Az Informatikai Biztonsági Szabályzat felhasználókra vonatkozó előírásai

1. Az Informatikai Biztonsági Szabályzat célja

Az Informatikai Biztonsági Szabályzat (továbbiakban: IBSZ) célja a Hivatalnak az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben (továbbiakban: Ibtv.), valamint az ASP szakrendszeri kapcsolódás okán a 257/2016. (VIII. 31.) Korm. rendeletben foglalt információbiztonsági követelményeknek való megfelelőségét biztosítani.

Az Ibtv. és végrehajtási rendelete – 41/2015. (VII. 15.) BM rendelet (továbbiakban: Vhr.) – a Hivatal által használ informatikai rendszerek, az azokban kezelt adatok védelmét célozza, közvetve pedig ez által a kormányzati szervek által biztosított központi szakrendszerek, így például az ASP-ben kezelt adatok biztonságát is hivatott garantálni.

Az informatikai rendszereket hatékonyan úgy lehet megvédeni, ha annak minden veszélyeztetett pontján megfelelő védelmet alakítunk ki, minden kiskaput becsukunk, emiatt fontos, hogy minden, a központi rendszerekhez hozzáférő, azokat használó Önkormányzatnál, Hivatalnál és egyéb szervezetnél – kvázi minden számítógépen, minden csatlakozó hálózaton – egyformán és jól működő informatikai biztonsági megoldásokat alkalmazzunk (ezt nevezik egyenszilárd védelemnek).

2. Az IBSZ hatálya

A szabályzat céljából kiindulva hatálya mindenkire kiterjed, aki bármilyen módon részt vesz a Hivatalnál keletkező, felhasznált, feldolgozott, tárolt, illetve továbbított adatok kezelésében. Így minden munkavállalóra, tisztviselőre, az IT üzemeltetőre, informatikusra, az információbiztonsági felelősre (IBF), a Hivatal weboldalának fejlesztőjére, illetve karbantartójára, valamint a számítógépek, nyomtatók, stb. javítását végző szervizes szakemberekre egyaránt.

Kiterjed továbbá minden a Hivatalnál a munkavégzéshez használt informatikai és infokommunikációs eszközre, így a számítógépekre, szerverekre, az azokon futtatott programokra, a nyomtatókra, hálózati eszközökre, az okostelefonokra és még a vagyonvédelmi rendszerekre is, úgymint a riasztó, a beléptető vagy a kamerás megfigyelő rendszerek.

Mindenre és mindenkire, ami vagy aki részt vesz a Hivatalnál az adatok kezelésében, feldolgozásában vagy továbbításában. Ezt a nagy halmazt hívja a törvény elektronikus információs rendszernek (továbbiakban: EIR).

3. Biztonsági osztályba sorolás, Intézkedési terv, Cselekvési terv, EIR nyilvántartás

A törvény a szervezeteket és az általuk használt informatikai rendszereket, EIR-eket egy 1-5-ig terjedő skálán különböző biztonsági szintekbe, illetve osztályokba sorolja. Minél magasabb a szervezet, illetve az általa használt EIR-ek biztonsági besorolása, annál több és szigorúbb biztonsági követelménynek kell megfelelnie.

A Hivatal jogszabályi előírások által megállapított szervezeti biztonsági szintje 3-mas, az általa használt EIR-eké általában 2-es, az ASP szakrendszer egyes moduljainak besorolása viszont ettől magasabb, 3-mas, illetve 4-es biztonsági osztályba tartoznak. A használt rendszerekről nyilvántartást kell vezetni, amelyben szerepel minden rendszer biztonsági besorolása is. Ez a nyilvántartás az IBSZ mellékletét képezi.

Amennyiben a szervezet nem teljesíti a törvény által előírt, a biztonsági besorolásának megfelelő biztonsági követelményeket, akkor az azok elérésére intézkedési vagy cselekvési tervet kell készítenie, s azt végrehajtania.

4. MI AZ ÖN FELADATA?

A jogszabályi előírások több mint ezer biztonsági követelményt fogalmaznak meg, amelyeknek meg kell felelni (ezeken alapul a szabályzat, az IBSZ is természetesen). Ezek közül számos olyan van, amit a Hivatalnak a napi működése során új tevékenységként kötelező alkalmazni (pl.: nyilvántartás vezetése a belépőkről), számos olyan is, amit csak az informatikus tud és neki is van jogosultsága beállítani (pl.: a számítógépen használható programok telepítése, jelszó szabályok, az internet böngésző programok biztonsági beállításai), s sok olyan, ami alapvetően adminisztratív, szabályozási vagy tervezési tevékenységhez kapcsolódik (pl.: üzletmenet-folytonossági terv elkészítése, szerződések biztonsági követelményeinek érvényesítése), melyekhez az információbiztonsági felelős (továbbiakban: IBF) módszertani támogatást biztosít, s vannak emellett olyan további követelmények is, amelyek kizárólag az IBF feladatkörébe tartoznak (pl.: ellenőrzési, jelentési kötelezettségek).

A jó hír, hogy mindezzel kapcsolatban hivatali dolgozóként gyakorlatilag csupán **két fő feladat**a van:

1. **a munkavégzéshez kapott eszközök** (pl.: számítógép, telefon, programok) előírásoknak megfelelő, **rendeltetésszerű használata;**
2. **a hibák vagy rendellenességek jelzése.**

A továbbiakban e két alapfeladathoz, főként pedig a rendeltetésszerű használathoz kapcsolódó, az IBSZ-ben megfogalmazott biztonsági szabályokat mutatjuk be, amelyek jelentős része feltételezhetően nem lesz ismeretlen, mivel „nincs új a nap alatt”, otthon is próbáljuk megóvni értékeinket, kihúzzuk a vasalót és bezárjuk az ajtót, ha elmegyünk valahová – gyakorlatilag a Hivatalban is ehhez hasonlóan egyszerű, örök érvényű igazságoknak megfelelő intézkedésekkel kell a biztonságos működést megvalósítani.

