# USB Flash / Thumb Drive Recommendations

**We are often asked for our advice regarding securing information on a USB flash drive. Our first response to this is that USB flash drives should NOT be used to store, exchange or transport sensitive information unless there is no other option. If you have no other option, then below are our recommendations for how to ensure your data remains protected. The first two options that utilize a keypad built-in to the USB device are the most secure and most versatile, but also the most expensive.**

**IMPORTANT!**

You should never rely on a USB flash drive as your sole data source. ALWAYS have a copy of your data stored securely in another location. In addition to being easily lost or stolen, USB flash drives can a do fail. Often they can be working fine one minute and the next they are completely inaccessible and your data is lost.

| USB Device | Pros / Features | Cons |
|---|---|---|
| **Apricorn Aegis Secure Key**<br>  | • Works in any system that reads USB drives<br>• No software needs to be installed on the host system<br>• FIPS 140-2 Level 3 certified<br>• Auto-lock secures your data as soon as the drive is removed from the computer<br>• Auto self-destruct deletes all data if incorrect PIN is entered 10 consecutive times | • Expensive<br>• With the introduction of additional circuitry and a rechargeable battery, there are more points of failure |
| **Kingtson DataTraveler 2000**<br>  | • Works in any system that reads USB drives<br>• No software needs to be installed on the host system<br>• FIPS 197 certified<br>• Auto-lock secures your data as soon as the drive is removed from the computer<br>• Auto self-destruct deletes all data if incorrect PIN is entered 10 consecutive times | • Expensive<br>• With the introduction of additional circuitry and a rechargeable battery, there are more points of failure |
| **Kingston DataTraveler Vault Privacy**<br>  | • Works with Windows 7 and higher, Mac OS X 10.9 and higher, Linux v2.6.x<br>• FIPS 197 certified | • Moderately expensive<br>• Must run software on the host to unlock the drive |
| **BitLocker Encryption of any standard USB flash drive**<br>  | • Very cheap<br>• Any Windows compatible USB drive of any size can be used<br>• While not FIPS compliant, still fairly secure and sufficient for most data that does not contain PII or PHI | • Only compatible with Windows-based machines<br>• Not FIPS compliant by default and not easy to enable<br>• NOT acceptable for PII or PHI data |

Unknown macro: 'hideelements-macro'