

**A Magyar Államkincstár Információ Biztonsági Szabályzatáról szóló 6/2025. számú Elnöki
körlevél részeként a Külső féllel történő együttműködés szabályzata (7. függelék)
1. és 2. számú mellékletei**

1. sz. melléklet

Informatikai biztonsági követelményrendszer

1. A Kincstárral munkavégzés érdekében szerződéses jogviszonyban álló természetes és jogi személy, jogi személyiséggel nem rendelkező szervezet és alkalmazottja – ide nem értve a Kincstár foglalkoztatottjait – (a továbbiakban: Külső fél vagy Külső felhasználó) kötelezettséget vállal arra, hogy a Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény és a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről szóló 7/2024. (VI.24) MK rendelet előírásait ismeri és azokat jelen szerződés teljesítése során betartja.
2. A Külső fél a Kincstár Külső Felekre vonatkozó Informatikai Biztonsági Előírásait (2. sz. melléklet) átvette, megismerte és azokat magára kötelező érvényűnek tekinti. A Külső fél vállalja, hogy általa a tevékenység végzésére felkért, ill. megbízott, a teljesítésben közreműködő összes személlyel ezen előírásokat maradéktalanul betartatja. A vonatkozó jogszabályi rendelkezések, valamint a jelen követelményrendszer be nem tartása miatt okozott kárért a Külső fél teljes mértékben felel.
3. A Külső fél köteles minden, a szerződésben közreműködő – és informatikai rendszerhez hozzáférést igénylő feladatot ellátó –, a Külső fél alkalmazásában vagy megbízásában álló személy számára egyedi hozzáférési igényét jelezni a Kincstár részére, és köteles biztosítani, hogy az egyedi hozzáférési adatokat a közreműködők nem osztják meg a Külső fél más közreműködőivel. A Kincstár által kiadott hozzáférések kizárólag a feladat ellátására használhatók. A Kincstár jogosult indoklás nélkül bármilyen hozzáférést felfüggeszteni, visszavonni, módosítani.
4. A Külső fél – a jogosultságok visszavonása érdekében – köteles haladéktalanul tájékoztatni a Kincstár érintett munkatársait, amennyiben a közreműködő státuszában változás következik be, vagy bármilyen más okból már nem vesz részt a teljesítésben.
5. A Külső fél kötelezettséget vállal arra, hogy a közreműködőt érintő változásról azonnali írásbeli tájékoztatást nyújt a Kincstárnak, továbbá vállalja, hogy amennyiben a Kincstár az adott közreműködő személlyel szemben írásban megalapozott kifogással él, haladéktalanul gondoskodik annak megfelelő szakmai helyettesítéséről.
6. Amennyiben a Külső fél tevékenysége során az informatikai biztonsági szabályok megsértésének gyanúja merül fel, vagy a Külső fél informatikai biztonsági eseményben érintett – beleértve a Külső félnek a saját rendszereiben a Kincstár adatvagyonát érintő informatikai biztonsági eseményt is – köteles az esemény kivizsgálását teljes mértékben támogatni, minden adatot és információt biztosítani