5. „Tiszta asztal, tiszta képernyő”

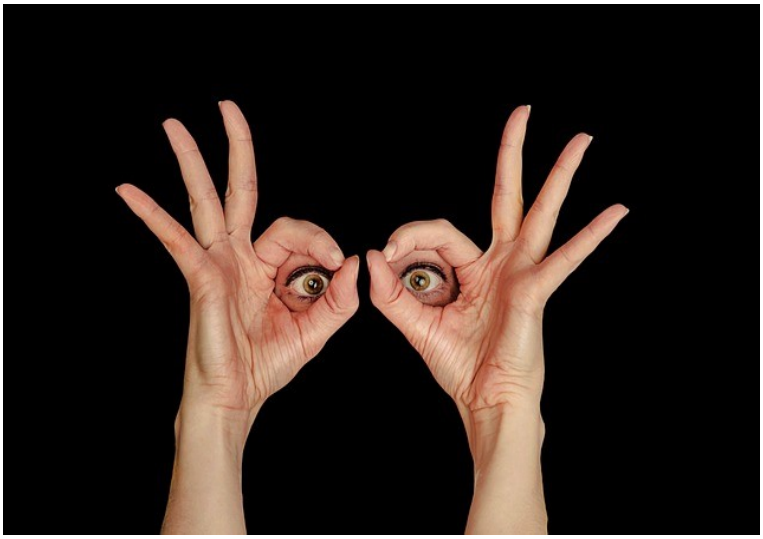
Adatvédelmi szempontból kiemelten fontos, hogy mindenki, aki a Hivatalban tartózkodik, legyen az ügyfél vagy egy látogató, csak olyan dolgokat láthasson meg – akár véletlenül is – amik rá tartoznak.

Erről az alábbiak szerint kell gondoskodnia:

Az ügyintézés időtartama alatt kizárólag az aktuális ügyhöz szükséges iratok lehetnek elől (pl.: az íróasztalon), s csak az aktuális ügyintézéshez szükséges alkalmazások, programablakok lehetnek megnyitva a képernyőn.

Az ügyintézés, illetve a munkavégzés befejezését követően minden iratot az eredeti tárolási helyére kell visszahelyezni, illetve a már nem szükséges alkalmazásokat, programablakokat be kell zárni.

A legjobb megoldás, ha a monitor eleve úgy van elhelyezve vagy elfordítva, hogy annak képét az ügyfél eleve nem láthatja.



6. Az információbiztonsággal kapcsolatos engedélyezési eljárás

A biztonságos működés egyik alapja, hogy minden változtatás (így például egy új program telepítése, jogosultság megadása vagy egy új számítógép üzembe helyezése) kizárólag engedélyhez kötötten és dokumentáltan történhet. A Hivatal vezetője, a Jegyző jogosult és köteles a Hivatal hatáskörébe tartozó minden információbiztonsággal kapcsolatos tevékenységgel, intézkedéssel kapcsolatban a szükséges engedélyezési eljárást lefolytatni.

Az Ön feladata, hogy új igény esetén azt a megfelelő dokumentum (Változáskezelési adatlap – IBSZ mellékletében található a minta ehhez) kitöltésével kezdeményezze. A jóváhagyás, engedélyezés szintén ezen történik.

Az új igényt ezen az adatlapon kell jelölnie, adott esetben indokolnia, s ezt a kitöltött igénylőlapot a döntésre jogosult (Jegyző) számára eljuttatnia.

Változáskezelési adatlap

I. Változás/igény bejelentés adatai *(a változást kezdeményező/igénylő tölti ki)*

Változást kezdeményező/igénylő/bejelentő adatai	
Név	***Beosztás/munkakör***
Változás/igény adatai	
Változás/igény típusa (a megfelelőt jelölje X-szel)	
1. Új infokommunikációs eszköz igénylése (pl.: számítógép, telefon)	
2. Hozzáférés, jogosultság beállítása/módosítása, konfiguráció megváltoztatása (pl.: felhasználói fiók létrehozása, törlése, rendszer vagy rendszerelem beállításainak módosítása)	
3. Hivatali – az elektronikus információs rendszereknek helyt adó – létesítményekbe, helyiségekbe történő belépés engedélyezése (pl.: karbantartás céljából eseti belépés – lásd: 5. pont)	
4. Információs rendszerelem be- és kiszállítása (pl.: hardver szállítás – 3. pont is kell hozzá!)	
5. Karbantartás, javítás (pl.: hardver csere, bővítés), valamint a munkavégzés engedélyezése (3. pont is kell hozzá!)	
6. Elektronikus adathordozók használata (pl.: CD/DVD írás, USB pendrive használat, stb.)	
7. Távoli, illetve vezeték nélküli hozzáférés biztosítása	
8. Együttműködésen alapuló számítástechnikai eszközök használata (pl.: audio és/vagy video kommunikációra alkalmas eszköz használatának engedélyezése)	
9. Új elektronikus információs rendszer bevezetése	
10. Új rendszerelem meglévő elektronikus információs rendszerbe illesztése (pl.: program telepítése, hardver bővítés, stb.)	
11. Az alkalmazott elektronikus információs rendszer más (helyi, illetve külső) elektronikus információs rendszer(ek)hez történő kapcsolódása	
A változás/igény részletes leírása (pl.: igényelt eszköz, szoftver típusa, paraméterei vagy a belépés tervezett időpontja, stb.)	
Változás/igény bejelentés időpontja (dátum):	

II. Változás/igény engedélyezésének adatai *(a változást jóváhagyó, engedélyező tölti ki)*

A változást/igényt **engedélyezem / nem engedélyezem**.	
(a megfelelő aláhúzandó)	
Az engedélyezett változás végrehajtásáért felelős neve (pl.: IT üzemeltető vagy a belépést felügyelő munkatárs, stb.):	
Változás végrehajtásának határideje (dátum):	
Dátum:	
aláírás	

7. Számítógép használattal összefüggő szabályok, feladatok

Általánosságban igaz, hogy a Hivatal minden informatikai eszközének (számítógép, az arra telepített programok, tűzfal, router, stb.) beállítását, karbantartását és javítását az IT üzemeltetési feladatokkal megbízott informatikus végzi.

