University of Florida
Encrypted USB Trade-In

"All portable storage devices must include built-in encryption. The only exceptions to this are for specific uses where no Restricted Data will be stored and encryption would interfere with the device's intended use."

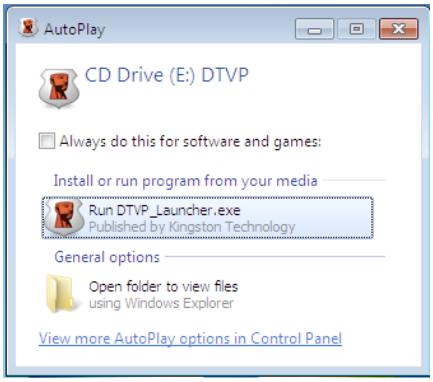
UF Mobile Computer and Storages Devices security standard
http://www.it.ufl.edu/policies/mobilecomputingstandard.html

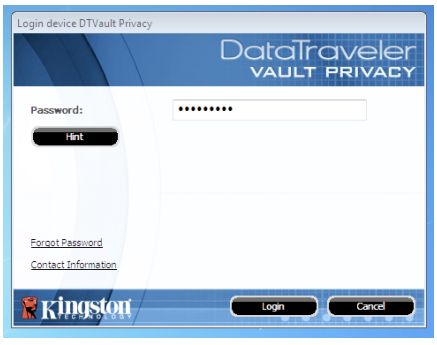
In order to help implement the new requirement for encrypted portable storage, the university has funded the purchase of a number of hardware encrypted USB drives. These drives are to replace current un-encrypted drives you are already using. In order to become compliant with the new standard, you need to discontinue use (destroy if they hold Restricted data) of any un-encrypted devices and use only encrypted drives.

Using your new encrypted USB drive

1. Insert the drive into a USB slot on your computer. In Windows, the application should launch automatically. If it does not, open the DTVP drive and double click on 'DTVP_Launcher.exe'. On Macs, open the DTVP drive, double click the 'Mac' folder, and double click on 'DTVP.app' . The DTVP drive will appear to be a CD, and no data can be stored on it.
2. For your very first use, you will need to initialize the drive and create a password. Please use a strong password that is at least 8 characters long and includes numbers and special characters.
3. You will now have a new drive labeled 'Kingston' which is your encrypted drive where you will store data.
4. Be sure to eject your drive before removing it from your computer. On Windows, do this by selecting the DTVault application from the taskbar and choosing 'Shutdown DTVault Privacy'. On a Mac, right- (or Control-) click on the DTVP icon in the Dock and select 'Quit'.
5. Every time you connect your drive to a computer, you will need to open the DTVP app and enter your password.

For additional instructions, visit http://security.ufl.edu/usb





Office of Information Security and Compliance
UNIVERSITY of FLORIDA

http://security.ufl.edu

Q: If I won't place any Restricted data on a flash drive, and typing a password will interfere with my use by making it less convenient, can I just use an un-encrypted USB drive?
A: The intent of the UF policy and standard is that all storage devices will be encrypted. The exception is for very limited cases in which the system cannot function with encryption, such as memory cards in digital cameras or devices used to boot a computer for repair or maintenance.

Q: What is Restricted data?
A: "Data in any format collected, developed, maintained or managed by or on behalf of the University, or within the scope of University activities, that are subject to specific protections under federal or state law or regulations or under applicable contracts."

Policies on Restricted Data
http://regulations.ufl.edu/chapter1/10103.pdf

Examples include, medical records, social security numbers, credit card numbers, Florida driver licenses, non-directory student records, some research protocols and export controlled technical data.

Q: Why am I required to encrypt all data, even when I don't plan on storing any Restricted data?
A: Computer is equipment is lost and stolen every day, and data breaches happen far to often. It is UF's duty to protect the information entrusted to it. Failure to do so could result in significant financial penalties, loss of grants and contracts, damage to our reputation, and harm to people whose data was disclosed. Internal audits have found Restricted data stored in many places it was not intended to be (and where the owners insisted it wouldn't be). To to be sure, we must protect the most vulnerable places data can be stored.

Q: What about external hard drives?
A: When purchasing new drivers, every attempt should be made to acquire hardware encrypted models. Drives currently in use can be encrypted with software. Contact your IT support for additional information.

Q: Can I use a different model of encrypted USB drive?
A: Yes, as long as it is fully encrypted, and there is a no way to store un-encrypted data on it. Contact your IT support for additional guidance.

Q: What about Linux compatibility?
A: The most current Kingston models support several versions of Linux. Our testing has also found that the Ironkey has very good support for Linux. These can be ordered from many online computer suppliers.

Q: How can I get additional drives?
A: Kingston Data Traveler Vault Privacy drives can be purchased at the UF bookstores. UF has arranged special pricing from Kingston for bulk purchases. Information is available at http://security.ufl.edu/usb