

2. Melléklet

Információbiztonságra vonatkozó szabályok kiegészítése

Adatvédelmet érintő szabályok

1. Fizikai hozzáférés

A Hivatal szervezet munkavállalóit érintően az adatvédelemre vonatkozó biztonsági szabályokat határoz meg. **Az adatvédelmi szabályzat mellékletében lévő szabályokat a Hivatal megismerteti az érintett felhasználókkal, melyeket minden foglalkoztatott munkavállalónak be kell tartania.** Az adatvédelem fizikai határa a papír alapú dokumentum. Ez a melléklet az adatvédelmi oktatás mellékleteként is használható a felhasználói tudatosság fejlesztésére. Ennek védelme adatvédelmi szempontból szükséges és a következő védelmi szabályok betartása követendő:

Szabály	Megvalósítás módja
A személyes adatokat tartalmazó dokumentumok fizikai hozzáférésnek védelme érdekében intézkedéseket kell tenni.	
Tiszta asztal és tiszta képernyő elve: csak a munkavégzéshez szükséges iratok és dokumentumok legyenek elől, amik az aktuális munka elvégzése során szükségesek. A munkavégzés befejezését követően a bizalmas iratokat el kell tenni az asztalról biztonságos helyére.	

A papír alapú dokumentumok felügyelet nélkül történő hagyása kerülendő.



A zárható szekrényeket kulcsra zártan kell tartani, a kulcsokat biztonságos helyen kell tárolni.



Egyeztetés/megbeszélést követően minden bizalmas információt tartalmazó dokumentumot a biztonságának megfelelő helyre kell visszatenni és elzárni. A kapcsolódó feljegyzéseket és a tervezési szakaszhoz kapcsolódó – pl. táblára felírt – információk törlésére is figyelni kell.



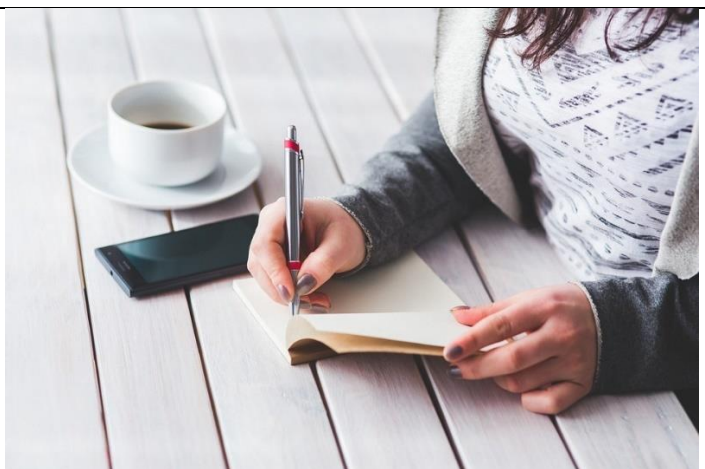
Személyes adatok, dokumentumok fénymásolóban történő másolása során sem eredeti, sem másolt példányt ne tároljunk a fénymásolóban.



A dokumentumok és a benne lévő információk csak a szervezet által meghatározott személyeknek vagy kijelölt megtekintési jogosultsággal rendelkezők számára adható át. Ennek jogalapjának tisztázását és az érintettek tájékoztatását követően lehet az érintett információkat a feldolgozó számára átadni.



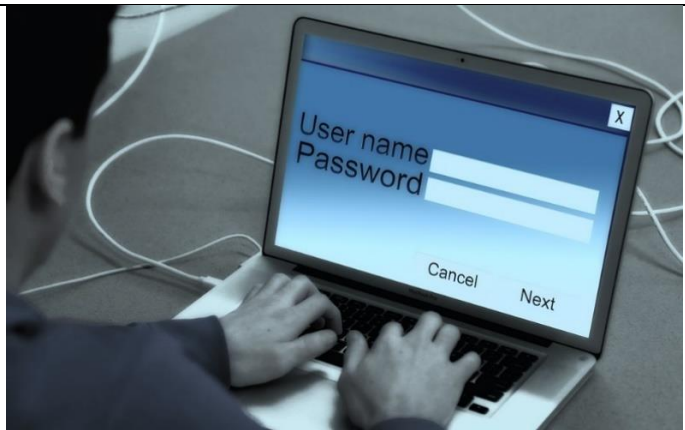
A személyes adatokat tartalmazó kézi feljegyzéseket az eredeti példányhoz hasonlóan megfelelő biztonsággal kell kezelni és tárolni.



