NEMZETI SZAKKÉPZÉSI ÉS FELNŐTTKÉPZÉSI HIVATAL

NEMZETI SZAKKÉPZÉSI ÉS FELNŐTTKÉPZÉSI HIVATAL INFORMATIKAI BIZTONSÁGI SZABÁLYZATÁNAK KIVONATA FELHASZNÁLÓK RÉSZÉRE

Ver. 1.0

2021. szeptember 20.

Készítette: Informatikai és Működtetési Főosztály

Tartalom

A kivonat célja

Jelen kivonat célja a Hivatal munkatársainak támogatása arra vonatkozóan, hogy a Nemzeti Szakképzési és Felnőttképzési Hivatal (a továbbiakban: Hivatal) Informatikai Biztonsági Szabályzatáról szóló 2021/26. számú elnöki utasításban foglaltakat ezen összefoglaló keretein belül megismerhessék, munkájuk során a megismertek szerint járjanak el.

A szabályzat célja

Az Informatikai Biztonsági Szabályzat (a továbbiakban: IBSZ) célja, hogy **a Hivatal működése és szolgáltatásai során biztosítsa a Hivatal által kezelt, feldolgozott, továbbított, valamint tárolt adatok kockázattal arányos védelmét (bizalmasság, sértetlenség és rendelkezésre állás) a felmerülő veszélyforrások ellen.**

A szabályzat személyi hatálya kiterjed a Hivatalnál bármely munkavégzésre irányuló jogviszonyban (munkaviszonyban) álló természetes személyre, azzal a megjegyzéssel, hogy a Hivatal által használt elektronikus információs rendszerek külső üzemeltetőire, fejlesztőire, szerződéses úton történő egyéb alkalmazóira e szabályzat rendelkezéseinek megtartását szerződésben, vagy egyéb megállapodásban rögzíteni kell.

A személyi hatály továbbá Hivatal informatikai rendszerével, szolgáltatásaival megbízatás, egyéb szerződés alapján kapcsolatba kerülő természetes és jogi személyekre, jogi személyiséggel nem rendelkező szervezetekre, a velük kötött szerződésben rögzített mértékben, illetve a titoktartási nyilatkozat alapján terjed ki.

A szabályzat elfogadása és kihirdetése az elnök feladata.

A szabályzat betartásának ellenőrzése az informatikai biztonsági felelős feladata, melyben közreműködnek az informatikai biztonsági megbízott(tak), szervezeti egységek, munkacsoportok, valamint az elektronikus információs rendszer üzemeltetéséért, fejlesztéséért felelős informatikai szervezeti egységek vezetői.

Az IBSZ többek között a következőket szabályozza részletesen:

I. A biztonsági események és incidensek kezelése

A **Biztonsági esemény** minden olyan 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.

A **Biztonsági esemény kezelése** az elektronikus információs rendszerben bekövetkezett biztonsági esemény dokumentálása, következményeinek felszámolása, a bekövetkezés okainak és felelőseinek megállapítása, és a hasonló biztonsági események jövőbeni előfordulásának megakadályozása érdekében végzett tervszerű tevékenység

II. Az emberi erőforrások biztonsága

II.1 A munkaviszony kezdetét megelőzően

Minden informatikai munkakört elektronikus információbiztonsági kategóriákba kell sorolni, az alábbi szempontok szerint:

- bármely elektronikus információs rendszerben privilegizált jogosultsággal rendelkezik, vagy
- egyéb szempontok alapján kiemelt kockázatot hordoz magában.

II.2 A munkaviszony kezdetekor fellépő kötelezettségek

A jog-, munka-, szerződéses viszonyban álló munkatársak a **felhasználói felelősségvállalási nyilatkozat** aláírásával elismerik, hogy az Informatikai Biztonsági Szabályzatban meghatározott biztonsági elvárásoknak, előírásoknak eleget tesznek.

A nyilatkozat mindenkor aktuális verziójának a felhasználóval történő aláíratása és adminisztrálása a munkatárs szervezeti egység vezetőjének a feladata és felelőssége.