- a Kincstár számára az esemény kivizsgálására, beleértve a Külső fél rendszerében bekövetkezett informatikai biztonsági esemény bejelentését is a Kincstár IBV-nek.
7. Amennyiben a Külső fél tevékenysége során a jelen szerződésben közreműködő személy(ek) kapcsán az informatikai biztonsági szabályok szándékos vagy súlyosan gondatlan megsértésének gyanúja merül fel, a Kincstár kérésére a Külső fél köteles az érintett közreműködő tevékenységét a teljesítésben felfüggeszteni.
 8. Amennyiben a Külső fél a tevékenysége során a Kincstáron kívül más adatkezelő vagy adatfeldolgozó szervezet számára is nyújt szolgáltatást, és/vagy a Kincstár információs vagyontárgyát saját rendszereiben (is) kezeli, köteles megfelelő műszaki és személyi feltételek mellett biztosítani a különböző adatállományok elkülönítését az adatok illetéktelenek általi hozzáféréseinek, megismerésének megakadályozása céljából, továbbá azt, hogy a fent jelzett szervezetek által kezelt adatok jogosulatlan összekapcsolására ne kerülhessen sor.
 9. A Kincstár jogosult a szerződés teljesítése folyamán a szerződésben foglalt feltételek betartását, valamint a Külső fél tevékenységét figyelemmel kísérni, ellenőrizni. Amennyiben a tevékenység jellege, illetve a kezelt adatok és információk kritikussága igényli, a Kincstár jogosult az informatikai biztonsági követelmények teljesülését audit formájában is vizsgálni a Külső félnél, melyben a külső fél együttműködésre kötelezett.
 10. A Külső fél kizárólag az informatikai üzemeltetésért felelős szervezeti egység (a továbbiakban: üzemeltető szervezeti egység) vezetőjének és az IBV együttes írásbeli jóváhagyását követően, kizárólag indokolt esetben csatlakozhat saját tulajdonú informatikai eszközzel a Kincstár infrastruktúrájához, amennyiben az eszközt az üzemeltető szervezeti egység vezetője által kijelölt személy ellenőrizte.
 11. A szerződés lejártakor a Külső fél köteles a részére a Kincstár által a szerződés teljesítéséhez rendelkezésre bocsátott vagyontárgyakat hiánytalanul visszaadni, a Kincstár működését, tevékenységét érintő adatokat, illetve információkat visszaállíthatatlanul törölni.

Külső Felekre vonatkozó Informatikai Biztonsági Előírások

Általános előírások

A Kincstárral szerződéses jogviszonyban álló Külső felek csak a Külső féllel kötött szerződésben meghatározott módon és a feladatok ellátásához szükséges mértékben és időtartamban kapcsolódhatnak a Kincstár belső hálózatára az IBV engedélyezését követően, az üzemeltető szervezeti egység vezetőjének felügyeletével.

Külső hálózatról csak biztonságos, titkosított csatornán keresztül és csak megfelelő hitelesítést követően lehet a Kincstár belső hálózatában működő számítógépre csatlakozni. A Kincstár jogszabály által védett adatait kezelő, produktív rendszereihez külső hálózatról történő csatlakozás – alapesetben – Külső fél részére nem engedélyezett.

Minden Külső felhasználónak fel kell tudnia ismerni – a saját tevékenységének körében, – a különböző biztonságot veszélyeztető eseményeket, és ismerniük kell annak bejelentésére vonatkozó eljárási rendet.

A Külső fél által végzett szoftverfejlesztés, illetve karbantartás során folyamatosan figyelemmel kell kísérni a szerződéses feltételek teljesülését, és a biztonsági követelmények betartását, amelyet a Kincstár bármikor ellenőrizhet.

Külső felhasználók kizárólag az üzemeltető szervezeti egység vezetőjének és az IBV együttes jóváhagyásával csatlakozhatnak saját tulajdonú informatikai eszközökkel a Kincstár infrastruktúrájához, amennyiben az eszközt a kijelölt személy ellenőrizte.

Az üzemeltetési szoftverek biztonsága, ellenőrzése tekintetében az üzemeltetési rendszerben történő frissítéseket csak az üzemeltető szervezeti egység vezetőjének a felhatalmazásával, az általa kijelölt személy végezheti.

A munkavégzéshez szükséges munkaállomást és az ehhez tartozó szoftver komponenseket, biztonsági beállításokat és a lokális hálózatra történő csatlakozást a Kincstár biztosítja a Külső felhasználó részére. Alapértelmezés szerint a munkaállomás biztosításával a munkaállomás a Kincstár tartományába beléptetésre kerül, a felhasználói fiókkal a hálózati alapszolgáltatás és a munkavégzés tárgyát képező alkalmazás érhető el. Az ettől eltérő igényeket (saját munkaállomás, notebook, távoli elérés, internet, kincstári levelező rendszer, hálózati könyvtár használata, stb.) az üzemeltető szervezeti egység vezetője és az IBV bírálja el.

Abban az esetben, ha a saját munkaállomás, notebook használata engedélyezésre került, úgy az érintett eszközre a Kincstár által biztosított szoftverkomponenseket kell telepíteni (operációs rendszer, alkalmazások, kártékony kód elleni védelem, stb.), melyeket a megbízás végén el kell távolítani. Ennek a végrehajtását a kijelölt személy (Kincstár foglalkoztatott) végzi el.

