törvény 11.§ (1) szakaszában részletezett módon. Tehát a Földművelésügyi Minisztérium Projektkoordinációs és IT Biztonságfelügyeleti Főosztály vezetője felel a Földművelésügyi Minisztérium és az általa üzemeltetett ágazati szakrendszerek körében az informatikai biztonság, valamint az adatbiztonság technológiai és ügyrendi felügyeletéért, adatok kezeléséért.

8.1. Feladatok, felelősségek, hatáskörök

Annak érdekében, hogy az Igazgatóság munkatársai és a munkavégzésre irányuló egyéb jogviszony alapján ott munkát végző munkatársak (például külső fejlesztők, támogatók) tisztában legyenek felelősségükkel, alkalmasak legyenek feladatkörük betöltésére, valamint a vétlen, vagy a rosszhiszemű tevékenységből, illetve az informatikai eszközökkel való bármilyen visszaélésből származó kockázatok csökkenjenek, a biztonsággal összefüggő feladat- és felelősségi köröket az IBSZ-szel összhangban kell meghatározni és dokumentálni.

A munkaköröket, feladatokat, felelősségeket és hatásköröket alapvetően az Igazgatóság Szervezeti és Működési Szabályzata, valamint az egyes munkatársak munkaköri leírásai határozzák meg. Az egyes szervezeti egységek IT biztonsági rendszereinek kialakítása során részletesen szabályozni kell az IT biztonság tekintetében kitüntetett szerepkörökhöz tartozó feladatokat, felelősségeket és hatásköröket az adott szervezeti egység sajátosságainak megfelelően.

Az informatikai eszközök előírásszerű és biztonságos üzemeltetésének biztosítására, az Igazgatóság vagyontárgyainak jogosulatlan illetve nem szándékolt módosítása, valamint a visszaélés lehetőségének csökkentése érdekében a feladat- és a felelősségi köröket megfelelően szét kell választani.

Tipikusan a következő szerepköröket kell meghatározni:

- Informatikai biztonságért felelős vezető
- Adatgazdák/vagyongazdák
- IT rendszer üzemeltetéséért felelős személy
- Személyzeti vezető
- IT üzemeltető (rendszergazda)
- Munkatársak

8.1. Belső szervezethez kapcsolódó további intézkedések

Titoktartási kötelezettség terhel minden, az Igazgatóság informatikai rendszereivel kapcsolatba kerülő természetes és jogi személyt, tekintet nélkül arra, hogy a kapcsolat milyen jogviszonyból ered. A titoktartási kötelezettség a szerződéses partnerek alvállalkozóira teljes körűen vonatkozik.

A titoktartási kötelezettség kiterjed a rendszerben kezelt adatokra, valamint a rendszer felépítésére, működési rendjére vonatkozó adatokra, a biztonsági rendszabályokra egyaránt. A titoktartási kötelezettség a időkorlát nélkül áll fenn és az érintett személy a mindenkor érvényes jogszabályok alapján tartozik ezen kötelezettségéért felelősséggel.

Minden munkatárs (beleértve az ideiglenes, ill. megbízási szerződés alapján munkát végző munkatársakat is) csak Titoktartási nyilatkozat aláírása után kezdheti meg az érdemi munkát, kaphat hozzáférést információkhoz, erőforrásokhoz.

A munkatársak informatikai biztonsághoz kapcsolódó felelősségi és hatásköreit a „Munkaköri leírások” tartalmazzák. Ezek kitérnek a hatóságokkal, felügyeleti és kormányzati szervekkel történő kapcsolattartásra, illetve a szakmai szervezetekkel, fórumokkal, szervezetekkel, személyekkel való kapcsolattartásra is.

8.3. Együttműködés külső szervezetekkel

Bármely informatikához kapcsolódó szolgáltatást nyújtó szolgáltató, ill. alvállalkozó valamint más együttműködő partnerrel való együttműködés megkezdése előtt a szerződést előkészítő munkatárs az informatikai biztonságért felelős vezető bevonásával megvizsgálja a felmerülő informatikai biztonsági kockázatokat, hozzáférési igényeket, és a szükséges kontrollokat beépíti a partnerrel kötött szerződésbe, kapcsolódó megállapodásba, Projekt Alapító Dokumentumba (PAD-ba). Szolgáltató, ill. alvállalkozó bevonása miatt fellépő új kockázat felmerülésekor a kockázatot az informatikai biztonságért felelős vezető a kockázat-felmérési eljárások során kezeli.

A külső partnerek képviselőivel az IBSZ-t a feladatnak megfelelő mértékben ismertetni kell. A betekintés mélységének meghatározása az IT üzemeltetésért felelős munkatárs felelőssége. A szerződéskötés és az együttműködés során biztosítani kell, hogy a külső partner (fejlesztő cég) az általa telepített, fejlesztett informatikai rendszert úgy konfigurálja, hogy annak minden eleme és egésze eleget tegyen az IBSZ-ben

előírtaknak.

9. Vagyontárgyak kezelése

Az IT vagyontárgyak védelmének megfelelő szintű védelme érdekében nyilvántartásba kell venni és vagyongazdákhoz kell rendelni, továbbá osztályozni szükséges az összes materiális és immateriális vagyontárgyat. Az Igazgatóság informatikai vagyonát folyamatosan frissülő listák tartalmazzák. Ezek kiindulásként szolgálnak a kockázatelemzéshez és a védelmi intézkedések meghatározásához.

Az Igazgatóság adatvagyona informatikai rendszerekben van tárolva. Annak érdekében, hogy a különböző informatikai rendszerek sajátosságaiból adódó eltérő védelmi igények érvényre juthassanak, ugyanakkor a rendszerek nagy számából adódó összetett követelményrendszer egységesen kezelhető legyen, szükség van arra, hogy az informatikai rendszerek biztonsági osztályokba kerüljenek besorolásra.