A belépő munkatárs munkavégzéséhez szükséges infokommunikációs eszközöket és jogosultságokat a munkatárs szervezeti egységének vezetője igényli meg. Az igényt papír alapon az IBSZ 8. és 9. függeléke szerinti űrlapokon kell benyújtani. Az igény a papír alapú kérelem tartalmával megegyező adattartalommal elektronikusan is beküldhető a HelpDesk szolgálatra e-mail-ben.

II.3 A munkaviszony fennállása során

Az IBSZ-ben foglalt előírások tudatosítása érdekében a felhasználók informatikai oktatását belépéskor, és utána rendszeresen meg kell tartani. A képzés tartalmának és felépítésének összhangban kell lennie az új belépő által betöltendő feladatkörrel. Az oktatásokon a felhasználókat fel kell készíteni a számukra kijelölt szerepkörökkel és felelősségekkel összhangban a lehetséges fenyegetések felismerésére, az

elektronikus információs rendszerek informatikai biztonsági szabályoknak megfelelő használatára, az informatikai biztonsági események és incidensek szabályszerű kezelésére.

Az oktatáson való részvétel minden felhasználó számára kötelező, aki a munkavégzése során informatikai rendszert használ. A részvételért a felhasználó szervezeti egységének vezetője a felelős.

A Hivatali információs rendszerrel, a rendszer üzemeltetésével vagy a rendszer elhelyezésére szolgáló objektummal kapcsolatban álló felhasználóknak kötelessége jelenteni olyan nem kívánt vagy nem várt egyedi vagy sorozatos informatikai biztonsági eseményeket, amelyek nagy valószínűséggel veszélyeztetik a Hivatali tevékenységet és fenyegetik az informatikai biztonságot. A bejelentést a Helpdesk bejelentő felületre e-mail-ben köteles a felhasználó elküldeni. Ennek akadályoztatása esetén, telefonon vagy személyesen kell elvégezni a bejelentést.

Az elektronikus levelezésre vonatkozó részletes szabályokat a Hivatal Levelezési szabályzata tartalmazza.

Internetes böngészésre vonatkozó szabályok:

Az internet szolgáltatás minőségének szinten tartása és a hivatali érdekek biztosítása céljából az informatikai feladatok ellátásáért felelős főosztályvezető korlátozhatja:

- egyes fájl típusok letöltését, különösen: *.mov, *.mp3, *.wav, *exe;
- a jogszabályi és társadalmi normákat sértő oldalak elérhetőségét; és
- a maximális fájl letöltési méretet.

A felhasználók csak az informatikai feladatokért felelős főosztályvezető által meghatározott internet kijáratokon keresztül csatlakozhatnak az internethez, bármely egyéb módon történő internet elérés létesítése a magas kockázat miatt tilos. Külön engedéllyel megoldható hivatali készüléken wifin keresztül elérni a világhálót. Ezt e-mail-ben kell jelezni az NSZFH HelpDesk-re.

Az informatikai rendszer biztonsága érdekében a rendszer által folyamatosan naplózásra kerülnek az internet felhasználók által meglátogatott oldalak, ezen információk illetéktelenek által nem ismerhetők meg, azokat az adatvédelmi előírásoknak megfelelően kell kezelni.

Kizárólag a munkavégzéshez, szakmai tájékozottság növeléséhez szükséges oldalak látogathatók, melynek során figyelemmel kell lenni a Hivatal érdekeire, továbbá a jogszabályokra, valamint a belső szabályok által meghatározott előírásokra.

Az internetről csak a munkavégzéshez szükséges adatállományok tölthetők le; az internetről letöltött fájlt a hálózatra csatlakoztatott gépre, vagy a szerverre való telepítés előtt egyéni vírusellenőrzés alá kell vetni. Amennyiben a felhasználó a vírusellenőrzést nem tudja lefolytatni, köteles értesíteni az NSZFH HelpDesk-et.