A Kincstár hálózatához csatlakoztatott munkaállomásokra – alapesetben – érvényes az USB porton keresztüli adatmásolás tiltása.

Külső felhasználó jogosultságainak kezelése

1. Külső felhasználó részére csak ideiglenes jogosultság adható.
2. Külső felhasználó részére csak abban az esetben adható ideiglenes jogosultság, amennyiben a külső felhasználó, vagy a munkáltatója szerződéses jogviszonyban (ide értve a garanciális időszak időtartamát is) áll a Kincstárral és rendelkezik aláírt titoktartási nyilatkozattal. A jogosultság biztosításához a szerződő félnek a cég szintű titoktartás nyilatkozata nem elegendő, személyre szóló titoktartási nyilatkozat kitöltése szükséges a külső felhasználó személy részéről.

3. Külső felhasználó részére jogosultságot a szerződést kezdeményező szervezeti egység vezetője igényelhet. A jogosultság igénylésének folyamata megegyezik az új hozzáférési jogosultság igénylésének folyamatával. Az igényléskor az ideiglenes hozzáférési jogosultság érvényességének idejét kötelezően meg kell adni.
4. Az ideiglenes jogosultság érvényessége a jogosultságigénylésben megjelölt időtartamra, de legfeljebb a Külső felhasználó vagy szervezet Kincstárral kötött szerződése hatályának (ideértve a garanciális időszakot is) lejártáig terjedő időre szólhat, azonban nem haladhatja meg a 6 hónapot. Amennyiben a hozzáférés lejáratát követően is szükség van a hozzáférés további biztosítására, akkor a hosszabbítást a szerződéskötést kezdeményező szervezeti egység vezetője jogosult igényelni jelen fejezet 3. pontjában leírtaknak megfelelően.

Felhasználói jelszavak gondozására vonatkozó követelmények

1. Az informatikai eszközök és szolgáltatások tekintetében jelszavak védik a Külső felhasználó informatikai személyazonosságát, azaz minden olyan tevékenységet, amelyet a felhasználó valósít meg:
 - a. az informatikai hálózatban,
 - b. az alkalmazói rendszerekben,
 - c. a munkaállomásán,
 - d. az elektronikus levelezésével és
 - e. az interneten.
2. A felhasználói név és a hozzá tartozó jelszó birtokában az informatikai rendszerekben végrehajtott minden művelet úgy jelenik meg, mintha a felhasználói névhez tartozó Külső felhasználó hajtotta volna végre. Ezért a Külső felhasználó védelme érdekében is szükséges, hogy a jelszóválasztással és jelszógondozással kapcsolatos alábbi szabályok betartásra kerüljenek.
3. A Külső felhasználók feladata és felelőssége, hogy a munkaállomásra történő belépéshez:
 - a. a jelszóválasztás során megfelelő minőségű jelszavakat válasszanak;
 - b. a választott személyes jelszavaikat titokban tartsák, azt mással meg nem oszthatják;
 - c. a választott jelszavak ne kerüljenek feljegyzésre (kivéve a felhasználó által használt biztonságos elektronikus jelszószóf alkalmazásban) és ne legyenek bármilyen más módon illetéktelenek számára hozzáférhetők.
4. A jelszóválasztással kapcsolatos követelmények:
 - a. alapesetben legalább 12 karakter hosszú jelszót, privilegizált felhasználói fiókhoz legalább 20 karakter hosszú jelszót kell választani,
 - b. a jelszóban nem célszerű az ékezetes betűk használata és kerülni kell a „0”, „z” és az „”, „y” billentyűzetenkénti felcserélődése miatt adódó bizonytalanságot,
 - c. a jelszó tartalmazzon legalább egy kis- és nagybetűt, egy számot és speciális karaktert (pl. „+”, „!”, „&”),
 - d. tilos jelszóként a jelszó tulajdonosával kapcsolatba hozható vagy ismert szót, kifejezést választani,
 - e. tilos az informatikai rendszerben ismert parancsot vagy alkalmazás nevet jelszóként használni,
 - f. a jelszó nem lehet azonos a felhasználói azonosítóval,
 - g. minden új jelszó kialakításánál törekedni kell arra, hogy szerkezetében ne hasonlítson az előző, lecserélendő jelszóra.
5. Az egyes alkalmazói rendszerek jelszavait illetően az adott rendszerre vonatkozó szabályozás az irányadó.