Az egyes biztonsági osztályokba az egymással közel azonos védelmi igényű rendszerek kerülnek. A követelmények az egyes kategóriák eltérő védelmi igényei alapján, differenciáltan kerültek meghatározásra. Az egyes informatikai rendszereket annak alapján kell biztonsági osztályokba sorolni, hogy a hozzájuk kapcsolódó adatvagyon elemek milyen biztonsági osztályba tartoznak. Több biztonsági osztály esetén a legszigorúbbat kell alapul venni. Az IT üzemeltetést leíró dokumentációnak tartalmaznia kell, hogy az egyes rendszerek milyen biztonsági osztályba tartoznak és ennek megfelelően milyen követelményeket szükséges érvényesíteni rájuk. Az egyes biztonsági osztályokra vonatkozó követelményeket a melléklet tartalmazza. Ez a minimálisan szükséges követelményeket tartalmazza, ennek megfelelően az egyes konkrét rendszerek esetén további követelmények is felmerülhetnek

A már meglévő rendszerek cseréje, megújítása esetén meg kell vizsgálni, és szükség esetén az aktuális kockázatoknak megfelelően módosítani kell a besorolást. Új rendszerek bevezetésénél el kell végezni a rendszerek osztályokba való besorolását. Amennyiben a módosítások vagy az újonnan történő besorolások esetén megállapítást nyer, hogy a meglévő kategóriák már nem megfelelőek, új osztályozási rendszert kell felállítani, és végre kell hajtani valamennyi rendszer újbóli besorolását. Új kategória rendszert csak működési folyamatok új, aktuális kockázatelemzése alapján lehet felállítani.

A kategóriákba való besorolás, illetőleg maguknak a kategóriáknak a szükség esetén való módosítása tekintetében a szakmai felelősöknek és az információbiztonságért felelős vezetőnek együttesen kell javaslatot tenniük, amit az igazgató fogad el, ill. hagy jóvá.

9.1. Informatikai eszközök

Az Igazgatóság informatikai eszközei a következő kategóriákba vannak besorolva.

- Alkalmazások.
- Szoftverek.
- Szerverek
- Hálózati aktív elemek.
- Hálózatok
- Felhasználói munkaállomások.
- Nyomtatók, szkennerek.
- Egyéb berendezések (helymeghatározó, navigációs (GPS, DGPS) eszközök, adathordozók, multimédiás eszközök stb.).

9.2. Adatvagyon

Az egyes adatkörök leginkább releváns jellemzőiként a következő biztonsági osztályok[1] vannak rögzítve:

9.2.1. Osztályba sorolás a bizalmasság tekintetében (IV: az információvédelem osztályai)

- **Nyilvános adatok**
  Azok az adatok, amelyek minél szélesebb körű megismerése az Igazgatóság érdeke (pl. honlapra kikerülő tájékoztató anyagok). Ezekre az adatokra vonatkozóan nincsenek előírva bizalmassági követelmények és ennek megfelelően a bizalmasság tekintetében biztonsági osztályokba sincsenek besorolva.

- **Alap biztonsági osztály (IV-A)**
  Tipikusan személyes adatok, szervezeti/üzleti titkok, pénzügyi adatok, illetve az Igazgatóság belső szabályozásában hozzáférés-korlátozás alá eső adatok biztonsági osztálya. Más rendelkezés hiányában a szervezeti dokumentumok az alap biztonsági osztályba tartoznak. Az alap biztonsági osztályon belül megkülönböztetjük a következő kategóriákat:

  - **Ágazat számára nyilvános adatok:**
    Azok az adatok, amelyek megismerése az Igazgatóságon belül minden munkatárs számára lehetséges.

  - **Szervezet számára nyilvános adatok:**
    Azok az adatok, amelyek megismerése az Igazgatóságon belül minden munkatárs számára lehetséges.

1 MEH ITB 12. sz. ajánlás alapján.

- **Szervezeti egység számára nyilvános adatok:**
  Azok az adatok, amelyek megismerése az adott szervezeti egységen (osztályok) belül minden munkatárs számára lehetséges.

- **Csoport számára nyilvános adatok:**
  Azok az adatok, amelyek megismerése az Igazgatóságon belül csak meghatározott munkatársakból álló csoport számára lehetséges.

- **Fokozott biztonsági osztály** (Érzékeny adatok biztonsági osztálya) **(IV-F)**
  Azon adatok biztonsági osztálya, amelyek megismerése szerződés vagy törvény által korlátozott (pl. szolgálati titok, különleges személyes adatok, nagy tömegű személyes adatok).

- **Kiemelt biztonsági osztály** (A minősített adatok védelméről szóló 2009. évi CLV tv. szerint minősített adatok biztonsági osztálya) **(IV-K)**
  Azon adatok biztonsági osztálya, amelyek megismerése állami előírás szerint korlátozott (államtitok). A minősített adatokról a Földművelésügyi Minisztérium minősített adat kezelésével kapcsolatos Biztonsági Szabályzatának kiadásáról szóló 3/B/2015. (II.3.) utasítás rendelkezik.

3-as szintű biztonság

A központi államigazgatási szervekre vonatkozik (a Kormány és a kormánybizottságok kivételével). Az Igazgatóság ebbe a 3-as szintű biztonsági osztályba tartozik.

9.2.2. Osztályba sorolás a sértetlenség, illetve rendelkezésre állás tekintetében (MM: a megbízható működés osztályai)

- **Alap biztonsági osztály (MM-A)**

  Azon adatok biztonsági osztálya, amelyek rendelkezésre állási, illetve sértetlenségi problémái az Igazgatóság szempontjából nem meghatározó. Az alap biztonsági osztályon belül megkülönböztetjük a következő kategóriákat:

  - **Jelentéktelen**
    Meghibásodása, kiesése, elveszítése nincs érdemi hatással a tevékenységekre (Bár bosszantó lehet, és kisebb mennyiségű többletmunkát okozhat).

  - **Minimális**
    Meghibásodása, kiesése, elveszítése többletmunkát, erőforrás lekötést okozhat (Ugyanakkor szervezeten belül kezelhető).

- **Fokozott biztonsági osztály (MM-F)**

  Azon adatok biztonsági osztálya, amelyek rendelkezésre állási, illetve sértetlenségi problémái az Igazgatóság működésben jelentős hatást válthatnak ki (pl. jogszabálysértés, bevétel kiesés, imázs vesztés, elmarasztalás stb.). A fokozott biztonsági osztályon belül megkülönböztetjük a következő kategóriákat:

  - **Érzékelhető**
    Meghibásodása, kiesése, elveszítése eseti követelménysértést okozhat (határidő,

elemzések lehetősége, stb.), amelynek hatása a szervezeten kívül is érzékelhető lehet.

- **Jelentős**
  Meghibásodása, kiesése, elveszítése jelentős anyagi, illetve jogi következményeket okozhat.

- **Kiemelt biztonsági osztály (Kritikus adatok biztonsági osztálya) (MM-K)**

  Azon adatok biztonsági osztálya, amelyek meghibásodása, kiesése, elveszítése az alaptevékenység ellátását akadályozhatja, súlyos anyagi és/vagy jogi következményeket, illetve reputációromlást okozhat.