A jelszókezelés általános szabályai:

- A felhasználó a számítógépre csak saját nevében és jelszavával léphet be, és az alkalmazásokat csak saját nevében használhatja.
- A jelszavak nem hozhatók nyilvánosságra és nem oszthatók meg senkivel.
- A jelszavak bizalmasságának megőrzéséért a felhasználó személyesen felel.
- Ha a felhasználónak a legkisebb gyanúja is felmerül a jelszó biztonságának integritása felől, azt köteles azonnal megváltoztatni és gyanújáról az informatikai biztonsági felelőst értesíteni.
- Más felhasználó azonosítóját átmeneti jelleggel sem szabad használni.
- A felhasználó köteles a jelszavát az előírt gyakorisággal és módon megváltoztatni.
- A felhasználónak az alapértelmezett jelszavakat az első belépés után kötelessége azonnal megváltoztatni.

A felhasználó jogai és kötelességei:

- A felhasználó azonosítójával és jelszavával az informatikai rendszerben végrehajtott műveletekért személyesen felel.
- A számára kiosztott jogosultságokkal a rendszer erőforrásait és szolgáltatásait (hálózati tárhelyek, hálózati nyomtatás stb.) használhatja.
- A nem mobil informatikai eszközök áthelyezése és/vagy leltárkörzet szerinti másik helyiségbe való áthelyezése a felhasználó által nem végezhető.
- Az informatikai eszközöket és szoftvereket rendeltetésszerűen kell használni.
- A felhasználó felelős a személyes használatra kiadott eszközök rendeltetésszerű használatáért és őrzéséért.
- Felelős a rábízott informatikai berendezések állapotának, állagának megőrzéséért.
- Az informatikai eszközöket a munka befejeztével, illetve a munkaidő végeztével áramtalanítani kell, amennyiben azok folyamatos üzemben tartása nem indokolt.
- Hetente egyszer mindenképpen köteles a felhasználó a számítógépét újra indítania.
- Az informatikával kapcsolatos igényeit (kivéve a fogyóeszközök) a szervezeti egység vezetője felé kell jeleznie, aki az igény jogosságát elbírálja.
- A számítógéptől való hosszabb (több mint 5 perc) távollét esetén a felhasználó köteles a munkaállomást, vagy mobil számítástechnikai eszközt zárolni, vagy kilépni a rendszerből.
- A számítógépekre szoftver telepítése önhatalmúlag szigorúan tilos, kizárólag informatikus részére engedélyezett.
- A saját használatra átvett számítógép rendszerszintű beállításainak módosítása (ebbe nem értendők bele az irodai programok felhasználói beállításai), felhasználó számára nem engedélyezett.
- Az informatikai hálózat fizikai megbontása, a számítástechnikai eszközök lecsatlakoztatása (kivételt képeznek a hordozható eszközök), illetve bármilyen számítástechnikai eszköz hálózatra történő fizikai csatlakoztatása és/vagy beszerelése tilos.

- A hivatali adatok nem hivatali céllal történő kijuttatása, magán célú felhasználása, vagy harmadik személy rendelkezésére bocsátása tilos.
- A munkaállomást illetéktelen személy (pl. ügyfél) jelenléte mellett a felhasználó nem hagyhatja felügyelet nélkül.
- Az informatikai rendszerek használata csak hivatalos célokra engedélyezett;
- A használt informatikai eszközök kezelésével kapcsolatos felhasználói és biztonsági ismereteket el kell sajátítani.
- Az informatikai rendszerekben csak azokat a feladatokat szabad elvégezni, amelyek a felhasználó vagy üzemeltető munkájának ellátásához szükségesek, függetlenül attól, hogy a rendszer esetleg ennél szélesebb körű tevékenységet enged meg.
- A Hivatal által rendszeresített biztonsági funkciókat (például automatikus képernyővédő-aktiválás) kikapcsolni, megkerülni tilos.
- A Hivatal eszközein csak a Hivatal által engedélyezett eszközöket és programokat szabad használni.
- Tartózkodni kell minden olyan tevékenységtől, amely az informatikai rendszerben a bizalmasság, sértetlenség vagy rendelkezésre állás sérülését okozhatja.

