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 common sense and best practices when traveling, especially when traveling overseas.

Note: If your University-issued computer is not managed by an IT professional or if it uses a non-standard operating system such as Linux, consult with your campus IT division and/or with your campus Information Security Officer.

DCL Cheat Sheet

The creator/manager (e.g., data custodian) of information and data has the latitude to classify data at a level higher than the definitions below. However, data/information cannot be classified at a lower level than the definitions below unless approved by your **ISO**.

DCL CHEAT SHEET GUIDELINES	
DCL1: **Public Data**	**DCL2:**
Most Web page content	
Policies	
Meeting agendas and minutes	
Strategic plans	
Marketing messages	

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