10. Emberi erőforrások biztonsága

Az emberi erőforrás rosszhiszemű és nem rosszhiszemű tevékenysége miatti károk megelőzése, illetve a károk hatásának minimalizálása érdekében védelmi intézkedéseket kell bevezetni a munkavégzés minden fázisában. Az emberi erőforrások védelme során figyelembe kell venni a hatályos jogszabályokat, szabályzatokat, eljárásrendeket.

A munkáltatás informatikai biztonsági feltételeit a munkaszerződéseknek (vállalkozói együttműködés esetén az vállalkozói szerződés), és a munkaköri leírásoknak is tartalmazniuk kell. A munkatársak kiválasztási folyamatában az munkáltatás feltételek között szerepeltetni kell az informatikai biztonsági követelményeket is. Az igazgató meghatározza, hogy mely munkakörök betöltéséhez szükséges nemzetbiztonsági átvilágítás. E munkakörökben a munkavégzés csak akkor kezdhető meg, ha a vizsgálat alapján a munkatárs az adott munkakör betöltésére alkalmasnak bizonyul.

A munkavégzés csak akkor kezdhető meg, ha a munkatárs megismerte a vonatkozó informatikai biztonsági szabályzatokat és erről írásban nyilatkozott. Törekedni kell arra, hogy a munkatársak informatikai biztonsági képzettsége és tudatossága folyamatosan fejlődjön. Az e területen megtett intézkedéseket dokumentálni kell.

A vezetőknek minden szinten feladata az informatikai biztonsági követelmények, eljárások működésének elvárása, betartatása és ellenőrzése. Az informatikai biztonsági követelmények megszegése esetén az alkalmazott fegyelmi eljárást és az alkalmazott szankciók részleteit rögzíteni kell.

Munkatársak foglalkoztatási viszonyának megszűnése, változása esetén a munkatárssal a közvetlen vezető átadás-átvételi megállapodást köt, mely tartalmazza a felelősségek, feladatok, a munkatárs által kezelt információk átadását. A megállapodás rögzíti az átadás ütemtervét, a hozzáférések megszűntetését, az eszközök visszaadását, visszavételét, az esetleges átmeneti intézkedéseket. A hozzáférések megszüntetéséért a közvetlen vezető felelős.

11. Fizikai védelem

Az illetéktelen fizikai behatolás, károkozás, rongálás, a vagyontárgyak fizikai károsítása, eltulajdonítása és egyéb fizikai jellegű negatív események megelőzése, illetve hatásuk mértékének csökkentése érdekében védelmi intézkedéseket szükséges bevezetni. Ennek megfelelően rögzíteni kell a következő szabályokat:

- A telephelyek, épületek és helyiségek védelmére vonatkozó szabályok.
- A berendezések védelmére vonatkozó szabályok, beleértve a mobil eszközöket is.

A fizikai védelemre vonatkozó szabályoknak a következő területeket kell lefednie (összhangban a szervezet adottságaival és lehetőségeivel):

- mechanikai védelem;
- elektronikai jelzőrendszer;
- élőerős védelem;
- beléptető rendszer;
- biztonsági kamera rendszer;
- villám- és túlfeszültség védelem;
- tűzvédelem.

12. A működés és kommunikáció védelme

A biztonságos és megbízható üzemeltetés érdekében védelmi intézkedéseket szükséges bevezetni. Ennek megfelelően rögzíteni kell a következő szabályokat:

- A rendszerek üzemeltetésére vonatkozó szabályok
- Külső szolgáltatók nyújtotta szolgáltatások igénybe vételére vonatkozó szabályok
- Rendszerek tervezésre és bevezetésre vonatkozó szabályok
- A rosszindulatú szoftverek negatív hatásainak megelőzésére, ill. kezelésre vonatkozó szabályok
- A biztonsági mentésre vonatkozó szabályok
- A hálózati működésre vonatkozó szabályok
- Az adathordozók kezelésre vonatkozó szabályok
- Az biztonságos adattovábbításra vonatkozó szabályok
- Az e-kereskedelemre vonatkozó szabályok
- A naplózásokra vonatkozó szabályok

13. Hozzáférés kontroll

Az Igazgatóság minden munkatársa számára biztosított az IT hálózathoz, az email rendszerhez, a felhasználói munkaállomásokra telepített standard konfiguráció szoftvereihez egyedi azonosítóval, jelszóval történő hozzáférés, ill. saját használatú munkaállomásán az adatok kezelése a munkavégzéshez szükséges mértékben. Olyan levelező rendszerek használata, amelyek kívül esnek a NEKI üzemeltetésén, nem megengedett. A tiltás alól különösen indokolt esetben eseti felmentést adhat az informatikai biztonságért felelős vezető. Az indoklást minden esetben írásban kell rögzíteni.

A fentiektől különböző alkalmazásokhoz való hozzáférés a szervezetben elfoglalt munkakörnek megfelelően lehetséges.

Az internet használatot és az email rendszer használatát saját döntése alapján az IT bármikor korlátozhatja, megtilthatja, a forgalmat ellenőrizheti, fekete és fehér listákat alkalmazhat, tartalomszűrést végezhet.

Az Igazgatóság informatikai rendszeréhez külső szervezetek, munkatársak VPN kapcsolaton keresztül történő hozzáférése alapvetően tiltott. Ugyancsak alapvetően tiltottak a WIFI rendszerek felhasználására épülő kapcsolatok. A tiltás alól különösen indokolt esetben eseti felmentést adhat az informatikai biztonságért felelős vezető. Az indokolást minden esetben írásban kell rögzíteni és engedélyezés esetén pontosan meg kell határozni a betartandó feltételeket (pl. elkülönült hálózat, VPA2 titkosítás stb.). Minősített adatok VPN-en keresztüli eléréséhez nem adható engedély.

Az IT üzemeltetés operatív feladatainak elvégzése, az alapbeállítások megtétele, telepítések elvégzése az IT üzemeltetők feladatai. Amennyiben lehetséges, a hozzáférés felügyeletet a központi címtárra épülően kell megvalósítani, funkcióhoz kapcsolódó csoportokra megadott hozzáférés beállítások segítségével.

A külföldi felhő-alapú tárhely-szolgáltatás[2] igénybevétele a munkatársak számára a fő szabály szerint a nemzeti adatvagyon vonatkozásában tilos. Amennyiben a munkatárs számára szükséges az ilyen szolgáltatás igénybevétele, azt a Nemzeti Elektronikus Információbiztonsági Hatóság (NEIH) engedélyezheti. Az Igazgatóság köteles gondoskodni arról, hogy az ilyen szolgáltatás igénybevétele (a fenti engedély hiányában) ne legyen lehetséges.