Felhasználók szerepe a vírusvédelemben:

- A felhasználókat meg kell ismertetni a kártékony kód felmerülésének esetében követendő előírásokkal, mivel aktív szerepet tölt be a tudatosság az előírt kártékony kódok elleni védelem alkalmazásában. Ha a felhasználók kellő odafigyelést tanúsítanak a vírusvédelemmel kapcsolatban, akkor a műszaki megoldásokkal együtt nagymértékben csökkenthető a kártevő programok okozta kockázat.
- A felhasználót tájékoztatni kell, hogy amennyiben a munkaállomás indítását követően az tapasztalható, hogy a vírusvédelmi program nem indult el (pl. ikonja nem látható), vagy ki van kapcsolva, akkor a munkavégzés megkezdése nem engedélyezett, az esetleges vírusfertőzésért a felhasználó felel. Ilyen esetben a munkaállomást le kell állítani, és értesíteni kell írásban a HelpDesket.
- Amennyiben a felhasználó a vírusvédelmi rendszer által generált riasztást kap, azt haladéktalanul jelentenie kell a HelpDesk felé.
- A hivatali belső hálózathoz nem (vagy régen) csatlakoztatott számítógépen (pl. notebook) a vírusvédelmi rendszer frissítése a felhasználó feladata és felelőssége. A belső hálózathoz vagy internethez nem csatlakoztatott munkaállomások esetén a vírusdefiníciós állományok frissítését a belső hálózathoz, vagy Internethez kapcsolódáskor el kell végezni a rendszernek automatikusan. A manuális frissítés elvégzésében a HelpDesk tud segítséget nyújtani.

Szoftverhasználati szabályok:

Kizárólag olyan szoftvereket és dokumentációkat szabad használni, amelyek megfelelnek a vonatkozó szerződésbeli, szerzői jogi vagy más jogszabályi elvárásoknak.

A számítógépeken csak és kizárólag az informatikai feladatok ellátásért, üzemeltetésért felelős szervezeti egység, valamint az erre jogosult külső felek munkatársai telepíthetnek, módosíthatnak, vagy távolíthatnak el bármilyen fajta szoftvert.

Távoli elérés biztonsági szabályai:

A Hivatal informatikai rendszerének távoli elérését a felhasználó – a rendszerek besorolásának függvényében – kizárólag az egyedi engedélyezési eljárás alapján, kétfaktoros autentikáció mellett, a szerződésben, az utasításokban meghatározott feltételekkel használhatja.

Nyomtatás és nyomtatáskezelés:

- Jelszavakat, hozzáférési kódokat és információkat tilos nyomtatásban megjeleníteni
- gondoskodni kell a kimeneti információ tartalmi ellenőrzéséről;
- gondoskodni kell arról, hogy a kimeneti információhoz történő fizikai és logikai hozzáférés kizárólag az arra jogosított személyekre korlátozódjon;
- gondoskodni kell arról, hogy a jogosult személyek időben megkapják az elkészült kimeneti információkat;
- biztosítani kell a kimeneti információk biztonságos tárolását;
- biztosítani kell, hogy a megsemmisítési eljárások során a kimeneti információk tartalma helyreállíthatatlanul megsemmisüljön.

II.4 Jogosultság változás egyes esetei

A munkavégzés várhatóan 1 hónapnál hosszabb szünetelése – GYES, GYED, hosszantartó betegség stb. – esetén a felhasználó jogosultságait a távollét időszakára le kell tiltani – de törölni nem szabad –, mely a munkatárs szervezeti egységének vezetőjének a felelőssége.

Kilépő dolgozó szervezeti egységének vezetője gondoskodik a jogosultság visszavonásáról. Másik feladatkörbe történő áthelyezés esetén, a felhasználó jogosultságait vissza kell vonni, majd az új szervezeti egység vezetőjének szükséges igényelni a szükséges jogosultságok megadását.

Hozzáférési jogosultságok visszavonása:

Valamennyi munkaviszonyban vagy munkavégzésre irányuló egyéb jogviszonyban álló természetes személynek az információkhoz és információ feldolgozó eszközökhöz való hozzáférési jogosultságát fel kell függeszteni, amikor alkalmazásuk megszűnik, szerződésük, illetve megállapodásuk lejár. Ha az érintett részéről fennállhat az ügymenetet vagy elektronikus információbiztonságot sértő magatartás veszélye, a jogosultságokat még az érintett tájékoztatását megelőzően vissza kell vonni!