6. 5 db egymás utáni sikertelen bejelentkezési kísérlet után a Külső felhasználó azonosítója zárolásra kerül.
7. A jelszógondozással kapcsolatos szabályok:
 - a. A jelszó más számára történő felfedése, kompromittálódása vagy ennek valószínűsíthetősége esetén a Külső felhasználó köteles azt haladéktalanul megváltoztatni,
 - b. amennyiben a Külső felhasználó a jelszavát elfelejtette, illetve a felhasználói azonosítója zárolásra kerül, akkor a szerződéskötést kezdeményező szervezeti egység vezetője tud számára új jelszót igényelni az értelmező rendelkezések pontban megjelölt e-mail címre tett bejelentés útján,
 - c. a Külső felhasználók nem adhatják ki jelszavaikat kollégáiknak,
 - d. a rendszergazda által beállított jelszót az első bejelentkezés alkalmával meg kell változtatni,
 - e. a felhasználói jelszavakat legalább 30 naponta meg kell változtatni, minimális élettartama 24 óra és legalább három generációig visszamenőleg nem lehet azonos jelszót megadni, azaz három egymás után következő jelszó nem lehet azonos,
 - f. tilos a jelszavakat internetes böngészőben menteni.
 - g. tilos a Külső felhasználóknak más felhasználók jelszavainak megszerzésére irányuló magatartást tanúsítaniuk

Adattárolás, adatvédelem

A Kincstár hálózatában történő munkavégzés során az érintett szervezeti egység közös könyvtárához a feladatvégrehajtás érdekében szükséges mértékig a Külső felhasználók hozzáférhetnek, mely hozzáférési jogosultságokat a könyvtár létrehozását kezdeményező szervezeti egység vezetője határoz meg. A jogosultságokat a szervezeti egység vezetője állítja be, vagy igényli meg. A közös könyvtárakban a Külső felhasználó csak a munkavégzéssel kapcsolatos adatokat tárolhatja.

A Kincstár hálózatában történő munkavégzés során a Külső felhasználók a Kincstárban végzett feladataikkal kapcsolatos adataikat az erre a célra kijelölt központi tárhelyen kötelesek tárolni, illetve oda kötelesek menteni a dokumentumaikat.

A Külső felhasználó saját, illetve a Külső fél tulajdonban lévő cserélhető adathordozó alapesetben nem, indokolt esetben a szerződéskötést kezdeményező szervezeti egység vezetőjének jóváhagyása, nyilvántartása és az IBV előzetes engedélye mellett használható. A nemzeti kifizető ügynökségi folyamatban érintett számítógépeken saját tulajdonú cserélhető adathordozó nem használható.

Magáncélú CD/DVD írás nem megengedett.

A Kincstár tulajdonában lévő cserélhető adathordozók használatát a feladatköri/munkaköri feladatoktól függően a szerződéskötést kezdeményező szervezeti egység vezetők engedélyezhetik a Külső felhasználóknak.

Cserélhető adathordozóról munkaállomást indítani tilos.

A munkavégzéssel kapcsolatos adatok kivitele, kiküldése a Kincstárból csak a szerződéskötést kezdeményező szervezeti egység vezetője által jóváhagyva az adatok pontos listájának dokumentálása és indoklása mellett lehetséges,

Érzékeny, nem nyilvános adatot tartalmazó adathordozó kivitele esetén minden esetben alkalmazni kell a Kincstár előírásainak megfelelő kriptográfiai eszközzel történő titkosítást.

A Kincstáron kívülre vitt adathordozók nem hagyhatók felügyelet nélkül (még zárt autóban sem). Az adathordozót kézipoggyászban, rejtett módon kell szállítani.