13.1. Felhasználó hozzáférés kezelés és felügyelet

Minden munkatársnak egyedi azonosítóval és ehhez kapcsolódóan egyedi jelszóval kell rendelkeznie. A felhasználói azonosítókat, ill. jelszavakat munkába álláskor az adott szervezeti egység vezető dokumentált kérésére az IT üzemeltetés biztosítja. A szervezeti egység vezető kérésében megadja, hogy a munkába álló munkatárs mely csoportoknak lesz tagja. A munkatárs az IT üzemeltetéstől kapott azonosítókat kizárólag személyesen veheti át és a jelszavakat a munkatársnak az első belépés során meg kell változtatnia.

Csoportosan használt accountok nem alkalmazhatók. A különböző jogosultságú felhasználók (alkalmazás, vagy hozzáférés) csoportonkénti korlátozása azonban nélkülözhetetlen (Group policy).

Jelszónak kell tekinteni a biometriai azonosítást is, azonban ez esetben törekedni kell a biometriai azonosítás és a hagyományos jelszó együttes alkalmazására.

A felhasználói fiókok (account) alkalmazásával korlátozásra kerülnek az információk és

2 Például: Dropbox, OneDrive, Google Drive.

erőforrások használata a felhasználó számára, úgy, hogy az munkaköri feladatainak ellátásához szükséges, de elégséges mértékű legyen, azaz minden egyes felhasználó hozzáférjen a munkavégzéshez szükséges minden adat- és programfájlhoz, de semmi olyan állományt ne érhessen el, amelyek nem szükségesek a feladatai maradéktalan ellátásához.

Az egyes adatkörökhöz hozzáférést csak az adatgazda dokumentált engedélyével lehet kiadni, a kiadott, érvényes hozzáféréseket az IT biztonságért felelős munkatárs kezdeményezésre évente ellenőrizni kell.

A dolgozó köteles adatkezelési nyilatkozatot tenni (4.sz. melléklet)

13.2. Eszközkezelés

Az eszközök kezelése, használata során minden Felhasználónak gondosan be kell tartani az alábbiakat:

- Minden olyan előírást, mely az Eszközök kezelési útmutatójában szerepel.
- Ha egy Eszközre nincs ilyen, akkor az intézmény által kiadott kezelési útmutatóban leírtakat. Amennyiben ilyen kezelési útmutató sincs, a Felhasználó a rendszergazdánál érdeklődhet, aki ezek után szóbeli bemutatót tart, vagy dokumentációt szerez az Eszközhöz.
- Minden Eszközt csak a kezelési útmutatóban leírtak szerint lehet használni.
- A szoftverek, dokumentumok használata, létrehozása során a szerzői jogokra vonatkozó jogszabályokat. Fokozott figyelmet kell fordítani az ún. jogtisztaságra.
- A munka és tűzvédelmi előírásokat, szabályokat.
- az adatvédelmi törvény általános rendelkezéseit.
- a Szervezeten belüli adatbiztonság érvényesítését.
- Tilos az Eszközöket és azok részeit áthelyezni, burkolatukat, csatlakozásaikat
- megbontani. Erre jogosultsága csak a rendszergazdának van. A rendszergazda is csak kkor bonthatja meg a burkolatot, ha az Eszköz ez által nem veszíti el garanciáját. Amennyiben ilyen eset áll fenn, a rendszergazda köteles a garanciális szerviz helyére szállíttatni az Eszközt és az intézmény garanciális jogait érvényesíttetni.
- Tilos a számítógépekre engedély nélkül szoftvert telepíteni, illetve letörölni. Amennyiben valamelyik Felhasználó ezt mégis megteszi, a felelősség őt terheli.
- A Felhasználók kötelesek minden meghibásodást jelenteni a rendszergazdának.
- A Felhasználóknak tilos az Eszközök elektromos csatlakozásait megbontani. Elektromos meghibásodás, pl. zárlat gyanúja esetén az Eszközt a Felhasználó köteles áramtalanítani. Ha a meghibásodás az elektromos hálózatában keletkezik, úgy az egész hálózatot áramtalanítani kell a főkapcsolóval.
- Az Eszközök kezelésének bemutatása a rendszergazda feladata, az ahhoz kapcsolódó speciális tudnivalók ismertetése is. Mindenki csak azokat az Eszközöket használhatja, melyekre engedélyt kapott, és kezelésükre ki lett oktatva. A

használható Eszközök körének meghatározása a felhasználói jogosultság kiadásával párhuzamosan történik.

13.3. Jogosultságok

- Az Eszközök használatának módját a felhasználói jogosultság szabályozza. A Felhasználók különböző jogosultságokkal rendelkezhetnek, melyeket jelen szabályzat alapján, a meghatározott jogosultsági szinteknek megfelelően kell meghatározni.
- A minimum jogosultsági szint mindenkit megillet, aki az Igazgatósággal kormányzati szolgálati jogviszonyban, vagy munkajogviszonyban jogviszonyban áll, és aláírásával igazolta, hogy a Szabályzat tartalmát megismerte, annak betartását vállalja. A minimum jogosultsági szint adható az intézménnyel jogviszonyban nem állók részére is. A további jogosultsági szinteket a minimum szint kiegészítéseként kell értelmezni.
- A felhasználótól a jogosultsági szintjének megfelelő jogot megtagadni csak indokolt esetben lehet. A jogosultsági szintnek megfelelő szabályok betartása a hálózatba nem kötött eszközök használata esetén is kötelező.

13.4. A felhasználói jogosultságok szintjei:

Szint	Jogosultak	Jogok
Minimum	bárki, aki nem kormánytisztviselő, vagy egyéb munkáltatói jogviszonyban áll az Igazgatóságnál	Általános azonosító, mely lehetővé teszi a munkához szükséges Eszköz elérését, esetlegesen fénymásoló használat
Alap	Az Igazgatóság bármely dolgozója	Egyéni azonosító az Eszköz eléréséhez + saját könyvtár a szerveren + fénymásoló, fax., illetve telefon kód
Közép	Az Igazgatóság bármely kormánytisztviselője	Alap + Internet hozzáférés + esetleges betekintés az engedélyezett másik munkacsoportba
Emelt szintű	Igazgatóhelyettesek, osztályvezetők	Alap + Internet hozzáférés + esetleges betekintés az engedélyezett másik munkacsoportba az SzMSz-ben meghatározott feladatkörükben
Maximum	Igazgató	Alap + Internet hozzáférés + betekintés minden munkacsoportba