A jogosultságok visszavonását az érintett felhasználó szervezeti egységének vezetője kezdeményezi, a végrehajtása az adott informatikai rendszer üzemeltetésért felelős szervezeti egység munkatársainak feladata.

Infokommunikációs eszközök visszaszolgáltatása:

Valamennyi felhasználónak vissza kell szolgáltatnia a Hivatal számára valamennyi használatra átvett infokommunikációs eszközt, amikor alkalmazásuk, szerződésük, illetve megállapodásuk lejár, illetve megszűnik.

Amennyiben nem kerül visszaszolgáltatásra az eszköz, abban az esetben ezt a szervezeti egység vezetőjének jeleznie kell az adott eszköz üzemeltetéséért felelős vezető felé, aki a szükséges intézkedést kezdeményezi.

II.5 Külső felekkel kötött megállapodások

Az informatikai rendszerekkel, illetve a szervezet által kezelt adatokkal kapcsolatba kerülő, vagy az elektronikus információbiztonságra közvetlen módon hatást gyakorló külső felekkel olyan írásbeli megállapodást kell kötni, amely tartalmaz vagy utal minden olyan elektronikus információbiztonsági követelményre, mely az IBSZ-ben vagy egyéb dokumentumban szabályozásra került. Az együttműködés során rendelkezésre bocsátott üzleti titkok és bizalmas információk megőrzésének szabályait és módját titoktartási nyilatkozatban kell rögzíteni.

A külső beszállítók és szolgáltatók számára a Hivatalon belüli kapcsolattartó igényli meg, valamint felügyeli a szükséges jogosultságokat, szükség esetén a visszavonásukat kezdeményezi.

A külső beszállítók és szolgáltatók hozzáférését a hozzáférés indokának megszűnte után, illetve a szerződés lejártakor azonnal meg kell szüntetni.

III. Rendszer és szolgáltatás beszerzés

A rendszer és szolgáltatás beszerzések szabályozva vannak az IBSZ-ben.

IV. Alkalmazásfejlesztés folyamata

Az illetékes szervezeti egység vezetője az alkalmazásfejlesztésért felelős vezetőnek jelzi a fejlesztési igényt a megfelelő dokumentumok kitöltésével. Az illetékes szervezeti egység vezetőjének feladatai ezen a téren:

- a felmerült igény összegyűjtése és jóváhagyása, amennyiben szakmailag helytálló;
- a felmerült igényre elkészített igénybejelentő dokumentum jóváhagyása és továbbítása az alkalmazásfejlesztésért felelős vezetőnek.

Az alkalmazásfejlesztésért felelős vezető dönt az igénybejelentő dokumentum elfogadásáról vagy elutasításáról.

Elfogadás esetén az alkalmazásfejlesztésért felelős vezető eldönti, hogy ez belső fejlesztéssel megoldható, vagy külső fejlesztőt kell igénybe venni.

V. Adathordozók védelme

Az elektronikus információs rendszerekben és a szervezetnél használt adathordozóknak és mobil eszközöknek a bizalmassága, sértetlensége és rendelkezésre állása érdekében biztosítani kell az adathordozók és mobil eszközök megfelelő fizikai és logikai védelmét.

Az adathordozó eszközigényléseket indoklással együtt papír alapon az IBSZ 9. függeléke szerinti űrlapokon kell benyújtani. Az igény a papír alapú kérelem tartalmával megegyező adattartalommal elektronikusan is beküldhető a HelpDesk szolgálatra e-mail-ben.

Az igénylésnek tartalmaznia kell:

- az igénylő szervezeti egységet,
- használatba vevő nevét (kinek a részére történik az igénylés),
- igényelt eszköz típusát (laptop, okostelefon, tablet, adathordozó, egyéb),
- valamint indoklását.

V.1 Adathordozók használata

A Hivatalnál kizárólag a Hivatal tulajdonába tartozó adathordozók használata engedélyezett, saját tulajdonú adathordozók használata és a számítógépekhez vagy egyéb Hivatali eszközökhöz való csatlakoztatása szigorúan tilos.