2. Az informatikai rendszerek, hordozható eszközök használatára vonatkozó szabályok

Szabály	Megvalósítás módja
A felhasználók az általuk használt számítógépeket rendeltetésüknek megfelelően, munkavégzés céljából, annak támogatására használják.	A person's hands are shown typing on a silver laptop keyboard. The laptop is open on a white desk. A small potted plant is visible in the background.

A felhasználói számítógépre csak felhasználó névvel és jelszóval lehet belépni a számítógépbe és az elektronikus információs rendszerbe is.



A felhasználói fiókok megosztására nincs lehetőség, minden felhasználó csak a saját jogosultsági szintjének megfelelően használhatja az elektronikus információs rendszereket.



A számítógéptől rövid időre történő távollét esetén a gépet zároljuk, csak jelszóval lehessen feloldani a rendszerbe történő belépést. Hosszabb távollét esetén a számítógépet kapcsoljuk ki vagy tegyük hibernált állapotba.



Hordozható eszközök (pl. laptop) esetén is a szabályzatban meghatározott szabályokat kövessük.



Az elektronikus úton tárolt dokumentumokat, üzleti titoknak számító információkat titkosított formában és csatornán kell közlekedtetni és tárolni (pl. email, telefon).	
--	--

3. Felhasználók által telepíthető szoftverek

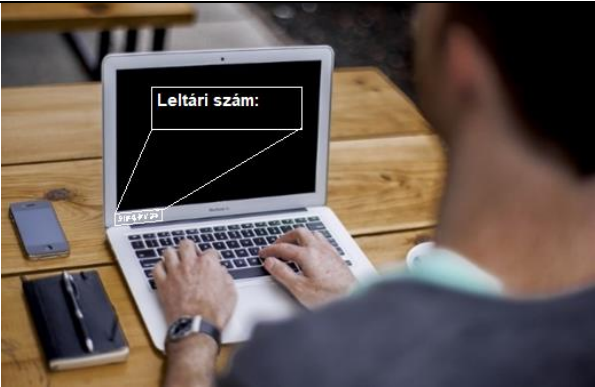
Szabály
- A Hivatal <u>rendszergazdája által telepített szoftvereket</u> használhatják a felhasználók.
- Bizonytalan származású vagy a rendszer működésére <u>magas kockázattal járó</u> alkalmazások nem telepíthetők
- A felhasználói gépekre alkalmazás telepítése csak a kinevezett rendszergazda által <u>besorolt alacsony kockázatú alkalmazások</u> közül lehetséges, illetve előzetes vezetői jóváhagyást követően.

4. Mobileszközök használata

Szabály	Megvalósítás módja
A mobil adathordozó eszközökön tárolt adatokat titkosítva kell kezelni.	
Hordozható számítógépet csak a munkavállalás céljából lehet használni előzetesen rögzített felhasználó névvel és jelszóval.	

Az adathordozókat, mobil eszközöket külső felek számára átadni TILOS!	
Nyilvános helyen történő eszközhasználat esetén ügyeljünk a bizalmas adatkezelésre, hogy a kezelt adatokat illetéktelenek ne ismerjék meg.	

5. Mobileszközök védelme

Szabály	Megvalósítás módja
Munkavégzés céljára csak a Hivatal által kiadott és jóváhagyott eszközök használhatók.	
Az adathordozókat gondosan kell elzárva tartani, megfelelő védelemmel ellátva.	

Részletszabályok	
-	Az adathordozók tárolását úgy kell megvalósítani, hogy biztosítva legyen az elvesztés, megsemmisülés, megsérülés, elcserélés, jogosulatlan hozzáférés kockázatának kizárása.
-	Azokat az adathordozókat, hordozható számítógépeket, amelyeket a szervezeti, üzleti cél mellett egyéb célra is használtak, csak előzetes formázás és felülvizsgálatot követően lehet kiadni ismételt használatra.
-	Személyes adatokat tartalmazó mobil eszközt, adathordozót, számítógépet, a Hivatal által jóváhagyott célon kívüli más célra nem lehet használni.
-	A hordozható eszközökön lévő adatok hozzáféréseinek védelméért a felhasználásra jogosultsággal rendelkező személy felel.
-	Meghibásodott személyes adatot tartalmazó eszközt (pendrive, külső meghajtó, merevlemez, hálózati merevlemez eszközt) csak előzetes adattisztítást követően lehet javítási célra kiadni.
-	Selejtezésre szánt eszközt csak a selejtezési eljárásrend szerinti megfelelő fizikai megsemmisítést vagy intézkedést követően lehet a Hivatalból kivinni.