Adminisztrátor	Az adott feladatra kijelölt személy	Speciális jogok, pl. hozzáférés az iktatórendszerhez, központi e-mailhez, ,web oldalak karbantartásával kapcsolatos feladatok ellátásához, bármi egyébhez
Rendszergazda	A BfNPI rendszergazdája	korlátlan

A speciális feladatok (pl. postamesterség, webmesterség), illetve az azokhoz tartozó jogok alapértelmezésben a rendszergazdát illetik meg. Ezek egy-egy jól elhatárolható hálózati adminisztrációs feladat elvégzéséhez rendelhetők, s a rendszergazda tudtával, és regisztráltan más személynek átadhatók. A speciális jogok, illetve az ezekhez tartozó azonosítók magán célra nem használhatók fel**.** Ezek használata csak a szükséges rendszeradminisztráció erejéig történhet. Az ehhez szükséges kiemelt jogokat a rendszergazda biztosítja. Amennyiben a rendszergazda úgy ítéli meg, hogy a speciális feladatokat ellátó személy a rendszer biztonságát veszélyezteti, úgy joga van a kiemelt jogok használatának lehetőségét felfüggeszteni. Erről, és a felfüggesztés okáról köteles haladéktalanul beszámolni az Igazgatónak.

A Felhasználók a számítógép hálózat szolgáltatásait a felhasználói azonosító és az ahhoz tartozó jelszó segítségével vehetik igénybe. Az egyéni azonosító és az alapjelszó (melyet első bejelentkezéskor kötelesek megváltoztatni) kiosztása a rendszergazda feladata, amennyiben a felhasználó igényt tart saját hálózati könyvtárra, melyhez csak ő fér hozzá. Ezt az igényt jeleznie kell a rendszergazdának. Az egyéni jelszót igénylő Felhasználókról nem szükséges külön nyilvántartást vezetni, mivel a szerver könyvtár struktúrájából egyértelműen kiderül.

13.5. Felhasználási azonosítók

Felhasználói azonosítók a szoftverekbe való bejelentkezéshez, vagy a saját hálózati könyvtárba való bejelentkezéshez használt jelszavakat jelenti.

A felhasználói azonosítók kezelésének szabályai:

- Minden Felhasználó felel a rábízott felhasználói azonosítók és az ahhoz rendelt jogok biztonságáért. Az azonosítók használatra másnak még a tulajdonos jelenlétében sem engedhetőek át.
- Minden Felhasználó csak a saját azonosítóival használhatja a hálózatot és az Eszközöket.
- A felhasználói azonosítóhoz tartozó jelszót csak annak birtokosa ismerheti.
- Amennyiben felmerül a gyanú, hogy a jelszó más tudomására jutott, úgy azt azonnal meg kell változtatni, vagy jelezni kell a rendszergazdának.
- Amennyiben valaki észleli, hogy mások kísérletet tesznek a felhasználói jelszavak megszerzésére, azt azonnal jelezni kell a rendszergazdának.

- Minden, más személy jelszavának vagy adatainak megszerzésére irányuló cselekedet súlyos fegyelmi vétség.
- A felhasználói azonosító tulajdonosa elsődlegesen felel az azonosító használatával elkövetett szabálytalanságokért. Akkor is felelősségre vonható, hogy ha bebizonyosodik, hogy azt nem ő használta, de gondatlansága folytán jutott az azonosító illetéktelen kezekbe.
- Ennek érdekében a Felhasználó a számítógépes munkahely elhagyásakor minden alkalommal köteles kilépni a hálózatból, illetve az általa használt azonosítóval védett alkalmazásokból.

- A felhasználó jelszó, azonosító átadását senki sem kérheti, még a rendszergazda sem.

13.6. Felhasználói felelősségek

A felhasználó felelős a szervezet által kezelt (birtokolt) adatok és erőforrások védelméért, etikus módon történő használatáért, a biztonsági és egyéb belső szabályozások, utasítások betartásáért. A munkatársaknak az IT biztonság megvalósítása során a tipikusan a következő kötelezettségeik vannak:

- Az informatikai erőforrások rendeltetésszerű használata, megóvása.
- A jogszabályokban, és a belső szabályozásokban megjelenő informatikai biztonsági követelmények, előírások betartása.
- Az informatikai biztonsági eseményt azonnali jelentése közvetlen felettesének, annak eredménytelensége esetén közvetlenül az IT biztonságért felelős vezetőnek.

14. Információs rendszerek fejlesztése, karbantartása

A fejlesztésekre vonatkozó szerződéseknek, ill. a szerződésekhez tarozó műszaki specifikációknak, ill. a fejlesztési projektekhez tartozó PAD-oknak ki kell térniük az IT biztonsági követelményekre és azokra az átadás-átvételi feltételekre, amelyek alapján ezek ellenőrzésre kerülnek.

A fejlesztés tervezése során az IT biztonsági követelményeket a fejlesztésért felelős az IT biztonságért felelős vezetővel együttműködve azonosítja, és illeszti a specifikációba. meghatározzák, hogy a rendszer működése során milyen bemenő adat ellenőrzési, feldolgozás ellenőrzési, titkosítási, üzenet sértetlenség ellenőrzési, kimenő adat ellenőrzési követelmények fogalmazódnak meg, és a kapcsolódó követelményeket szintén beépítik a specifikációba. A specifikációt elfogadás előtt írásban véleményezi az IT biztonságért felelős vezető.

Minden fejlesztés esetén át kell venni és el kell tárolni a forráskódot és a fejlesztői környezetet.

A bevezetésre kerülő rendszereket bevezetés előtti tesztelni szükséges. A tesztelésnek ki kell térnie a bevezetés által érintett kapcsolódó rendszerek tesztelésére is. A tesztelések és a bevezetés során az IT üzemeltetésnek kell gondoskodnia arról, hogy

éles rendszeren csak engedélyezett és felügyelt módosítás történhessen. Ugyancsak az IT üzemeltetésnek kell gondoskodnia arról, hogy a megfelelőség ellenőrzéséhez használt teszt adatokhoz, illetve a forráskódokhoz illetéktelen ne férjen hozzá.

Amennyiben külső fejlesztők működnek közre a fejlesztésben, a fejlesztéshez kijelölt projektvezető feladata az információ kiszivárgás kockázatának csökkentése és a fejlesztőkkel együttműködés során a biztonsági követelmények betartása, betartatása. E célból együtt kell működnie az IT biztonságért felelős vezetővel.

Annak érdekében, hogy az informatikai rendszereknek a biztonság szerves részét képezze, a biztonsági követelményeket már az életciklus tervezési, fejlesztési, beszerzési szakaszában figyelembe kell venni. Az üzemeltetés és karbantartás során az információbiztonsági követelményeket folyamatosan fenn kell tartani.