A gyártók berendezés védelmi utasításait kell mindenkor figyelembe venni, például megvalósítani az erős mágneses mezőnek való kitétel elleni védekezést,

Internet használat, elektronikus levelezés

Az internet biztonságos használata érdekében a Kincstár a következő alapelveket mondja ki, melyeket a Külső fél tudomásul vesz és a szabályokat betartja:

1. Az internetet a Külső felhasználók elsősorban feladatkörükből/munkakörükből adódó feladataik elvégzéséhez, mint szolgáltatást használhatják, betartva a vonatkozó szabályokat, utasításokat. Ezen szolgáltatás minden egyéb célú használata során az esetlegesen bekövetkezett károkért a felhasználó teljes felelősséggel tartozik.
2. Amennyiben a központi vírusvédelmi rendszer nem üzemel, az üzemeltető szervezeti egység vezetője által kijelölt személy a felhasználók egyidejű értesítése mellett az internet elérés szolgáltatást automatikusan felfüggeszti.
3. Az üzemeltető szervezeti egység vezetője és az IBV jogosultak meghatározni azoknak az információknak, tartalmaknak a körét, amelyek az internet használata, a hozzáférés során korlátozhatók, valamint jogosultak az internet használat ellenőrzésére.
4. Hálózati munkaadások az internethez kizárólag a Kincstár hivatalos internet kijáratán (központi tűzfalán) keresztül csatlakozhatnak.
5. A Kincstár hálózatához csatlakoztatott munkaadáson modemes vagy vezeték nélküli hálózaton kommunikáció nem folytatható.
6. Kincstár hálózatát vezeték nélküli eszközzel, vagy bármilyen más, a Kincstár felügyelete alá nem tartozó módon és eszközzel megosztani tilos.
7. A Külső felhasználó teljes felelősséggel tartozik a rendszergazdák által beállított Web-böngésző biztonsági paraméterek (cookie-k, a JavaScriptek, JVM-ek, ActiveX környezetek, plug-in-ek, jelszó megjegyzés tiltás beállításai) megváltoztatására visszavezethető, bekövetkezett károk tekintetében.
8. Az internetről történő letöltés előtt ellenőrizni kell a munkaadáson futó vírusvédelmi program futását és naprakészségét (a Windows tálca jobb oldalán található vírusvédelmi program ikonja látszik, és nem mutat rendellenességet).
9. Futtatható állományok letöltése tilos.
10. A nem megbízható forrásból származó információk nem tekinthetők hitelesnek.
11. Tilos tudatosan kihasználni az Internet szolgáltatást biztosító rendszerekben esetlegesen előforduló szoftver hibákat, védelmi hiányosságokat.
12. Fórumok és Kincstáron kívüli levelezőlisták használatát kerülni kell, legfeljebb a munkavégzés céljából, olvasásra szabad használni azokat, valamint a Kincstár által biztosított e-mail címmel beregisztrálva tilos fórum-bejegyzéseket tenni.
13. A Kincstár által kezelt adatok, illetve a Kincstár tevékenységére vonatkozó információk nem tölthetők fel felhő szolgáltatásokba és web-es tárhelyre (Dropbox, Google Drive, stb.), illetve nem továbbítható végpont-végpont közti kapcsolaton keresztül (pl. Facebook Messenger, Skype, Torrent, stb.).
14. Interneten található proxy szerver használata tilos.

Az elektronikus levelezés biztonságos használata érdekében a Kincstár a következő alapelveket mondja ki, melyeket a Külső fél tudomásul vesz és a szabályokat betartja::

1. A Kincstár elektronikus levelezés szolgáltatását a Külső felhasználók csak a szerződés teljesítése érdekében szükséges feladataik elvégzéséhez használhatják. Vonatkozó szabályok szándékos megszegése miatt bekövetkező károkért a Külső felhasználó teljes felelősséggel tartozik.