6. Titkosítás

Szabály	
A mobil eszközöket, adathordozók, számítógépek megfelelő titkosítással kell védeni a Hivatal telephelyein, illetve a szállításkor.	
Személyes adatok továbbítása esetén lehetőség szerint biztonságos kommunikációs csatornán keresztül kell az adatokat továbbítani, például külső távoli kapcsolat esetén csak VPN biztonságos kommunikációs csatornán lehet az adatokat továbbítani.	VPN

7. Végpont és hálózatvédelem

Szabály	Típusa
A számítógépeken telepített vírusvédelmi rendszert TILOS kikapcsolni!	
Az adathordozók – különös tekintettel az idegen eszközök – használatbavétele előtt előzetes vírusellenőrzést kell alkalmazni.	!
Hordozható számítógépek hálózatra kapcsolódása előtt előzetes vírusellenőrzést kell alkalmazni.	!

A hálózaton csak a rendszergazda által üzemeltetett eszközök lehetnek.	!
Szomszédos helyiségbe hálózati kábelt áthúzni TILOS!	⊘
Hálózati azonosítót és jelszót átadni TILOS!	⊘
Eszközök megosztása a hálózaton TILOS!	⊘

8. Vírusvédelem, fertőzés jelei, teendők

Szabály
A Hivatal számítógépeit, csak az általa kijelölt rendszergazda által telepített vírusvédelmi alkalmazás telepítését követően lehet használni.
Ha a vírusvédelmi szoftver nem működik megfelelően, illetve a felhasználó valami rendellenességet észlel, azt azonnal jelezni kell a rendszergazda felé.
A vírusellenőrző vírusadatbázisának frissítését TILOS kikapcsolni és folyamatosan le kell futtatni.
Idegen vagy külső adathordozó használata előtt előzetes vírusellenőrzést kell végrehajtani.
Rendszeres vírusellenőrzést kell a rendszereken végezni.
A külső forrásból érkező dokumentumokat előzetesen meg kell vizsgálni, a vírusmentességről meg kell győződni.

Vírusfertőzés jelei:

TÜNETEI	
A rendszer a megszokottól eltérő módon működik	
Ha a képernyőn olyan információ jelenik meg, ami a megszokottól eltérő	

Ha a rendszer működése lelassul	
Az adatok a megszokottól eltérő formában jelennek meg	❌
Ha a hálózati megosztás valamiért nem érhető el	❌
Ha a mappa tartalma egyik napról a másikra eltűnik	❌
TEENDŐ	
1.	Azonnal értesíteni a rendszergazdát és az érintett munkavállalókat
2.	A biztonsági mentést tartalmazó meghajtót, adathordozót NE helyezze a gyanús számítógépbe
3.	egyéb adathordozót NE helyezzen a számítógépbe
4.	Kövesse a mindenkor RENDSZERGAZDA UTASÍTÁSAIT
5.	A számítógépet KARANTÉNBA HELYEZNI csak a rendszergazda jogosult

9. Jelszóhasználati szabályok

A jelszó előállítás elvei:

Szabály	Megvalósítás módja
A jelszónak legalább 8 karakterből kell állnia	*****
Kisbetűt, nagybetűt, számot tartalmazzon	Abcd123456
Egyedi jelszavakat használjunk (pl. jelmondat)	Sussfelnap123456

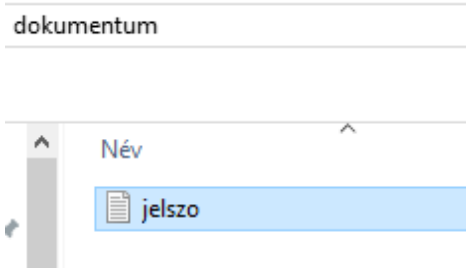
A jelszó karbantartásának elvei:

Szabály	Megvalósítás módja
korábban használt jelszavainkat többet ne használjuk	Abcd123456

a jelszót rendszeres cserélni kell	
a jelszó valamilyen okból történő megadása esetén (pl. karbantartás miatt) a jelszót mielőbb meg kell változtatni	 <u>Jelszó módosítás</u>
a rendszerben felmerülő incidens bekövetkezésének gyanúja esetén jelszócserét kell végrehajtani	INCIDENS → Jelszó csere
különleges esetben (pl. elfelejtett jelszó) megfelelő rendszergazdai azonosítással, vezetői jóváhagyással új jelszó igényelhető, amit a belépést követően azonnal le kell cserélni	Elfelejtett jelszó → Új igénylése

A jelszó bizalmasságának megőrzési elvei:

Szabály	Megvalósítás módja
A jelszavak titokban tartása	

A jelszavakat ne ragasszuk ki a monitorunkra, sem olyan helyre ahol mindenki számára elérhető	
A jelszavak ne osszuk meg egymás között még helyettesítés céljából sem	
Jelszavakat ne tároljunk dokumentumokban	
A jelszavakat ne adjuk ki telefonon, sem más megkeresés esetén	
A jelszó beírásakor ne hagyjuk, hogy bárki mögöttünk álljon és kifigyelje a jelszavainkat	

10. Viselkedési szabályok az interneten

A Hivatal internet használatra vonatkozó szabályait a 12.2.1 pont szabályozza

A Hivatal munkavállalóival szemben elvárt magatartásszabályok:

Szabály	Típusa
A Hivatal az internethasználatot munkavégzés céljából, a feladatok ellátásának támogatása érdekében biztosítja	!
Az internet használata személyre szóló, kizárólagosan csak a Hivatal munkavállalói vehetik igénybe	!
Az illegális tartalommal rendelkező oldalak használata, megtekintése TILOS!	
Kompromittáló tartalommal rendelkező oldalak használata, megtekintése TILOS!	
Online játék használata TILOS!	
Minden olyan oldal használata és megtekintése TILOS, amelynek látogatása a BTK-ba ütköző jogi következményt von maga után (pl. szexuális, pornográf, torrent, gyűlölet, rasszizmus, erőszakot népszerűsítő oldalak)	
Bizonytalan forrású, biztonsági tanúsítványt nem tartalmazó oldalak használata, megtekintése TILOS!	
Szervezeti és személyes adatok küldése, kiszivárogtatása bármilyen médián keresztül TILOS!	
Közösségi médián történő információ kiadása, feltöltése TILOS!	
Bizalmas, titkos információ bármilyen nem vezetőség által megadott információs csatornán történő átadása TILOS!	
Minimalizálás elve, csak a munkavégzéshez szükséges mennyiségű oldal legyen megnyitva a munkavégzéshez.	!

11. Elektronikus levelezés elvei

Az elektronikus levelezés adatvédelemre vonatkozó elveit az IBSz 12.2.1 és a 12.2.2 pontjai szabályozzák.

Szabály	Típusa
A levelező fiók munkavégzésből történő használata és abban lévő személyes adatok kezelése.	!

Magáncélú levelek fogadás és küldés a Hivatali levelezésből TILOS, illetve fordítva, TILOS a munkavállalással kapcsolatos email címek magán célra történő felhasználása.	
Munkaviszony megszűnése esetén a felhasználó fiók Hivatali leveleinek átadása a Hivatal által kinevezett munkavállaló részére. Továbbá a levelező fiók megszüntetése. Általános Hivatali fiók esetén a felhasználó név és jelszó átadása csak a kinevezett személy részére.	!
A felhasználói fiók munkafolyamattal kapcsolatos tartalmát a munkaviszony megszűnése esetén TILOS törölni!	
A Hivatal által nem támogatott levelezőrendszer (pl. Gmail, Freemail) használata munkavégzésre nem engedélyezett. (Részlet az IBSzből)	
Csatolmányt küldeni csak megfelelő biztonsággal és a kezelt adatoknak megfelelő arányos védelemmel lehet küldeni (pl. titkosítással)	!