A programok telepítésére, a beállítások megváltoztatására szintén az informatikus jogosult. Kivételt képeznek ez alól például az ASP és az ahhoz hasonló olyan központi rendszerek, amelyek esetében a programokon belüli beállításokat az erre feljogosított felhasználó (pl.: tenant admin) módosíthatja.

7.1. A szoftverhasználat korlátozásai, szoftverek telepítése

A Hivatal a munkatársai számára az informatikai eszközöket és erőforrásokat a hivatali munkavégzés céljára biztosítja, azokon kizárólag az IT üzemeltető által telepített szoftverek, alkalmazások és szolgáltatások használatára jogosultak.

A Hivatal informatikai rendszereiben kizárólag a Jegyző által engedélyezett, jogtiszta, a Hivatal által megvásárolt kereskedelmi és/vagy szabad felhasználású (pl.: nyílt forrású: open source vagy ingyenesen használható: freeware), valamint jogszabályban előírt központi szolgáltató által biztosított programokat szabad telepíteni és használni.

A munkaállomásokra a felhasználók nem telepíthetnek programokat, továbbá nem módosíthatják a telepített szoftverek beállításait, működését és nem törölhetik, nem távolíthatják el azokat!

A hivatali munkavégzés, az ügymenet, illetve az adott folyamat hatékonyságát javító szoftverek használatára ugyanakkor javaslatot tehet a Jegyző felé, aki az engedélyezési eljárás keretében dönt a program beszerzésének, illetve telepítésének engedélyezéséről.

Az IT üzemeltető feladata ellenőrizni a telepített és futtatott programokat és alkalmazásokat, valamint az állomány megosztásokat az esetlegesen szerzői joggal védett tartalmak jogosulatlan megosztására, megjelenítésére, végrehajtására vagy reprodukálására irányuló tevékenységek szűrése céljából.

Nem engedélyezett tevékenység vagy szoftverhasználat észlelése esetén az IT üzemeltető köteles a Jegyzőt haladéktalanul tájékoztatni, valamint az utasításának megfelelően a szükséges intézkedéseket (pl.: nem engedélyezett szoftver vagy jogvédett tartalom eltávolítása) megtenni.

Az engedély nélküli tevékenységet végrehajtó, szabályszegő személy felelősségre vonására, fegyelmi intézkedés kezdeményezésére a Jegyző jogosult.

7.2. Viselkedési szabályok az interneten

A Hivatal a munkatársai számára az informatikai eszközöket és erőforrásokat, így az internet elérését szintén kizárólag a hivatali munkavégzés céljára biztosítja.

A hivatali internet használata során TILOS

- a Hivatallal kapcsolatos információk nyilvános internetes oldalakon való illegális közzététele;
- a hivatali email cím magáncélú használata, azzal történő regisztráció nem a munkavégzéshez kapcsolódó internetes szolgáltatások (pl.: hírlevél, levelező lista feliratkozás; webáruház, stb.) igénybevételéhez;
- fájlcserélő vagy chat szolgáltatás használata, valamint a munkavégzéshez nem kapcsolódó letöltések végrehajtása.

A Jegyző a munkavégzés által indokolt esetben fenti szabályok betartása alól felmentést adhat. Például a bárki számára kiadható információk esetében (jellemzően pl.: kitöltetlen űrlap, ügyintézéshez köthető folyamatleírás, közérdekű tájékoztató anyag) a Jegyző általános engedélyével továbbíthatók korlátozás nélküli megtekintésre, illetve felhasználásra például az ügyfelek számára, illetve a közzétételi kötelezettség teljesítésével kapcsolatban feladatot ellátó munkatárs a Hivatal honlapján vagy jogszabályban meghatározott központi kiszolgálón kezelhet (feltölthet) ilyen, nyilvánosan elérhető tartalomnak minősülő adatokat.

A Hivatalban csak a Jegyző által engedélyezett információkat lehet közzétenni. Minden más információ közzététele TILOS!

7.3. Az internet böngésző programok biztonsági beállításai

Az internet elérésére használt programokban (pl.: Internet Explorer, Mozilla Firefox, Google Chrome, Safari, Opera, stb.) a végrehajtható programok, script-ek (pl.: Java Applet, JavaScript, VB Script, CGI, stb.) letöltését, futtatásának lehetőségét, valamint web és alkalmazásba csomagolt ActiveX objektumok működését le kell tiltani, továbbá gondoskodni kell arról, hogy a böngésző program biztonsági frissítése rendszeresen megtörténjen.

A beállításokat az IT üzemeltetési feladatokkal megbízott informatikus hajtja végre, a beállítások engedély nélküli megváltoztatása viszont TILOS!

7.4. Azonosítás és hitelesítés

A számítógépes munkavégzéshez szükséges felhasználói fiókok létrehozását és a jogosultságok beállítását az engedélyezési eljárás alapján a Jegyző engedélyezi és az IT üzemeltető hajtja végre.

A munkaállomásokon a felhasználó 15 perc időtartamú inaktivitása esetén azonosítója letiltásra kerül (pl.: számítógép automatikus zárolása, képernyőkímélő program elindítása), s újbóli használatához ismételten be kell jelentkeznie.

Ennek célja megakadályozni, hogy távollétében (ha esetleg bekapcsolva is hagyta a gépét) az Ön bejelentkezési adataival véletlenül vagy szándékosan ne lehessen a számítógépén semmilyen tevékenységet végrehajtani. **Fontos, hogy minden olyan műveletért, ami az Ön nevében került végrehajtásra, azért Ön a felelős!**

Az informatikai rendszerek általában naplózzák (logolják) a bennük végrehajtott tevékenységeket, a hivatal által használt számítógépek és programok, s természetesen a központi rendszerek (pl.: ASP, ÁNYK, stb.) is. A naplókban a bejelentkezett felhasználó adatainak marad nyoma, a tényleges személy ellenőrzését jellemzően egyetlen rendszer sem képes végrehajtani. Ezzel a biztonsági beállítással a visszaélésektől és a kollégák esetleges tréfáitól (pl.: háttérképe viccesre cserélése) egyaránt védve lesz.

7.5. Sikertelen bejelentkezési kísérletek

Szintén a biztonságot szolgálja, hogy a számítógépeken 3 egymást követő sikertelen bejelentkezési kísérlete esetén a munkaállomás automatikusan zárolja a felhasználói fiókot.