Cserélhető adathordozók esetében az adathordozót átvevő (használó) személy felel az adathordozón lévő információk kitudódása és illetéktelen kézbe kerülése esetén az okozott károkért.

Az adathordozók kizárólag munkavégzés céljából használhatóak hivatal tevékenységek végzéséhez. A felhasználók munkájához nem kapcsolódó adatok tárolása, illetve az adathordozók magáncélú felhasználása nem engedélyezett.

A Hivatalon kívül történő eszközhasználat esetén az adathordozókon tárolt adatokat, dokumentumokat a lehető leghamarabb fel kell másolni a megfelelő hálózati meghajtóra, ezután az adathordozóról pedig törölni kell azokat.

Az adathordozók Hivatal telephelyein kívülre vitele esetére a következő eljárások vonatkoznak:

- Adathordozó csak engedéllyel vihető ki a Hivatal telephelyein kívülre, melyet a szervezeti egység vezető engedélyez;
- A telephelyen kívülre történő szállítás esetén az adathordozó biztonságáért a szállítást végző felel;
- Az adathordozón tárolt adatok biztonsági osztályához tartozó előírásokat minden esetben be kell tartani;

Az ismeretlen (nem egyértelműen beazonosítható) tulajdonosú adathordozók használata tilos. Ilyen esetben a talált adathordozót nem szabad a számítógépekhez csatlakoztatni vagy mások számára továbbadni, ilyen esetben haladéktalanul értesíteni kell a HelpDesket.

V.2 Mobil eszközök használata

Hivatali munkavégzéshez kapcsolódó adatkezelésre saját tulajdonú mobil eszköz kizárólag eseti engedély alapján használható a Hivatalnál. Ebben az esetben a felhasználó felelőssége az eszközön tárolt adatok védelmének biztosítása.

A hivatali mobil eszközt átvevő (használó) személy felel az eszközön lévő információk kitudódása és illetéktelen kézbe kerülése esetén az okozott károkért.

A hivatali mobil eszközt kizárólag az eszközt átvevő hivatali munkatárs használhatja, azt nem adhatja át másnak használatra.

A szervezeten kívüli használat esetén a mobil eszközt nem lehet felügyelet nélkül hagyni, valamint látható helyen hagyni (otthoni munkavégzés esetén vagy szekrényben, vagy széfben kell tárolni). Amennyiben másképpen nem biztosítható az eszköz megfelelő védelme, a dolgozónak magával kell vinnie az eszközt.

Szabályos használatban informatikai eszközként használt hivatali mobil telefonon magán adat nem tárolható, magán informatikai elérésre nem használható. A magán adat sérüléséért – bizalmasság, sértetlenség, rendelkezésre állás – és az abból eredő kárért a Hivatal nem tartozik felelősséggel.

A mobil eszközök használata során ügyelni kell arra, hogy harmadik fél ne tekinthessen bele az eszköz megjelenítő felületébe.

A mobil eszközök képernyőjét zárolni kell használatukat követően.

Informatikai eszközként csak azok a mobil telefonok használhatók, amelyekkel a szabályozásban meghatározott követelmények teljesíthetők.

A mobiltelefonon be kell állítani az alábbiakban felsoroltak közül legalább egy, a felhasználót hitelesítő eszközt (szolgáltatást):

- jelszó,
- ujjlenyomat azonosítás,
- arcfelismerés vagy írisz felismerés,
- PIN kód,

E-mail és más rendszerhozzáférés csak a fentiekben meghatározott hitelesítési eszközök alkalmazásával lehetséges.

Hivatali adatot, dokumentumot a mobiltelefonon – amennyiben az eszköz támogatja – titkosítva kell tárolni.

Biztonsági esemény kezelése:

Haladéktalanul jelenteni kell az informatikai feladatok ellátásáért felelős belső szervezeti egység felé a következő eseményeket:

- a mobiltelefon elvesztése, eltulajdonítása;
- a mobiltelefon illetéktelen használata, illetéktelen hozzáférés.