Levélküldés/fogadás elvek:

Szabály	Típusa
A feladó a levélben küldött tartalomért felelős	!
Az e-mail küldését TILOS más nevében megtenni csak a vezető által jóváhagyott személyek számára	
Az e-mailt másolatban, titkos másolatban TILOS más magánszemélynek tovább küldeni	
A címzetteket mindig egyértelműen definiálni kell, TILOS ismeretlen címekre üzenetet küldeni	
Az e-mail csak az előzetesen egyeztetett megbízható fogadó címekre kerülhet kiküldésre	!
A címzett felelős az e-mail fogadásáért, további feldolgozásáért és továbbításáért	!
Az e-mailt küldő személyek hitelességéről mindig meg kell győződni mielőtt a küldő által megfogalmazott kérésre válaszolnánk	!
Ismeretlen helyről származó e-maileket megnyitás nélkül törölni kell	!
Belső vagy külső félrevezető címzett vagy tárgy, tartalom esetén azonnal értesíteni kell az érintett rendszergazdát	!

Az e-mailben küldött csatolmányokat csak előzetes vírusellenőrzést követően lehet megnyitni fokozott figyelemmel és körültekintéssel	!
---	----------

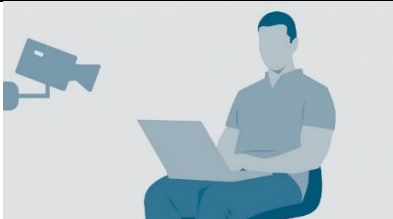
12. Fizikai védelem

Szabály	Megvalósítás módja
A számítógépeket TILOS hőmérséklet, mágneses hatás, magas páratartalom vagy bármilyen füstképződés hatásának kitenni.	
A számítógépeket csak kikapcsolt állapotban lehet szállítani, beleértve a hordozható számítógépeket is. Kivételt képez a mechanikus alkatrészt nem tartalmazó eszköz, de csak speciális esetekben a vezető által jóváhagyottan.	
A személyes adatok szállítása esetén el kell kerülni bármilyen a rendszer állapotát rongáló szituációt.	

13. Biztonsági mentés

Szabály
- A rendszerben tárolt adatokról a rendszer felhasználóinak kötelességük folyamatos biztonsági mentést készíteni amennyiben a Hivatal erre biztosított adathordozót. A munkamenethez szükséges adatokról a helyi számítógépre biztonsági mentés céljából készíthet mentést. A külső adathordozókon tárolt adatokat titkosított formában, fizikailag elszeparált helyen kell tárolni. - A hordozható számítógépen kezelt adatokról a kinevezett fájlserverre kell biztonsági mentést készíteni, ezt követően az adatokat a hordozható számítógépről törölni kell.

14. Kamerás megfigyelés szabályai

Szabály	Megvalósítás módja	
A képfelvételek megtekintésére és visszánézésére szolgáló monitort úgy kell elhelyezni, hogy a képfelvételek sugárzása alatt azokat a jogosultsági körön kívül más személy ne láthassa.		
A megfigyelés és a tárolt képfelvételek visszánézése kizárólag a jogsértő cselekmények kiszűrése, az azok megszüntetéséhez szükséges intézkedések kezdeményezése céljából végezhető.		
A kamerák által sugárzott képekről a központi felvevő egységen kívül más eszközzel felvételt készíteni nem lehet.		
A tárolt képfelvételekhez hozzáférés csak biztonságos módon, és akként történhet, hogy az adatkezelő személye azonosítható legyen.	felhasználó név	admin
	jelszó	*****
A felvétel hordozó eszközeit elzárt helyen kell tárolni.		
A tárolt képfelvételek visszánézését és a képfelvételekről készített mentést dokumentálni kell.		

Jogsértő cselekmény észlelését követően a cselekményről készült felvétel tárolása és a szükséges hatósági eljárás kezdeményezése felől intézkedni kell, egyben tájékoztatni kell a hatóságot, hogy a cselekményről képfelvétel készült.



15. Kockázatelemzés

A Hivatal kockázatelemzésre vonatkozó szabályait a 11.pont rögzíti. A kockázatkezelést az értelmező rendelkezésre részben kifejtettek szerint végzi.

16. Adatvédelem és tudatosság

A Hivatal az adatok védelme érdekében biztonság tudatos szemléletet alakít ki, ennek szabályait a Hivatal IBSz 9.4 pontja szabályozza.