Ha eltéveszti a jelszavát többször is, akkor például a harmadik hibás jelszó megadását követően ez fog történni. A fiók zárolása 30 perc múlva automatikusan megszűnik, azaz újra be tud jelentkezni a helyes jelszóval. Ha elfelejtette a jelszavát, mielőbb jelezze az informatikusnak.

7.6. A jelszavak és egyéb hitelesítésre szolgáló eszközök kezelése, védelme

A számítógépeken és minden további eszközön és olyan programban, amely képes kezelni, azokon kötelező a jelszavas védelem beállítása és alkalmazása.

A számítógépen beállítandó felhasználói jelszavakra vonatkozó általános jelszó követelmények:

- a jelszó minimális hossza (legrövidebb jelszó): 8 karakter;
- a jelszó bonyolultsága (komplexitás): tartalmaznia kell legalább egy kis- és nagybetűs, speciális karaktert (pl.: írásjelet), valamint számjegyet;
- előző jelszavak megőrzése: legutolsó 5 jelszó tárolása (azaz ezeket nem lehet újra megadni a jelszócsere alkalmával, újat kell kitalálni);
- a jelszavak minimális és maximális élettartama: 0 és 90 nap (azaz kb. 3 havonta kötelező a jelszócsere).

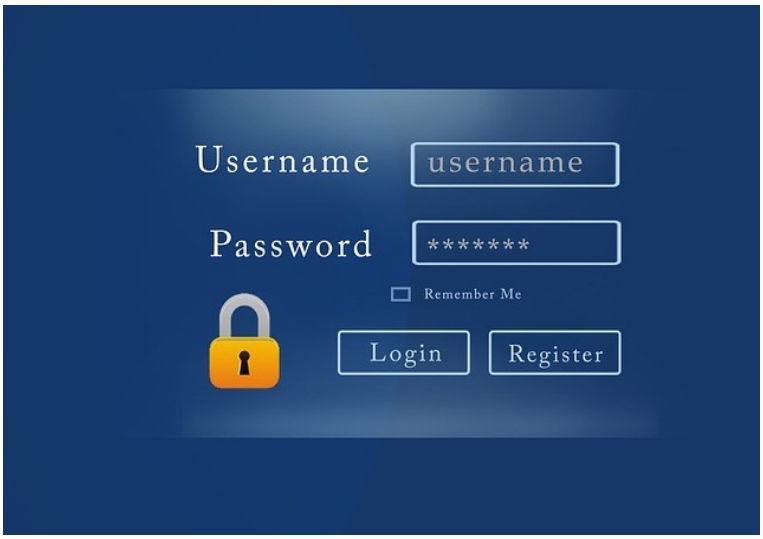
Fenti jelszóképzési szabálytól az erősebb jelszavak alkalmazása felé (pl.: hosszabb jelszó vagy „jelszó helyett jelmondat”) el lehet térni.

A központi üzemeltetésű rendszerek (pl.: ASP) esetében a rendszer tulajdonosa által meghatározott jelszóképzési szabályokat kell alkalmaznia.

A felhasználói jelszavakat tilos papír alapon, felírva tárolni! A jelszavak elektronikus tárolása (pl.: jelszókezelő programban) kizárólag offline tárolással engedélyezett; azaz egy okostelefonon vagy tableten futó alkalmazásban, állandó internetkapcsolattal rendelkező eszközön TILOS!

Az interneten keresztül közvetlenül (külön tűzfalas védelem nélkül) elérhető eszközök általában sokkal nagyobb veszélynek vannak kitéve, mint a hivatali, belső hálózaton működő gépek, emiatt ezeken tárolni a fontos jelszavakat felettébb kockázatos.

Az internetkapcsolaton keresztül elérhető rendszerek, EIR-ek esetében az internet böngészőprogramok beépített kényelmi funkciójának, a bejelentkezési adatok tárolásának (pl.: automatikus kiegészítés, felhasználói jelszavak megjegyzése) a használata tilos, a funkciót ki kell kapcsolni! Egy vírustámadás esetén az így tárolt jelszavakat a számítógépes vírus könnyedén meg tudja szerezni és elküldheti a vírus terjesztőjének, emiatt fontos ezt megelőzendő a jelszavak megjegyzésének letiltása.



mennyiben valamely rendszerhez egyéb hitelesítő eszközt (pl.: hardver token, kódkártya, PKI tanúsítvány) is alkalmaznak, úgy a kapott eszköz, illetve jelszó bizalmasságának és sértetlenségének megőrzése az Ön feladata és felelőssége. Bármely hitelesítésre szolgáló eszköz kompromittálódását (pl.: a jelszó illetéktelen személy általi megismerése) vagy sérülését, az eszköz elvesztését, ellopását az észlelést követően haladéktalanul köteles a Jegyzőnek jelenteni.

Kiemelten fontos, hogy minden rendszerben különböző jelszót használjon, továbbá, hogy a hivatali munkavégzés során a rendszerekben beállított jelszavait véletlenül se használja saját céljára (pl.: magánjellegű email fiókjához)!

7.7. Adathordozók használata, kezelése és védelme

A hivatali számítógépekhez és hálózathoz kizárólag a Hivatal által biztosított és/vagy ellenőrzött mobil eszközök (pl.: laptop, tablet, okostelefon) és adathordozók (pl.: pendrive, memóriakártya, külső merevlemez, CD, DVD lemez, digitális fényképezőgép, stb.) csatlakoztatása engedélyezett. Eltérni ettől indokolt esetben, a Jegyző jóváhagyását (lásd: engedélyezési eljárás) és a szükséges biztonsági ellenőrzések (pl.: vírusellenőrzés) lefolytatását követően lehet.

Idegen eszköz – ide tartozik a saját pendrive vagy egyéb, a fentiekben felsorolt eszköz is – csatlakoztatási igényét a Jegyző számára engedélyezés céljából az igénylő köteles előzetesen jelezni.

Adathordozó vagy mobil eszköz engedély nélküli csatlakoztatása biztonsági eseménynek minősül, amely a fegyelmi eljárást vonhat maga után.