Illetéktelen hozzáférésnek minősül az is, ha a telefont javításra adatokkal, hozzáférési lehetőséggel adják át.

V.3 Adathordozók biztonságos tárolása

A nem beépített adathordozókat a napi munkavégzés befejezését követően – amennyiben lehetséges – le kell választani a számítógépekről és elzárva kell tartani (páncélszekrényben, széfben, zárt szekrényben vagy fiókban stb.), erről az adathordozó használójának kell gondoskodnia. Ügyelni kell arra, hogy ilyen adathordozó semmi esetre se maradjon szem előtt (például asztalon hagyva).

A tárolás során a gyártói előírásokat be kell tartani, és a gyártó által előírt megfelelő környezeti paramétereket biztosítani kell.

Amennyiben az adathordozókon levő jelölések valamilyen okból kifolyólag már nem olvashatóak (például lekopott vagy megrongálódott a jelölés), vagy esetleg a megjelölést egyéb okból változtatni szükséges (például az adathordozó terjesztési korlátozásának megváltozása miatt), az adathordozó használójának ezt a tényt jelentenie kell az Informatikai feladatok ellátásáért felelős szervezeti egység felé, melynek a feladatra kijelölt munkatársai a szükséges intézkedésekről gondoskodnak.

VI. Hozzáférés-felügyelet

VI.1 Azonosítás

Az elektronikus információs rendszereknek minden belső és külső felhasználót egyedileg kell azonosítaniuk annak érdekében, hogy:

- minden, egy adott időpontban végzett tevékenység összerendelhető legyen egy természetes személlyel;
- az összerendelés egyértelmű, megváltoztathatatlan, később is visszakereshető legyen.

VI.2 Hitelesítés

A Hivatal tulajdonában vagy használatában lévő valamennyi elektronikus információs rendszer esetében az azonosítást legalább egy hitelesítő mechanizmussal is ki kell egészíteni. A hitelesítés mechanizmus általános módszere a felhasználói azonosítóhoz tartozó jelszó alkalmazása.

Felhasználói fiókok jelszavai:

A jelszavakkal kapcsolatos minimális elvárások – melyeknél csak szigorúbbakat szabad alkalmazni – minden hivatalon belül használt rendszer esetében:

- a jelszavak hossza legalább 12 karakter kell, hogy legyen;
- sem részben, sem egészében nem tartalmazhatja a fiókazonosítót;
- az alább felsorolt karaktertípusok mindegyikéből legalább egyet-egyet tartalmaznia kell:
  - kisbetű (a..z)
  - nagybetű (A..Z)
  - számjegy (0..9)
- a jelszavakat legalább 90 naponként meg kell változtatni;
- az új jelszónak legalább egy karakterében különböznie kell a legutóbb használt 10 bármelyikétől;
- amennyiben az informatikai rendszer, illetve az alkalmazás lehetővé teszi, a jelszavak képzésének szabályait szoftver útján ki kell kényszeríteni.

A kezdeti jelszót az első belépéskor meg kell változtatni, továbbá a jelszavak bizalmasságát minden felhasználónak meg kell őriznie, azokat más személy tudomására hozni szigorúan tilos! A jelszavakat azok kompromittálódása – vagy annak gyanúja – esetén haladéktalanul meg kell változtatni, vagy a hozzá kapcsolódó fiókot le kell tiltatni.

VI.3 Engedélyezés

A felhasználók csak a számukra kijelölt feladatok végrehajtásához szükséges és elégséges jogosultságokat kaphatják meg az információkhoz és a rendszer erőforrásaihoz való logikai hozzáférés során.

VI.4 Felügyelet

Hat sikertelen bejelentkezési kísérletet követően az elektronikus információs rendszer automatikusan zárolja magát – legyen az felhasználói vagy privilegizált, hagyományos vagy technikai – legalább 15 perc időtartamra. A zárolást az informatikai feladatok ellátásáért, üzemeltetésért felelős szervezeti egység munkatársai oldhatják fel.

VII. Rendszerüzemeltetés

Az Hivatalban lévő informatikai rendszerek üzemeltetését az Informatikai Osztály végzi szabályozott keretek között.