# Kedves Pedagógusok!

Az alábbi leírásban ismertetem a RRF-1.2.1-2021-2021-00001 (továbbiakban RRF-1.2.1) azonosító számú „Digitális oktatáshoz való egyenlő hozzáférés feltételeinek biztosítása a tanulók és a pedagógusok számára" című projekt keretében kapott notebookon esetlegesen bekapcsolt „BitLocker-titkosítás” kezeléséhez.

### Mi a célja ennek a leírásnak?

A cél a figyelemfelhívás a RRF-1.2.1 projekt keretében kapott notebookokon esetlegesen nem direkt aktivált BitLocker-titkosítás használatára, tudnivalóira. Figyelmen kívül hagyása adatvesztést okozhat az alábbi esetekben:

- garanciális javítás
- hitelesítőadatok elvesztése, elfelejtett jelszó

A BitLocker olyan esetekben aktiválódhat automatikusan, amikor Microsoft fiókkal üzemeltük be a számítógépet (nem offline fiókkal), illetve később adtuk hozzá a rendszerhez a saját Microsoft fiókunkat. Lentebb ellenőrizheti, hogy Önnél be van-e kapcsolva ez a funkció.

### Mire szolgál a BitLocker-titkosítás?

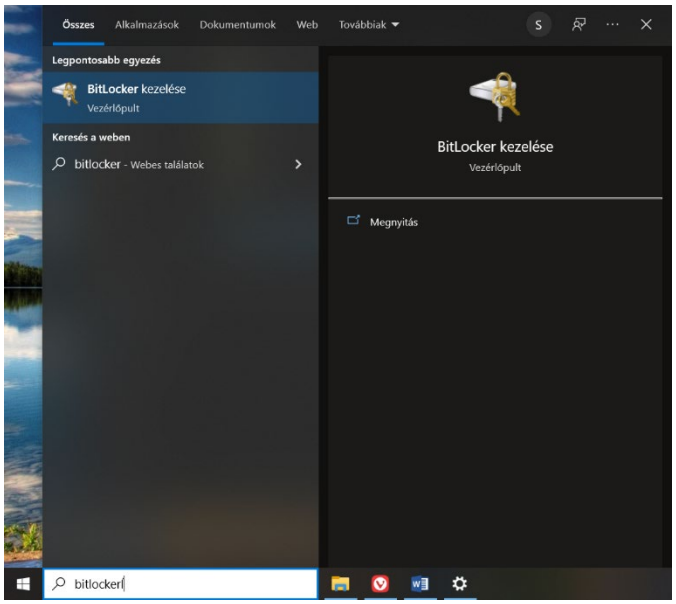
„Az adatokhoz való hozzáférés általában a Windowson keresztül történik, és a szokásos védelmi beállításokat biztosítja a Windowsba való bejelentkezéshez. Ha valaki meg szeretné kerülni ezeket a Windows-védelmeket, megnyithatja a számítógép házát, és eltávolíthatja a fizikai merevlemezt. Ezután, ha a merevlemezt egy általa vezérelt gép második meghajtójaként adja hozzá, előfordulhat, hogy anélkül férhet hozzá az adataihoz, hogy az Ön hitelesítő adataira lenne szüksége.

Ha azonban a meghajtó titkosítva van, amikor ezzel a módszerrel próbálja elérni a meghajtót, meg kell adnia a visszafejtési kulcsot (amellyel nem kellene rendelkeznie), hogy hozzáférhessen a meghajtón tárolt adatokhoz. A visszafejtési kulcs nélkül a meghajtón található adatok halandzsának fognak tűnni neki.”

Idézet az alábbi hivatalos Microsoft ügyféltámogatási oldalról: Link

### Hogyan lehet megállapítani, hogy aktív-e a BitLocker-titkosítás?

Legegyszerűbb módon a bal alsó sarokban lévő keresőmezőbe, illetve Start menüt megnyitva beírjuk, hogy „bitlocker”, és a „BitLocker kezelése” menüpontot megnyitjuk. Ha ott azt látjuk, hogy a „BitLocker bekapcsolva”, akkor kérem, hogy olvassanak tovább.