A hivatali munkavégzéshez a Hivatal által biztosított, beépített adathordozót tartalmazó mobil eszközök és mobil adattároló eszközök fizikai védelméről és biztonságos tárolásáról és kezeléséről Ön köteles gondoskodni, az alábbiak szerint:

A mobil eszközt az adathordozó típusának megfelelően lehetőség szerint fájl- vagy tárolószintű titkosítással kell védeni. Az eszköz biztonságát – amennyiben technológiai oldalról támogatott – további hozzáférés védelmi megoldás (pl.: jelszó, PIN kód, stb.) alkalmazásával is biztosítani kell.

A titkosítás beállításában az IT üzemeltető feladata közreműködni, a titkosításhoz használt jelszó biztonságos kezelése és megőrzése az Ön feladata és felelőssége.

Használaton kívül az eszközt, adattárolót el kell zárni, illetve illetéktelenek számára hozzáférhető helyen folyamatos felügyelet nélkül, őrizetlenül hagyni (pl.: közterületen parkoló zárt gépjárműben is) TILOS!

Az adathordozó vagy eszköz elvesztése, ellopása biztonsági eseménynek minősül, melyet az észlelést követően haladéktalanul köteles jelenteni a Jegyző számára.

A meghibásodott eszköz vagy adathordozó tartalmát törölni kell olyan módon, hogy az adatokat arról ne lehessen visszaállítani. A megfelelő, biztonságos törlésről az informatikus gondoskodik a selejtezés vagy például a szervízbe szállítás előtt.

7.8. Vezeték nélküli hozzáférés (WI-FI)

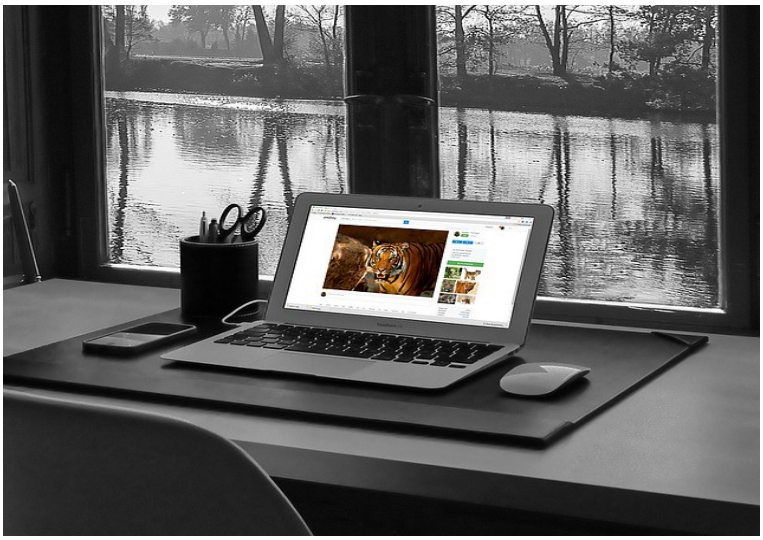
A Hivatal épületeiben vezeték nélküli hálózati hozzáférést a Jegyző engedélyével lehet létesíteni, illetve igénybe venni. Hivatali munkavégzés céljára biztosított vezeték nélküli hálózat (minimum jelszavas védelemmel) ellátottan és a csatlakoztatható eszközök szűrésével létesíthető. A hivatali munkavégzés céljára biztosított vezeték nélküli hálózathoz kizárólag a Hivatal tulajdonát képező, a Hivatal által felügyelt mobil infokommunikációs eszköz csatlakoztatható.

Kivételt képez ez alól – amennyiben az adott telephelyen elérhető – a Hivatal által biztosított, a Hivatal hálózatáról leválasztott nyilvános hálózati hozzáférés (pl.: „vendég” wi-fi), amelyhez a Hivatal munkatársai is csatlakoztathatják saját mobil eszközeiket.

A Hivatal vezeték nélküli hálózati beállításainak kezelése, dokumentálása az IT üzemeltető feladata.

7.9. Távoli hozzáférés

Távoli hozzáférés – pl.: otthoni munkavégzés céljából – csak megfelelően biztonságos, titkosított adatátviteli csatorna használatán (pl.: VPN) keresztül, a Jegyző erre vonatkozó írásos engedélyével lehetséges! A szükséges beállításokat az IT üzemeltető végzi el.



7.10. Kártékony kódok elleni védelem, vírusriadó

A Hivatal minden interneteléréssel rendelkező munkaállomásán és a Hivatal által munkavégzés céljára biztosított mobil infokommunikációs eszközén (pl.: laptop, tablet, telefon, stb.) víruskereső programot kell működtetni, amelynek telepítése, biztonsági beállításainak konfigurálása az IT üzemeltető feladata.

Minden munkavállaló köteles a vírusvédelmi program által megjelenített riasztásról az IT üzemeltetőt haladéktalanul értesíteni.

Vírusfertőzés tényének fennállása esetén az IT üzemeltető jelzése nyomán a Jegyző kihirdeti a vírusriadó állapotot, s erről tájékoztatja a hivatali munkatársakat és az információbiztonsági felelőst.

A vírusriadó időtartama alatt minden munkavállaló köteles együttműködni a vírusfertőzés továbbterjedését, valamint a helyreállítási tevékenységeket érintően az IT üzemeltető, illetve az információbiztonsági felelős által meghatározott intézkedések (pl.: munkaállomások ideiglenes leállítása, internet használat felfüggesztése, stb.) végrehajtásában.

7.11. Számítógép újraindítása

Előfordulhat olyan eset, amikor a számítógépet újra kell indítani (pl.: egy biztonsági frissítés telepítését követően). Ehhez természetesen nem szükséges külön az informatikus szakembert odahívni, ezt az eszköz használatára feljogosított hivatali munkavállalóként Ön is végrehajthatja például, ha az informatikus megkéri erre vagy jelzi (akár telefonon, akár emailben), hogy tegye meg ezt.

7.12. Biztonsági mentések

A biztonsági mentések beállítása és rendszeres végrehajtása a dokumentált mentési rend alapján az IT üzemeltető feladata. A mentendő adatok meghatározásában részt vesz minden munkavállaló (pl.: helyi gépen tárolt kritikus fájlok, dokumentumokat jelezni kell az informatikus felé, hogy tudja, hogy azokat is menteni kell).

