SPG U-M Standard Practice Guide

UNIVERSITY OF MICHIGAN

Standard Practice Guide Policies

Security of Personally Owned Devices That Access or Maintain Sensitive Institutional Data

601.33

Applies to: All Faculty and Staff

I. Overview

When conducting University activities, it may at times be necessary for University employees, agents, affiliates or workforce members to access or maintain *sensitive institutional data* on *personally owned devices*. There is often risk of data loss or unauthorized access when sensitive data is accessed or maintained via self-managed personally owned devices.

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.

II. Policy

Sensitive institutional data 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.

A. Permission to Use Personally Owned Devices

Units 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.

B. Device Security

University employees, agents, affiliates and workforce members 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 to protect sensitive institutional data be put in place and maintained on the device.

C. Data Return/Deletion

Users shall return or delete sensitive 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.

D. Incident Reporting

Personally owned 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 within 24 hours per SPG 601.25, Information Security Incident Reporting Policy.

E. Device Inspection

In the course of an incident investigation, the University reserves the right to inspect a personally owned device that accesses or maintains sensitive institutional data. Any access to a personally owned device will be carried out inaccordance with SPG 601.11, Privacy and the Need to Monitor and Access Records, as well as follow other relevant University protocols, and legal or law enforcement requirements.

F. Response to Document Requests and Production

Records or data maintained by the University or University employees, agents, workforce members, 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.

III. Applicability

This policy is applicable to any member of the University community including affiliates, whether housed at the University or elsewhere. In accordance with SPG 601.07, Responsible Use of Information Resources, 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, non-reappointment, discharge, dismissal, and/or legal action. Disciplinary action for faculty and staff, if any, for violation of this policy shall be consistent with the University Standard Practice Guides and the Bylaws of the Regents of the University.

IV. Definitions

Device: For purposes of this SPG, a device is defined as an object with the ability to engage in computational operations, including the accessing or storing of electronic data.

Sensitive Institutional Data: SPG 601.12, Institutional Data Resource Management Policy, defines sensitive institutional data as follows:

Institutional data is data that satisfies one or more of the following criteria:

- It is relevant to planning, managing, operating, controlling, or auditing administrative functions of an administrative or academic unit of the University;
- It is created, received, maintained, or transmitted as a result of educational, clinical, research or patient care activities;
- It is generally referenced or required for use by more than one organizational unit;
- It is included in an official University administrative report;
- It is used to derive an element that meets the criteria above;
- It is generated by a University workforce member or agent using any of the above data.

Sensitive data is defined as information whose unauthorized disclosure may have serious adverse effect on the University's reputation, resources, services, or individuals. It includes information protected under federal or state regulations or subject to proprietary, ethical, or privacy considerations.

Personally owned: For purposes of this SPG, *personally owned* includes devices for which a user receives a university subsidy or stipend as well as those wholly owned by the employee.

File Attachments

Printable PDF of SPG 601x33 (http://spg.umich.edu/sites/default/files/601x33.pdf)

SPG Number:
601.33

Applies To:
All Faculty and Staff

Date Issued:
June 30, 2013

Owner:
Provost and Executive Vice President for Academic Affairs, Executive Vice President and Chief Financial Officer, Executive Vice President for Medical Affairs, and Vice President for Research

Next Review Date:
June 30, 2018

Primary Contact:
Office of the CIO

Related Policies:
Defense and Indemnification (/policy/601.09)
Information Security Incident Reporting (/policy/601.25)
Information Security Policy (/policy/601.27)
Institutional Data Resource Management Policy (/policy/601.12)
Responsible Use of Information Resources (/policy/601.07)
Tech Tools: Cell Phones and Portable Electronic Resources (/policy/514.04)

Related Links:
Sensitive Regulated Data: Permitted and Restricted Uses Standard (http://cio.umich.edu/policy/sensitive-regulated-data.php)
Information Technology Policies and Standards (http://cio.umich.edu/policy)