2. Az üzemeltető szervezeti egység vezetője és az IBV jogosultak meghatározni azoknak az információknak a körét, amelyeknek elektronikus levelezés útján történő forgalmazása korlátozható.
3. A Kincstár által biztosított, a felhasználók nevét tartalmazó, illetve a funkcionális e-mail címek hivatalos e-mail címek, csak a Kincstár tevékenységi körébe tartozó feladatok elvégzéséhez használhatóak.
4. A Külső felhasználóknak a Kincstár által biztosított e-mail címükön kívül más elektronikus levelezési szolgáltató rendszert (például gmail, freemail, hotmail, citromail, stb.) szerződéses tevékenységet érintő ügyekre használni tilos.
5. Tilos tudatosan kihasználni az esetlegesen előforduló szoftver hibákat, védelmi hiányosságokat.
6. A kérésre, gyanús e-mail üzeneteket, SPAM leveleket jelezni és a HelpDesknek (hibabejelentes@allamkincstar.gov.hu) mellékletként csatolva továbbítani kell, SPAM tárggyal. Az ismeretlen forrásból származó (esetenként tárgy megnevezése nélkül érkező) elektronikus leveleket a Külső felhasználók fenntartással kezeljék, ne bízzanak meg bennük. Ezek a levelek nagy valószínűséggel tartalmaznak/tartalmazhatnak az informatikai rendszerre és az adatvagyonra káros hatást kifejtő, rosszindulatú program-kódokat, ezért az ilyen e-maileket – bármilyen linkre kattintás és a mellékletek megnyitása nélkül, a HelpDesknek történő megküldést követően – törölni kell (a törölt elemek mappából is).
7. A véletlen félrecímzésből eredő, esetlegesen bizalmas jellegű adatok illetéktelen személy számára történő postázása megelőzése érdekében az elektronikus levelek elküldését megelőzően mindig ellenőrizni kell a címzettet.
8. Elektronikus levelekben érkezett futtatható állományok (pl.: .exe, .bat, .pif, .vbs) futtatása, illetve továbbítása nem engedélyezett.
9. Tilos az olyan levelek (ú.n. lánclevelek) továbbítása, amelyek a felhasználót a levél „továbbküldésre” kéri vagy szólítják fel. Az ilyen leveleket törölni kell.
10. Tilos továbbá a Kincstár által rendelkezésre bocsátott e-mail címmel, különböző webes szolgáltatásokhoz regisztrálni, hírlevélre feliratkozni, amennyiben az nem kapcsolódik szorosan a munkavégzéshez.

Az érzékeny adatok papír alapon történő kiszivárgásának megelőzése érdekében a Külső felhasználóknak különös figyelmet kell fordítaniuk:

Fénymásoló használata esetén:

1. Az érzékeny adatokat tartalmazó dokumentumokat tilos őrizzetlenül hagyni,
2. Többpéldányos másolás esetében egy példány fénymásolóban történő hagyása is illetéktelen hozzáférést eredményezhet, ezért meg kell győződni valamennyi példány eltávolításáról.

Hálózati nyomtató használata esetén:

1. A hálózati nyomtatóra végzett nyomtatást követően tilos az érzékeny adatokat, információkat tartalmazó iratokat az eszközben őrizzetlenül hagyniuk,
2. Meg kell győződni arról, hogy a kívánt nyomtatóra küldi-e a Külső felhasználó a nyomtatandó anyagot, mivel a nyomtató hibás átirányításakor a dokumentum illetéktelen kezekbe kerülhet.

Az információbiztonsághoz kapcsolódóan a felhasználóknak az „üres íróasztal és üres képernyő” irányelvvel összhangban az érzékeny adatokat tartalmazó nyomtatott dokumentumokat, információkat hordozó adathordozókat zárható helyen kell tartaniuk.

Kártékony kód elleni védelem, incidenskezelés

Minden felhasználói munkaállomáson kizárólag a központilag telepített, frissített vírusvédelmi szoftver fut, egyéb vírusvédelmi szoftver nem használható. A munkaállomáson futó vírusvédelmi szoftvert kikapcsolni, eltávolítani tilos. Akkor, ha a Külső felhasználó vírusfertőzésre utaló jeleket lát, akkor azt köteles jelenteni a HelpDesk részére.

Külső felhasználó teendői vírus észlelése vagy gyanúja esetén:

