Use of Personal / Un-Managed Devices for Work

Statement and Purpose

There are many state and federal regulations that govern the handling, usage and security of sensitive data stewarded by the University. If you use a personally-owned computer or a University-owned computer not managed by CIS for University work then **you are responsible for properly securing it** in accordance with University policy to comply with federal and state data privacy regulations.

If you use a University-managed computer issued to you by CIS, then your security settings are managed for you.

> ⚠ Data classified as *Restricted* or *Confidential* may not be stored on a personal or un-managed devices.

Data classified as *Internal* or higher shall be accessed or maintained on personally owned devices only when necessary for the performance of University-related duties and activities. University employees shall take all required, reasonable, and prudent actions necessary to ensure the security and retention of sensitive institutional data.

Regardless of the presence of sensitive or regulated Institutional Data, your computer may contain personal and private information, such as financial or medical information, notes, photos, contacts, documents, or saved passwords, that you wish to protect from theft or accidental loss. As such, taking security precautions as described below also safeguards your personal information.

Download Policy as PDF

Entities Affected By This Policy

All University employees.

Reason for Policy

This policy directs members of the University community who access or maintain sensitive Institutional Data to meet their shared obligation and responsibility to secure such data by properly self-managing the privacy and security settings on their personally owned device.

Table of Contents

- Statement and Purpose
  - Reason for Policy
- Permission to Use Un-Managed Devices
- Device Security
  - Personal Computers Best Practices
  - Mobile Devices
  - USB Stick / External Storage
- Records Requests and eDiscovery
- Data Return / Deletion
- Incident Reporting
- Enforcement
- Related Policies and Procedures

Policy Version: *1.0*

Responsible Office: *Computer and Information Systems*
Responsible Executive: *AVP for Information Technology*

Effective Date: *July 1, 2019*
Last Updated: *July 1, 2019*

Permission to Use Un-Managed Devices

Departments shall decide on a unit-by-unit basis whether to allow University employees, agents, affiliates or workforce members to use personally owned devices to access or maintain sensitive Institutional Data. Deans and department heads authorizing the use of personal devices are responsible to communicate the boundaries of personal use and raise awareness of appropriate regulations and risk.

Device Security

University employees shall maintain up-to-date, device-appropriate security safeguards and follow the policies, standards, and guidance provided by the University, as well as comply with appropriate safeguards required by state and federal regulations. In addition, the University or individual units may require that specific security settings and/or software be put in place and maintained on the device to protect sensitive Institutional Data.

Most regulations require the securing of devices used to store data. Securing your devices doesn't just mean keeping them in a safe place. It means setting a strong password, encrypting file storage, keeping your software up-to-date, backing up your data, choosing appropriate privacy and access settings, deciding what networks to connect to, and more.

> ⓘ See the Regulated Data Chart to see which systems and platforms are compliant for storing Regulated Data.

Personal Computers Best Practices

- **Encrypt File Storage** of your personal computer to protect sensitive data in the event the device is lost or stolen
- **Keep your operating system and other software up-to-date.** Software updates include patches for newly identified vulnerabilities and other important security updates.

- **Back up your data**. Computer hardware wears out or fails. Devices can be lost or stolen. The University offers several file storage options, including OneDrive for Business, that you can use. Check the Regulated Data Chart to see which services are appropriate for certain types of sensitive data. Institutional Data must be backed up or stored on protected University provided services.
- **Choose web browser security settings** that protect your privacy and enhance security.
- **Put a sticker on your computer** with your name and contact information so somebody who finds your lost computer can reach you.
- **Travel safely with technology.** Protect your privacy and the University's sensitive data when you're away from home. Don't leave devices unattended in unsecured locations like your car or public spaces.
- **Use anti-virus software**. Use anti-virus and anti-malware software to protect your personally-owned computer.

Mobile Devices

All mobile devices accessing University employee email are required to have a pass-code or use bio-metric security (finger print, facial-recognition, etc) enabled to protect against unauthorized access.

USB Stick / External Storage

All external storage containing Institutional Data classified as *Internal* or higher must be encrypted to prevent exposure of sensitive data.

Records Requests and eDiscovery

Records or data maintained by the University or University employees and affiliates may be the subject of document requests (e.g., Freedom of Information Act or Family Educational Rights and Privacy Act) or document production (e.g., warrants, subpoenas, court orders, etc.). University employees, agents and affiliates must produce these records or data (or the devices on which they are stored) upon request of the University.

In the course of an incident investigation, the University reserves the right to inspect any personally owned device that accesses or maintains sensitive Institutional Data. Any access to a personally owned device will be carried out in accordance with other relevant University protocols, and legal or law enforcement requirements.

⚠ Any records request requires the written approval of the president, the provost, or the area vice president.

Data Return / Deletion

Users shall return or delete Institutional Data maintained on personally owned devices upon request from the University or when their role or employment status changes such that they are no longer an authorized user of that data.

Incident Reporting

Devices that access or maintain sensitive Institutional Data and that are lost, stolen, have been subject to unauthorized access, or otherwise compromised must be reported to Computer and Information Systems or the Office of Risk Management within 24 hours.

Enforcement

The University characterizes certain activities related to misuse of sensitive data as unethical and unacceptable. Violations of this policy may result in disciplinary action up to and including restricting the ability to use a personally owned device for work-related activities, lost of data and systems access, dismissal, and/or legal action.

Related Policies and Procedures

Computer and Information Systems • Data Classification Levels • Data Laws and Regulations • Data Regulatory Compliance • Handling Confidential Data • Institutional Data Policy • Meet the Staff • Regulated Data • Regulated Data Chart