### Bekapcsolt BitLocker-titkosítás esetén

Három különböző módja van, hogy kezeljük az adatainkat:

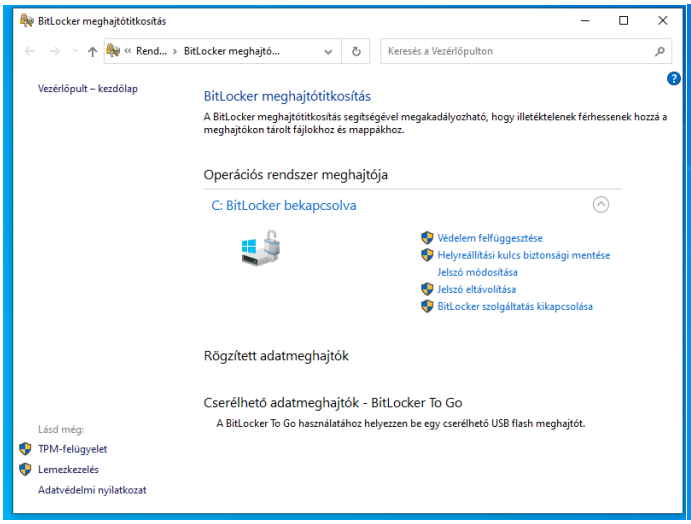
1. Microsoft fiók alkalmazása
2. helyreállító kulcs elmentése
3. BitLocker-titkosítás kikapcsolása

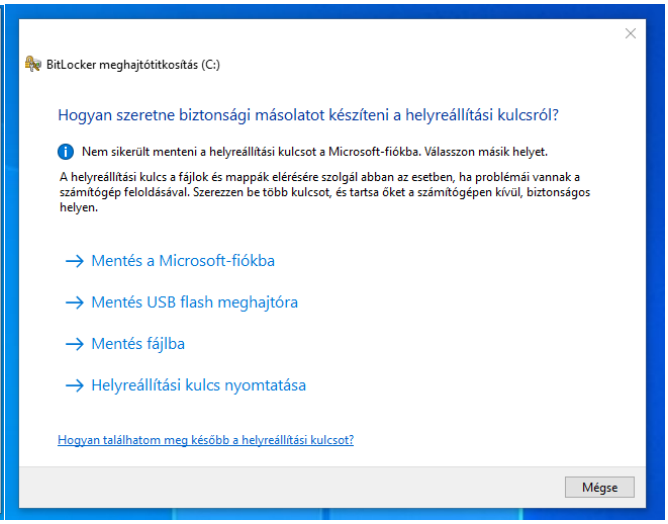
**Microsoft fiók alkalmazása**

Microsoft-fiók alkalmazása esetén a helyreállító kulcs automatikusan el van mentve az említett fiókban online. Ugyanezen fiókkal való bejelentkezéskor automatikusan feloldja a zárolt számítógépet.

**Helyreállító kulcs elmentése**

A „BitLocker kezelése” beállításoknál maradva a meghajtó ikonja mellett jobbról található a „Helyreállítási kulcs biztonsági mentése” hivatkozás. Arra kattintva különböző opciók találhatók, melyből a szimpatikusabb megoldást választva elmenthetik a helyreállítási kulcsot, így biztonságban tudhatják adataikat esetleges garanciális javítás esetén.




**BitLocker-titkosítás kikapcsolása**

Szintúgy a „BitLocker kezelése” beállításoknál maradva a meghajtó ikonja mellett jobbról található „BitLocker szolgáltatás kikapcsolása” lehetőséget választjuk ki, így a titkosítás megszüntetésre kerül. A szolgáltatás kikapcsolása olyan veszéllyel járhat, hogy a notebook ellopása esetén adatszivárgás történik a titkosítatlan adatok végett.

Remélem, hogy ez a leírás hozzásegíti Önöket a biztonságosabb munkavégzéshez, és az adatvesztések elkerülését.

További jó munkát kívánok!

**Szabó András**
Informatikai ügyintéző
**Informatikai és Pályázati Osztály**
**Monori Tankerületi Központ**
2200 Monor, Petőfi Sándor u. 28.
Mobil: +36307498446
E-mail: andras.szabo@kk.gov.hu