Data & Assets

Device DCS Guidelines

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:** You are responsible for the following:
    - Keep portable devices physically secure.
    - Lock your screen/device when not in use.
    - When connecting to your campus network or campus resources, use VPN or other secure remote access services as deemed appropriate by your campus IT department.
    - Do not share your password with anyone and do not use your University password on non-University web sites or other accounts.
    - Put a PIN or pattern on portable devices such as your smartphone and iPad.
    - Make sure your device is disposed of properly. For University-owned devices, give your aged device to your IT support staff. For personal devices, make sure they are wiped before disposal.
    - Do not disable the firewall or antivirus.
    - Use mapped network drives or collaboration applications provided by your campus to store work files rather than storing files exclusively on your workstation (protects against device failure).
    - Do not join unsecure wireless networks when working or, if you must use such networks, use VPN or other secure remote access services.
    - Report the loss or theft of a device, regardless of ownership, to your campus police department, your IT support person and to your campus Information Security Office.

Additional steps you can take to secure devices both at work and at home:

- Do not make online purchases or other financial transactions over a publicly-available wireless network.

- 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: Sensitive Data**	**DCL3: Restricted Data**	**DCL4: Highly Restricted Data**
Most Web page content	Internal memos	Non-directory student information	Social Security Numbers
Policies	Procedures	Financial aid information	Patient information
Meeting agendas and minutes	Budgets	Donor information	Credit card numbers
Strategic plans	Business emails and other correspondence	Job candidate resumes and applications	Biometric data
Marketing messages	Project plans	Personnel evaluations and other HR-related information such as EMPLID	Passwords
	Drafts	Some forms of intellectual property and unpublished research	Intellectual property including information and data with commercial value
		Floor plans, diagrams, etc.	Information/data affected by federal export control regulations
		Birthdates and other personal information	Documentation about critical infrastructures (floor plans, power systems, diagrams, etc.)
			Applicable laws and standards (not exhaustive): HIPAA, Payment Card Industry (PCI),

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