Data & Assets

User Responsibilities

What does the Device DCS cover?

Laptops, desktops, tablets, smartphones, flash drives and other portable storage drives used for work purposes regardless of ownership.

What do I need to do to comply?

Step 1: Determine which data classification level applies to the data on your device(s). See the DCS cheat sheet or the UM DCS definitions.
Step 2: Inform your IT support staff of the DCS level that aligns with your device(s).
Step 3: Your IT professional is responsible for ensuring your device(s) is deployed, configured and managed in accordance with the Device DCS.
Step 4:

Do not use a flash drive if you don't know where it came from (it could hold a virus).
For personal devices, keep the operating system and applications current.
Encrypt personal devices, including flash drives, that hold DCL4 data. If you own a device that can't be encrypted, you should not store DCL4 data on it.
Do not download suspicious or obscure applications onto your computer and never click on links in emails.
Use

		Applicable laws (not exhaustive): FERPA, GLBA, Federal Trade Commission regulations on identity theft protection	Missouri Breach Law, federal export control laws