15. Informatikai biztonsági események kezelése

A munkatárs feladata, hogy minden olyan veszélyforrást, amely az informatikai biztonságra nézve érdemi fenyegetést jelent vagy jelenthet, azonnal jelentse közvetlen felettesének, eredménytelenség esetén pedig az igazgatónak.

Veszélyforrások és fenyegető tényezők alatt különösen a következők értendők:

- az IBSZ-ben vagy egyéb hatályos szabályzatban, jogszabályban előírt informatikai biztonsági rendszabályok lényeges megszegése illetve ennek gyanúja;
- a felismert vagy felismerni vélt, az informatikai biztonságot lényegesen veszélyeztető esemény, ezen belül különösen:
  - nem nyilvános adat illetéktelen személy általi megismerése,
  - informatikai rendszerekben tárolt adatok illetéktelen személyek általi megváltoztatása, törlése vagy hozzáférhetetlenné tétele,
  - informatikai rendszer működésének, használatának jogosulatlan akadályozása,
  - a szervezet által nem engedélyezett vagy licenccel nem rendelkező szoftver telepítése,
- a fentiek bármelyikére tett kísérlet (például felhasználói jelszavak egymás közötti megosztása, vírus-fertőzés);
- a felismert, vagy felismerni vélt védelmi gyengeség, biztonsági rés, sérülékenység, hiányos vagy pontatlan szabályozás.

Az értesített feladati sorrendje:

1. a beérkező jelentések rögzítése a Hibajegy-kezelő rendszerbe
2. a beérkező jelentés kivizsgálása,
3. amennyiben a jelentés biztonsági eseményként kerül azonosításra, úgy annak késedelem nélküli kivizsgálása,

4. a szükséges intézkedések meghozatala és azok felelőseinek kijelölése,
5. a teljes elhárítási folyamat dokumentálása,
6. a tanulságok kiértékelése és szükség esetén a szabályozások módosítása,
7. az esetleges szankciók végrehajtása.

Az informatikai biztonsági események szabályozott kezelése érdekében az Ágazat egyes szervezeteinek a következő szabályokat kell rögzíteni (a **Hiba! A hivatkozási forrás nem alálható.**, #11 dokumentumban):

- Az informatikai biztonsági eseménynek és gyengeségek bejelentésének és eszkalációjának szabályai.
- Az informatikai biztonsági eseménynek és gyengeségek kezelésére vonatkozó szabályok.

16. Működésfolytonosság

A Működésfolytonossági tervben rögzíteni szükséges azokat a kontrollokat, amelyek a működési folyamatok kiesésmentes menetét biztosítják. A követelményeknek tartalmaznia kell az informatikai rendszerek, eszközök rendelkezésre állási követelményeit. Azonosítani kell azokat az intézkedéseket, amelyek elősegítik a kiesésmentes működést, továbbá azokat, amelyek az esetleges kiesések esetén alkalmazhatók.

Kockázatelemzésre épülően működésfolytonossági tervet kell készíteni a működésfolytonosság megszakadásának megelőzésére, elkerülésére, illetve az informatikai katasztrófa helyzetek kezelésre, a folytonosság helyreállítására.

A terveket rendszeresen karban kell tartani, ill. tesztelni szükséges. A felülvizsgálatoknak az IT biztonsági felelős kezdeményezésre legalább évente (ill. nagyobb változások esetén a változást követően) meg kell történnie.

A kritikus működési folyamatok megszakadásának megelőzése, továbbá az esetleges kiesések kezelése érdekében a következőket kell rögzíteni:

- A kritikus működési folyamatok és maximális megengedett kieséseik
- A megszakadások megelőzésre vonatkozó preventív jellegű szabályok
- Reaktív jellegű informatikai katasztrófa tervek

17. Megfelelőség

17.1. Megfelelés a jogi követelményeknek

Folyamatosan követni kell az informatikai biztonság tekintetében releváns jogszabályokat és az Igazgatóság által kötött szerződések informatikai biztonságot érintő összetevőit. Az informatikai biztonságot meghatározó belső szabályozást a

releváns jogszabályok változása esetén aktualizálni szükséges.

Az informatikai biztonságot érintő jogszabályok változásának követése **az informatikai biztonságért felelős vezető feladata.** A jogszabályok megváltozása esetén az IT biztonságért felelős vezető feladata, hogy szükség esetén javaslatot tegyen intézkedésekre, folyamatok, eljárások módosítására. Amennyiben szerződés keretében keletkezik új, informatikai biztonságra vonatkozó követelmény, a projektvezető feladata a követelmény jelzése az IT biztonságért felelős vezetőnek.

A szoftverek jogtisztaságának betartása érdekében **a szoftverek használatához szükséges licencekről nyilvántartást kell vezetni.**

A licence nyilvántartás kérdése hozzákapcsolódik más **IT eszközök nyilvántartás**ához. A licencek nyilvántartása az IT üzemeltetés, a nyilvántartás értékelése az IT biztonságért felelős vezető feladata. Amennyiben licence-igény következik be, az IT biztonságért felelős vezető tesz javaslatot a probléma feloldására.

Az Információs önrendelkezési jogról és az információszabadságról szóló törvénynek való megfelelés érdekében el kell készíteni és folyamatosan naprakészen kell tartani a törvény által előírt **adatvédelmi nyilvántartások**at. A nyilvántartások elkészítése és karbantartása az adatvédelmi felelős felelőssége. A nyilvántartás elkészítéséhez az Adatgazdáknak információt kell nyújtaniuk.

17.2. Megfelelés a politikának, szabványoknak és műszaki megfelelés

A folyamatos vezetői, informatikai biztonsági felelősi ellenőrzések mellett a **megfelelőségeket belső felülvizsgálatok, ill. külső, független felülvizsgálatok lefolytatásával időszakonként vizsgálni szükséges**. A felülvizsgálatoknak az IT biztonságért felelős vezető kezdeményezésre legalább évente (ill. nagyobb változások esetén a változást követően) meg kell történnie.

A vizsgálatok során feltárt eltérésekre a kockázatokkal arányos helyesbítő és megelőző intézkedéseket kell végrehajtani. Az intézkedések kezdeményezése az IT biztonságért felelős vezető tesz javaslatot.