7.13. Együttműködésen alapuló számítástechnikai eszközök

A hivatali számítógépeken olyan, úgynevezett együttműködésen alapuló számítástechnikai eszközök, amelyek például kamera, webkamera vagy mikrofon használatával működnek (ilyen például a Skype, a Messenger, stb.) használata TILOS! Kivételt képezhet ez alól, s a Jegyző engedélyezheti az adott program működtetését, amennyiben az adott rendszer használata a hivatali munkavégzés céljából indokolt (pl.: ügyfelekkel való kapcsolattartás).

A funkciót biztosító eszközzel (alkalmazás, szoftver) szembeni követelmény, hogy közvetlen kijelzést nyújtson a távoli aktivitásról annak a felhasználónak, akik fizikailag jelen van az eszköznél (a gép előtt ül), azaz jelezze, hogy a webkamera vagy a mikrofon bekapcsolt állapotban van és a távoli partner láthatja és/vagy hallhatja, hogy mi történik a hivatali helyiségben.

8. Fizikai védelemmel kapcsolatos szabályok és feladatok

A Hivatal nyitvatartási idejében az ügyintézésre használt helyiségeibe, irodáiba az ügyfelek ügyintézési célból az ügyintézésben eljáró munkatárs szóbeli engedélyét (távirányítású ajtónyitó vagy elektronikus ügyfélkezelő, hívó rendszer alkalmazása esetén annak jelzését) követően léphetnek be.

Az ügyfelek elől elzárt területekre, köztük a Hivatal által használt EIR-ek elemeinek helyt adó helyiségekbe a látogatók és munkavégzés céljából a Hivatallal munkavégzésre irányuló szerződéses jogviszonyban álló személyek (pl.: üzemeltető, karbantartó, stb.) csak kísérettel léphetnek be és felügyelet mellett tartózkodhatnak ott.

A felügyelet biztosítása ügyfél esetében az ügyében eljáró ügyintéző, látogató és szerződéses partner esetében a Jegyző által ezzel megbízott munkavállaló feladata.

Nyitvatartási időn kívül a Hivatal épületeiben ügyfél, látogató vagy a Hivatal számára munkát végző, szerződött partner kizárólag a Jegyző erre vonatkozó külön írásos – rendkívüli, indokolt esetben szóbeli – engedélyével, s az általa e feladattal megbízott munkavállaló felügyelete mellett tartózkodhat. A nyitvatartási időn kívül történő belépési igényről – vészhelyzet, például tűzeset kivételével – a Jegyzőt minden esetben előzetesen tájékoztatni kell.

Minden munkatárs kötelessége, hogy a Hivatalban kialakított fizikai és elektronikus védelem elemeit (zárható nyílászárók, beléptető-, riasztó-, megfigyelő rendszerek, stb.) rendeltetésüknek és az IBSZ-ben meghatározott szabályoknak megfelelően használja.

Tilos a védelmi eszközök funkcionalitásának megváltoztatása, mint például:

- az automatikusan záródó, illetve a folyamatosan zárt állapotban tartandó nyílászárók, ajtók kitámasztása;
- az elektronikus védelmi rendszerek érzékelőinek (szenzor, kamera, stb.) letakarása, pozíciójának megváltoztatása (pl.: elforgatása) vagy leszerelése, megbontása.

A zárható helyiségek ajtóit azok elhagyását követően (ha nem tartózkodik már bent senki természetesen) minden alkalommal be kell zárni.

Minden munkatárs köteles ellenőrizni a felügyelete alatt álló hivatali helyiség nyílászáróinak megfelelő működését, zárhatóságát. Rendellenesen működő, nem zárható nyílászáró javításáról

haladéktalanul intézkedni kell, emiatt azt soron kívül jelezni köteles a hibát észlelő vagy arról értesülő munkatárs a Jegyző felé.

A környezeti károk megelőzése érdekében, például a víz-, és más, csővezetéken szállított anyag okozta kár elleni védelem biztosítása céljából a főelzárócsapok hozzáférhetőségét (helyét), működtetésének módját (hogyan kell elzárni) minden hivatali munkatárs köteles megismerni.

8.1. Fizikai belépési engedélyek

A Hivatal épületeibe belépésre jogosult hivatali munkavállalók és a Hivatallal munkavégzésre irányuló szerződéses jogviszonyban álló személyek listájának elkészítéséről és kezeléséről, valamint naprakész állapotban tartásáról a Jegyző gondoskodik (IBSZ melléklete: Belépésre jogosultak nyilvántartása). A Jegyző által jóváhagyott lista írásos belépési engedélynek minősül.

Belépésre jogosultak nyilvántartása

Hivatal megnevezése:	
Épület, telephely megnevezése, címe:	
Dátum:	

Név	**Beosztás**	**Szervezet** (belső: KÖH; külső: szervezet megnevezése)

A belépésre alkalmas nyílászárók kulcsainak, illetve a bejutáshoz szükséges további eszközök (pl.: egyéni belépőkártya, hozzáférési vagy riasztókód) védelméről a Hivatal az alábbi szabályok szerint gondoskodik:

a) a Hivatal épületeibe belépést lehetővé tevő kulcs, illetve egyéb eszköz kizárólag belépési engedéllyel rendelkező személynek, s dokumentált átadás-átvételi folyamat keretében adható ki (az átadás-átvételt igazoló dokumentum egy példányának megőrzése a Jegyző feladata);

b) a kulcsok és egyéb eszközök biztonságos kezeléséről, megőrzéséről az átvevő köteles gondoskodni;

c) egy-egy kulcspéldányt minden nyílászáró esetében letétbe kell helyezni a Jegyzőnél (mesterpéldány biztosítása);

d) a kulcs, egyéb eszköz elvesztése vagy ellopása, illetve a kód kompromittálódása biztonsági incidensnek minősül, amely esetben birtokosa haladéktalanul értesíteni köteles a Jegyzőt a szükséges intézkedések (zárszerkezet cseréje, kód visszavonása, megváltoztatása) megtétele érdekében;

e) azon hozzáférési kódok megváltoztatásáról, amelyek esetében év közben kilépő munkavállaló jogviszony változása vagy a d) pontban meghatározott biztonsági incidens bekövetkezése azt nem tette az év folyamán szükségessé a Jegyző köteles évente legalább egy alkalommal gondoskodni.