1. A Külső felhasználónak a munkaállomásán a munkavégzést a vírusmentesítés végrehajtásáig fel kell függeszteni.
2. A megnyitott fájlokat a bezárás előtt menteni kell, a futó alkalmazásokat le kell zárni, a meglévő hálózati kapcsolatból azonnal ki kell lépni és ki kell kapcsolni a számítógépet.
3. Értesítenie kell a vírusfertőzés tényéről a HelpDesket telefonon vagy elektronikus levélben (hibabejelentes@allamkincstar.gov.hu) még akkor is, ha a vírusvédelmi szoftver a vírust eltávolította. Minden olyan jelenséget, amely eltér a megszokottól, köteles jelenteni. A jelentésnek tartalmaznia kell a jelenség pontos leírását, előfordulásának körülményeit, gyakoriságát.
4. A vírusfertőzéseken túl a felhasználónak az alábbi eseményeket is jelentenie kell a HelpDesk felé:
 - a. Ha a vírusvédelmi szoftverek nem megfelelően üzemelnek,
 - b. Ha a vírusmintákat tartalmazó adatbázis túl régi – amelyet a vírusvédelmi szoftverek többsége jelez –, mivel ez a vírusvédelmi rendszer hatásosságát, illetve hatékonyságát veszélyezteti.
5. Vírussal fertőzött fájlt, vagy elektronikus adathordozót, bármilyen formában szándékosan továbbítani, továbbadni, illetve fertőzött állománnyal munkát végezni tilos.
6. Zsarolóvírus gyanúja esetén – pl. a számítógép adatainak titkosítására és pénzkövetelésre történő figyelmeztető ablak jelenik meg a számítógép képernyőjén – a számítógépet haladéktalanul ki kell kapcsolni, majd a Helpdesket és az IBV-t soron kívül értesíteni kell.

Minden olyan informatikai biztonsági eseményt, amely a Kincstár információs és egyéb vagyonelemeinek rendelkezésre állását, bizalmasságát, sértetlenségét veszélyezteti, valamint minden olyan eseményt, melynek során általános biztonsági előírások, informatikai biztonsági szabályok vagy az elfogadható használatra vonatkozó előírások megszegése van folyamatban, illetve gyanúja áll fenn, haladéktalanul jelezni kell az IBV-nek.

Egyéb előírások

Külső felhasználó a kincstári munkavégzés támogatásának céljából az üzemeltető szervezeti egység vezetője és az IBV együttes jóváhagyásával csatlakozhatnak saját tulajdonú mobil informatikai eszközökkel a Kincstár infrastruktúrájához, amennyiben az eszközt az üzemeltető szervezeti egység kijelölt személye ellenőrizte.

Távoli hozzáférés igénylésére Külső felhasználó önállóan nem jogosult. Jogosultságot a szerződéskötést kezdeményező, a Kincstár legalább főosztályvezetői besorolású munkahelyi vezető/projektvezető igényelhet.

Külső felhasználó részére a Kincstár éles, produktív, illetve jogszabály által védett adatokat kezelő elektronikus információs rendszereihez távoli hozzáférés – kivéve a katasztrófa elhárítás esetét – nem biztosítható.

Külső felhasználó a gépterembe kíséret nélkül, önállóan nem léphet be, csak kísérettel, és csak indokolt esetben. A be- és kilépések nyilvántartásában szükséges rögzíteni a belépő

személy nevét, szervezeti egységét (külső felhasználó esetén a külső felhasználót alkalmazó cég megnevezését), pontosan meg kell határozni a belépés célját, a belépés időpontját, a kilépés időpontját, valamint külső támogató személy esetén a kísérő személy nevét.

1. A belépési jogosultsággal nem rendelkező külső támogató személyeket – akik általában nem üzemeltetői, hanem eseti feladatokat végeznek – az üzemeltető szervezeti egység kijelölt személyének kell a gépterembe kísérni, majd ott a munkájukat folyamatosan felügyelni.
2. Minden, a külső felhasználó által végzett munkáról jegyzőkönyvet kell vezetni, amit a munkavégzés befejeztével a felügyelő személynek az aláírásával hitelesítenie kell.
3. A jegyzőkönyv alapján a munka befejezése után az Üzemeltetési naplóba be kell jegyezni a munkavégzést, ez a felügyelő személy feladata.

Minden olyan informatikai biztonsági eseményt, amely a Kincstár információs és egyéb vagyonelemeinek rendelkezésre állását, bizalmasságát, sértetlenségét veszélyezteti, valamint minden olyan eseményt, melynek során általános biztonsági előírások, informatikai biztonsági szabályok vagy az elfogadható használatra vonatkozó előírások megszegése van folyamatban, illetve gyanúja áll fenn, haladéktalanul jelezni kell az IBV-nek.

A Kincstár adatvagyonához való hozzáférés, illetve a Kincstár rendszereihez való csatlakozás során tilos a nyilvános hálózatok használata (beleértve a jelszóval nem védett otthoni hálózatokat is), továbbá tilos a munkavégzés minden nyilvános, nem kellően biztonságos helyszínen (például kávézó, repülőtér stb.).