Amennyiben a vizsgálatokhoz szoftvereket, teszt adatbázisokat kell használni, úgy ezeket hozzáférési szempontból elkülönítetten kell kezelni. Az éles rendszereket, meg kell védeni az illegális betekintés, módosítás ellen. A vizsgálatokat úgy kell tervezni, hogy biztosított legyen a kellő mélység, de a vizsgálat a bizalmassági, sértetlenségi, rendelkezésre állási követelményeket ne sértse.

A jogi, törvényi vagy szerződéses kötelezettségek betartása érdekében a következőket kell rögzíteni:

- A releváns jogszabályok követésének szabályai
- A rendelkezésre álló licencek
- Adatvédelmi nyilvántartások

- Auditálási szabályok
- esetben lehet. A jogosultsági szintnek megfelelő szabályok betartása a hálózatba nem kötött eszközök használata esetén is kötelező.

18. Jogszabályok, rendeletek, szabványok, ajánlások

8. 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról.
9. 2009. évi CLV. törvény a minősített adat védelméről.
10. 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról.
11. 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.
12. 1069/2014. (II. 19.) Korm. határozat Magyarország Nemzeti Infokommunikációs Stratégiájáról.
13. 1139/2013. (III. 21.) Kormányhatározat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról.
14. 38/2011. (III. 22.) Kormányrendelet a nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozásának biztosításáról.
15. 2010. évi CLVII. Törvény a nemzeti adatvagyon körébe tartozó állami nyilvántartások fokozottabb védelméről.
16. ISO/IEC 2700x szabványsorozat az információbiztonságról.

19. Melléklet

19.1. Informatikai rendszerek védelmi igényei

Biztonsági osztály	**A biztonsági osztályra vonatkozó minimális védelmi igények**
3-as szintű biztonsági osztály	• A 3-as szintű biztonsági osztályba tartozó anyagok logikai hozzáférését jelszavakon és hozzáférési jogosultságokon alapuló védelmi rendszerrel kell biztosítani. • A jelszavak használatára vonatkozó fő szabályok a következők: o Legalább 8 karakterből kell állnia. o Legalább 1 számot, 1 nagybetűt és nem értelmes karakter sorozatot kell tartalmaznia. o Jelszavak helyett biometriai azonosítás használható. • A naplózni kell a következőket: o Sikeres bejelentkezések.

Biztonsági osztály	A biztonsági osztályra vonatkozó minimális védelmi igények
	○ Sikeres alkalmazás és rendszerindítások ill. leállítások. • A 3-as szintű biztonsági osztályba tartozó adatok képernyőkön történő megjelenítése csak felügyelet esetén lehetséges (üres képernyő policy). • A 3-as szintű biztonsági osztályba tartozó papíralapú anyagok nyomtatott példányai csak munkaidőben, felügyelet mellett lehetnek elzáratlanok (üres íróasztal policy), munkaidőn kívül elzárva kell őket tartani. Amennyiben nem feltétlenül szükséges, kerüljük az anyagok kinyomtatását. • A 3-as szintű biztonsági osztályba tartozó adatokat tartalmazó adathordozókat, ill. ezek papír alapú változatait selejtezni kizárólag fizikai megsemmisítés útján lehetséges. • A 3-as szintű biztonsági osztályba tartozó adatokat tartalmazó meghibásodott számítógép szervizbe történő szállítása előtt belőle az adathordozót el kell távolítani. • Adatátvitelre valamint mentésre, archiválásra használt adathordozók tárolása csak megbízhatóan zárt helyen történhet. • Biztosítani kell az adathordozók és dokumentációk tűz- és vagyonvédett tárolását. • Figyelembe kell venni a 2011. évi CXII. törvény az információs önrendelkezési jogról és az információ-szabadságról törvény előírásait • A rendszer megbízhatóságát jó minőségű és megfelelő számú referenciával rendelkező hardver és szoftver termékek beszerzésével kell biztosítani. • A szerverek és a hálózati aktív elemek számára olyan szünetmentes villamos energia ellátást kell biztosítani, amely képes legalább 30 percnyi villamos energia kiesés áthidalására. • A szervereket és a hálózati aktív elemeket, valamint a kábelrendezőket, továbbá a dokumentációt zárható helyiségekben kell elhelyezni. • A szervereket és a hálózati aktív elemeket hideg tartalékolással kell ellátni. • Hibatűrő diszk alrendszereket és tápegységeket kell alkalmazni. • Adatbázisokról (beleértve a biztonsági napló állományokat is) heti teljes és napi inkrementális mentést kell végezni külön adattárolóra. Biztosítani kell, hogy a külső adattárolók ciklikus csere esetén legalább 1 hétig ne kerüljenek felülírásra. • A rendszerek üzemeltetésének támogatására 24 órán belüli hibaelhárításra vonatkozó support szükséges.

19.2. Releváns IT biztonsági szerepkörök – szervezeten belüli munkakörök összerendelése

IT biztonsági szerepkör	Szervezeten belüli munkakör
IT biztonságért felelős vezető	Nemzeti Környezetügyi Intézet (NEKI)
Adatgazdák/vagyongazdák	igazgató
IT rendszer üzemeltetéséért felelős vezető	informatikus

19.3. Fogalomtár

Fogalom	Meghatározása
Adat	Az információ absztrakt, egyezményes jelrendszerben rögzített reprezentációja. Tények, elképzelések, utasítások emberi vagy technikai eszközökkel történő formalizált ábrázolása ismertetés, feldolgozás, ill. távközlés céljára.
Adatállomány	Valamely informatikai rendszerben lévő adatok logikai összefogása, amelyet egy névvel jelölnek.
Adatátvitel	Adatok szállítása összeköttetéseken, összekötő utakon (például számítógépek között).
Adatbázis	Informatikai szemléletű megközelítés esetén használatos: strukturált adatok összessége, amelyet egy tárolására, lekérdezésére és szerkesztésére alkalmas szoftvereszköz kezel.
Adatbiztonság	Az adatok jogosulatlan megszerzése, módosítása és tönkretétele elleni műszaki és szervezési intézkedések és eljárások együttes rendszere.
Adatfeldolgozás	Az adatok gyűjtése, rendszerezése, törlése, archiválása.
Adatkör	A szervezeti működést szem előtt tartó megközelítés fogalma: az azonos működési területekhez tartozó adatok összességét jelenti.
Adatgazda	Az a szervezeti pozíció, aki rendelkezik az adott adatkörhöz történő hozzáférésekről.
Adathordozó	Adatok tárolására alkalmas eszköz (diszk, pen drive, memóriát tartalmazó kisméretű eszköz, mikrofilm, papír stb.)
Adatvagyon	A külső szervezetek számára szolgáltatott, ill. a szervezet saját belső működéshez szükséges releváns adatok összessége, függetlenül attól, hogy az milyen adathordozón, ill. milyen jelleggel (adatbázis, fájl, papír) áll rendelkezésre.