A belépésre jogosultak számára a Jegyző gondoskodik a Hivatalban rendszeresített további belépési jogosultságot igazoló dokumentum (pl.: kitűző, azonosító kártya, intelligens kártya) kibocsátásáról, valamint jogosultság, illetve jogviszonyt érintő változás esetén annak visszavonása, érvénytelenítése, törlése vagy megsemmisítése ügyében.

8.2. A fizikai belépés ellenőrzése és nyilvántartása

A Hivatal épületeinek ügyfelek, illetve látogatók számára biztosított bejáratain, valamint az ügyfelek és látogatók számára nyitott területein és az ügyintézésre használt, az ügyintéző munkatárs által felügyelt helyiségein kívül minden más be- és kilépésre alkalmas ajtót használaton kívül nyitvatartási időben is zárt állapotban kell tartani. A Hivatal ezzel biztosítja, hogy a belépésre jogosultak kizárólag az engedélyezett be-, és kilépési pontokon keresztül közlekedjenek, illetve haladhassanak át, továbbá csak azokba a helyiségekbe léphessenek be, ahol személyes felügyelet nélkül jogosultak tartózkodni.

Ha nincs a Hivatal épületében portaszolgálat, akkor a nem a Hivatal állományába tartozó személyek (ügyfelek, látogatók, a Hivatallal munkavégzésre irányuló szerződéses jogviszonyban álló üzemeltetők, karbantartók, stb.) belépésének adatait a felügyelet biztosító munkatárs köteles a belépési naplóban rögzíteni, az alábbi minta szerint.

Belépési napló

(A belépési naplót telephelyenként, naponta külön kötelező vezetni!)

Hivatal megnevezése:			
Épület, telephely megnevezése, címe:			
Dátum:			
Név	**Belépés időpontja:** (óra, perc)	**Kilépés időpontja:** (óra, perc)	**Belépés célja:** **Ü**: ügyfél ügyintézés; **L**: látogató (vendég); **SZ**: szerződött partner (pl.: IT üzemeltető, karbantartó)

8.3. Be- és kiszállítás, karbantartók felügyelete

A Hivatal által használt, felügyelete alá tartozó informatikai rendszerek és eszközök karbantartását kizárólag a Hivatallal e feladat ellátására vonatkozóan szerződéses jogviszonyban álló szervezetek, illetve személyek, s minden esetben csak felügyelet mellett végezhetik.

Amennyiben új informatikai eszköz vagy javításból visszahozott szállítása történik, akkor a be- és kiszállítás felügyeletét, figyelemmel kísérését a Hivatallal munkavégzésre irányuló szerződéses jogviszonyban álló személy felügyeletével megbízott munkatárs látja el, szakmai ellenőrzésében szükség szerint közreműködik az IT üzemeltető.

A be- és kiszállítások dokumentálása – az alábbi nyilvántartásba felvétele – a felügyeletet biztosító munkatárs feladata.

Információs rendszerelemek be- és kiszállításának nyilvántartása

(Telephelyenként vezetendő!)

Hivatal megnevezése:	
Épület, telephely megnevezése, címe:	

Dátum	**Hardver eszköz, rendszerelem megnevezése** (azonosító/sorozatszám/leltári szám – ha van!)	**Szállítás iránya** (jelölje X-el)		**Szállítást végző adatai** (Név/beosztás/szervezet)
		Be	**Ki**	

9. A biztonsági események kezelése, jelzése

A Hivatal által használt rendszerek bármely rendellenes vagy hibás működéséről, működési zavarairól vagy hibajelzéseiről lehetőség szerint elektronikus formában (email) – vagy ha az nem működik, akkor telefonon keresztül köteles tájékoztatni az IT üzemeltetőt, aki biztonsági incidens gyanújának felmerülése esetén köteles haladéktalanul tájékoztatni az információbiztonsági felelőst és a Jegyzőt.

Amennyiben a bekövetkezett esemény hatására a Hivatal által kezelt adatok bizalmassága, sértetlensége vagy rendelkezésre állása sérül vagy sérülhetett, akkor azt minden esetben biztonsági eseményként kell kezelni. Például ilyen lehet az adatok véletlen vagy szándékos törlése, az azokhoz való illetéktelen hozzáférés vagy egy zsarolóvírus által történő titkosításuk.

A bekövetkezett kár, illetve a veszélyhelyzet elhárításában, megszüntetésében az információbiztonsági felelős által javasolt és szükséges, illetve a Jegyző által meghatározott intézkedések végrehajtásában köteles együttműködni.

10.Üzletmenet-folytonossági terv

A Hivatalnak arra az esetre, ha bármilyen hiba miatt az általa használt informatikai rendszerek működése ellehetetlenül (pl.: leáll az internet szolgáltatás, meghibásodik a szerver vagy az ügymenetéhez kritikus programot futtató számítógép) tervet kell készítenie az ilyen helyzetek kezelésére, amennyiben lehetséges, akkor olyan elkerülő megoldásokkal, tartalék intézkedésekkel, amelyek a hiba elhárításáig lehetővé teszik valamilyen szinten a munkafolyamatok – például az ügyfélfogadás – biztosítását.

Ez az úgynevezett „Üzletmenet-folytonossági terv” szintén az IBSZ melléklete, vészhelyzet esetén, amikor a Jegyző elrendeli, akkor az ebben foglalt intézkedések szerint kell eljárni. A tervet minden hivatali munkavállalónak ismernie kell, aki a végrehajtásában bármilyen módon érintett (szerepel a tervben nevesítve vagy munkaköre alapján), s erről nyilatkozatot is kell tennie.

Hibák, informatikai erőforrás kiesések jelzése

Fentieken kívül az a feladata, hogy amennyiben olyan esemény következik be, amely a Hivatal munkavégzéshez szükséges informatikai eszközöket, illetve rendszereit részben vagy teljesen működésképtelenné teszi, a Jegyzőt haladéktalanul értesítse.

11.Személybiztonsági feltételek

A Hivatal által használt informatikai rendszerekhez, EIR-ekhez hozzáféréssel rendelkező munkatársak biztonsági szempontból azonos követelményeknek kell, hogy megfeleljenek. A munkaköri alkalmassági követelményeknek történő megfelelés, a munkavégzésükre vonatkozó hivatali előírások, szabályozók, illetve eljárásrendek megismerése és maradéktalan betartása, valamint a titoktartási nyilatkozatban vállalt felelősségük képezik a biztonsági besorolásuknak megfelelő kötelezettségek alapját, az ezzel kapcsolatos garanciális feltételeket.

A Hivatal informatikai rendszereihez, illetve kezelt adataihoz történő hozzáférés biztosítása, a tényleges munkavégzés megkezdése előtt köteles a munkaköri feladatellátását érintő előírások, szabályozók, illetve eljárásrendek megismerésével és betartásával kapcsolatos felelősségéről a jogviszonyt megalapozó szerződés aláírásával, valamint titoktartási kötelezettségéről (egyes esetekben, mint például az ASP rendszereivel kapcsolatban a központi előírásoknak megfelelően külön) nyilatkozatot tenni.

11.1. Eljárás a jogviszony megszűnésekor

Munkaviszonyának megszűnése esetén az informatikai rendszerekhez kapott jogosultságok megszüntetésre kerülnek, továbbá köteles a kapott, a Hivatal tulajdonát képező minden eszköz (pl.: infokommunikációs eszközök, belépőkártya, kulcsok, hitelesítési eszközök, hozzáférési kódok, stb.) visszaadására legkésőbb a munkavégzés alóli felmentésének időpontjában. A munkakör átadását-átvételét minden esetben dokumentáltan, jegyzőkönyvben rögzítetten kell megtenni.

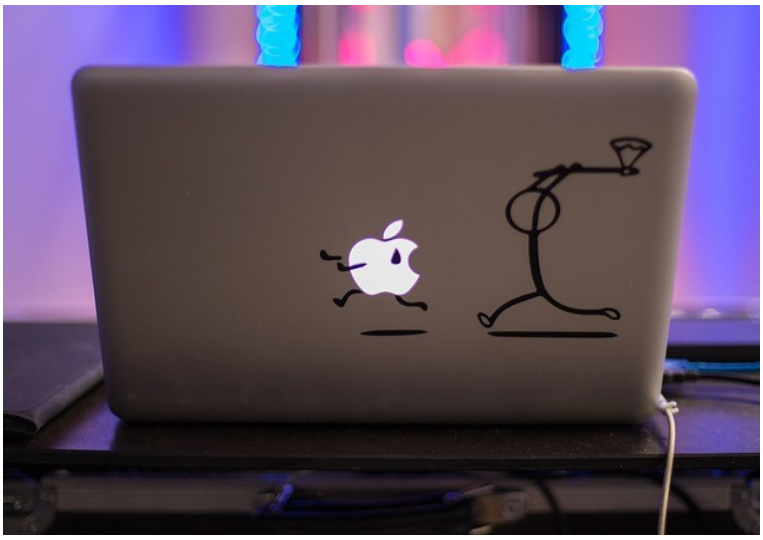
11.2. Az áthelyezések, átirányítások és kirendelések kezelése

Munkakörének vagy feladatainak megváltozása, illetve áthelyezése, átirányítása esetében az előző, a jogviszony megszűnésére vonatkozó szabályokat az alábbi eltérésekkel kell alkalmazni:

Az új munka-, illetve feladatkör által nem igényelt korábbi, meglévő fizikai és logikai hozzáférések megszüntetését, illetve az áthelyezés miatt megváltozott hozzáférési engedélyek módosítását vagy megszüntetését, továbbá az ahhoz nem szükséges eszközök visszavételét követően a Jegyző feladata gondoskodni arról, hogy a használandó, új rendszerek és azokhoz szükséges jogosultságok, hozzáférések beállítása, valamint a kapcsolódó felhasználói fiókok létrehozása, módosítása, illetve indokolt esetben törlése megtörténjen.

11.3. Fegyelmi intézkedések

A biztonsági szabályok szándékos megsértőivel szemben a Hivatal fegyelmi eljárást indít. Ha felmerül a lehetősége annak, hogy a biztonsági eseményt kiváltó ok számítógépes bűncselekmény elkövetéséhez kötődik, abban az esetben a Hivatal jogi képviselője, valamint a Jegyző jogosult büntetőjogi feljelentést is tenni.



12.Tudatosság és képzés

Minden hivatali munkatárs köteles részt venni az információbiztonsággal kapcsolatos számára előírt képzéseken, évente legalább egy alkalommal.

A képzésekről dokumentáció, jelenléti ív készül.

12.1. Kapcsolattartás az elektronikus információbiztonság jogszabályban meghatározott szervezetrendszerével és az e célt szolgáló ágazati szervezetekkel

Az elektronikus információbiztonság jogszabályban meghatározott szervezetrendszerével való kapcsolattartás – a Hivatal számára az Ibtv.-ben, illetve kapcsolódó rendeleteiben előírt bejelentési és adatszolgáltatási kötelezettségek teljesítésének kivételével – elsődlegesen az IBF feladata és felelőssége.

Ennek keretében a Nemzeti Kibervédelmi Intézeten (NKI) belül működő felügyeleti hatóság (NEIH: Nemzeti Elektronikus Információbiztonság Hatóság), illetve a Kormányzati Eseménykezelő Központ (GovCert) által kiadott biztonságtudatosító, ismeretterjesztő és oktatóanyagokra felhívja a Hivatal munkatársainak figyelmét, illetve számukra elérhetővé teszi azokat folyamatos oktatásuk, képzésük elősegítése érdekében, továbbá jelzi az aktuális, a Hivatal által használt rendszereket érintő fenyegetésekre, sebezhetőségekre és biztonsági eseményekre vonatkozó legfrissebb információkat, az e szervezetek által kiadott biztonsági riasztásokat a Hivatal, illetve az IT üzemeltető felé.