Fogalom	Meghatározása
Biztonság	Kedvező állapot, amelynek a megváltozása nem kizárt, de kis valószínűségű.
Bizalmasság	Az a tulajdonság, amely arra vonatkozik, hogy az adatot csak az arra jogosultak ismerhessék meg, illetve rendelkezhessenek a felhasználásáról.
Fenyegetettség	Olyan állapot, amelyben az erőforrások bizalmassága, sértetlensége, rendelkezésre állása sérülhet.
Hoax	Leggyakrabban emailben terjedő álhírek, megtévesztő lánclevelek elnevezése.
Informatikai biztonság	Olyan állapot, amikor a cég vagy intézmény informatikai erőforrásai bizalmassága, sértetlensége, hitelessége és rendelkezésre állásának a fenyegetettsége minimális, azaz igen kicsi a kedvező állapot megváltozásának valószínűsége.
Informatikai szolgáltatás	Információtechnológián alapuló rendszerek által működtetett kapcsolódó funkciók rendszere, amely egy vagy több szervezeti tevékenységet támogat. Bár számos hardver, szoftver, telekommunikációs elem alkotja, a felhasználó számára koherens és önálló entitásként érzékelhető.
IP cím	Az internetre csatlakoztatott gépek egyedi azonosításra szolgáló logikai szintű cím.
ITIL	IT Infrastructure Library – Az IT rendszerek tágabb értelemben vett üzemeltetésére vonatkozó nemzetközi ajánlásgyűjtemény.
Megengedő lista	Klasszikus spamszűrési módszer (whitelist), amellyel biztosítható, hogy a legitim levelek véletlenül se kerüljenek a spamek közé.
PIN kód	Personal Identification Number, személyes azonosító kód.
Rendelkezésre állás	Olyan állapot, amelyben a rendszer az eredeti rendeltetésének megfelelő szolgáltatásokat nyújtani tudja elvárt performanciával, meghatározott helyen és időben.
ServiceDesk	Az a szervezeti egység, amely felé a felhasználók jelezhetik az informatikai rendszer használata során fellépő problémáikat és amely ezek elhárításában támogatást, segítséget nyújt.
Sértetlenség	Az a tulajdonság, amely arra vonatkozik, hogy az adat az eredeti állapotnak megfelel, fizikailag és logikailag teljes és bizonyítottan vagy bizonyíthatóan az elvárt forrásból származik.
SPAM	Kéretlen reklámlevelek, melyek küldése a legtöbb esetben törvénybe ütköző tevékenység.

Fogalom	Meghatározása
Szakrendszer	Jogszabály által szabályozott, az FM, illetve egy vagy több háttérintézmény szakmai munkáját támogató egyedi fejlesztésű alkalmazás, adatbázis, illetve egyéb szoftver.
Torrent	Tartalmak felhasználók egymás közötti cseréjére létrehozott elosztott rendszer. Sok esetben jogvédett tartalmak illegális megosztására alkalmazott szolgáltatás.
Tűzfal	A szervezet hálózatának határfelületén elhelyezett berendezések és szabályok összessége, amelyek segítségével a külső és belső hálózat közötti forgalom naplózásra és korlátozásra kerül.
Veszélyforrás	Olyan tényező, amelynek hatására, ill. bekövetkezésekor az IT rendszerben nem kívánt állapot jön létre, az IT rendszer biztonsága sérül.
Vírus	Szándékosan károkozás céljából készített kód, amely a felhasználó szándéka ellenére települ fel a számítógépre és annak hibás működését okozza
VPN	Virtual Private Network. Olyan magánhálózat, amely az internet felhasználásával, de azon keresztül titkosított csatornán valósul meg.
Warez oldal	A szerzői jogvédett tartalmak jogsértő kereskedelme céljából létrehozott tartalomszolgáltatás.

19.4. Adatkezelési nyilatkozat - minta

ADATKEZELÉSI NYILATKOZAT

Alulírott név: …….., munkakör: …….., a Balaton-felvidéki Nemzeti Park Igazgatóság munkavállalója nyilatkozom, hogy a munkakörömhöz tartozó feladatok ellátása során a tudomásomra jutott információkat megőrzöm, azt illetéktelen személyek részére nem adom át.

A munkavégzés során csak a részemre hozzáférhető adatokkal dolgozom, más adatok hozzáférésére kísérletet sem teszek.

Nyilatkozom, hogy a munkáltató Balaton-felvidéki Nemzeti Park Igazgatóság Informatikai Biztonsági Szabályzatát ismerem, azt rám nézve kötelezőnek fogadom el, és annak betartására kötelezettséget vállalok.

Tudomásul veszem, hogy kezelésembe kizárólag az alábbi adatok tartoznak:

1. …….

2. …….

3. …….., stb.

Dátum: ……..

a nyilatkozatot adó munkavállaló aláírása

Kapja: 1. Munkavállaló
2. Informatikus
3. Személyzeti irattár - helyben

19.5. Jogosultság igénylő lap

Iktatószám: ……./20…...

Név:	
Beosztás/jogállás:	
Munkakör:	
Szervezeti egység:	
Szervezeti egység vezetője:	

- ☐ Új jogosultság/eszköz igénylése
- ☐ Meglévő jogosultság(ok) törlése
- ☐ Már meglévő jogosultság(ok) módosítása

A kívánt eljárást kérjük X-el jelölni!

Igényelt jogosultságok/eszközök[3]	**Dátum-tól**	**Igénylés (X) / Törlés (T) / Felfüggesztés (F)**

Megjegyzés:

Dátum: szervezeti egység vezetője

igénylő

Engedélyezte:

Igazgató

Dátum: aláírás

Informatikus

Dátum: aláírás

[3] Hálózati belépés, Levelezés, / Belépőkrátya / Belépőkártyához kód és jelszó / TAKARNET program telepítése ArcMap 102 térképprogram telepítése / TIR-hez belépési jelszó / Belső vezetékes telefon és kód / Fénymásolóhoz kód (scan) / E-mail fiók / H és B meghajtókhoz való hozzáférés / Hálózati mappa (könyvtár) hozzáférés / Eszköz hozzáférés / Eszköz áthelyezése / Eszköz használati igény / Alkalmazás (szoftver) telepítés, frissítés, hozzáférés / Alkalmazáshoz (szoftverhez) való jogosultság / Adathordozó eszközök csatlakoztatása (jog)
Egyéb igény .