What to Consider When Implementing SPG 601.33 in Your Unit

Accessing or Maintaining Sensitive Institutional Data on Personally Owned Devices (SPG 601.33)
• **Why U-M needed a policy**
  - Personal devices used widely
  - Risks of using personal devices

• **What the policy covers**
  - SPG 601.33 overview
  - Who is affected

• **Units/Departments can customize implementation**
  - Discretion to decide
  - Leadership responsibilities
  - Online toolkit guides decisions
  - 1. What sensitive data is used in your unit?
  - 2. Who works with sensitive data in your unit?
  - 3. Additional restrictions needed for your unit?

• **Impact on individuals**
  - Responsibilities of individuals
  - Device management expectations
  - Network use expectations
  - Security settings expectations

• **Implementation support**
• People increasingly use their own devices (smartphones, tablets, laptops, etc.) to access and work university data and IT resources—including sensitive institutional data.

• It’s convenient for individuals and can be more efficient for the university.
Risks of using personal devices

- 3.1 million cellphones stolen in 2013 (2014).
- Coca-Cola: Unencrypted laptops stolen, containing names, SSNs, addresses, drivers license numbers on 74,000 people. (2014).
- 2.47 million **new mobile malware** samples collected by McAfee (2013).
- Horizon Blue Cross Blue Shield: Unencrypted laptops stolen, containing a mix of sensitive information on nearly 840,000 people. (2013).
- 12,000 laptops lost or left behind in airports every week (2012).
- Americans lost **$30 billion worth of cellphones** (2011).
Security of Personally Owned Devices That Access or Maintain Sensitive Institutional Data (SPG 601.33)

• Recognizes the **beneficial use** of personally owned devices at U-M and the **associated risks**.

• Outlines **individual and departmental responsibilities** that appropriately balance personal privacy and institutional data security.

• Supports **Tech Tools: Cell Phones and Portable Electronic Resources** (SPG 514.04).
Who is affected

● **Data Stewards**, who decided that units can permit individuals to use their own devices to work with the sensitive data for which they are responsible with these exceptions: credit card or Payment Card Industry (PCI) information, export controlled research, and security camera data.

● **Unit Leadership**, who need to decide whether to be more restrictive in their units regarding the use of personally owned devices that work with sensitive institutional data.

● **Individuals**, who may be permitted, for business reasons, to use their own devices to work with sensitive institutional data. This includes devices wholly owned by the individual or for which they receive a U-M stipend.
Decision Needed: Will your unit be more restrictive than the expectations and responsibilities laid out in the SPG?

Unit/Department leaders have the discretion to decide

- Whether there should be additional unit-specific expectations or restrictions for users who work with sensitive institutional data on properly secured, personally owned devices.

These restrictions are in addition to the user responsibilities and expectations outlined in *Security of Personally-Owned Devices that Access or Maintain Sensitive Institutional Data* (SPG 601.33) and its supporting documentation.
1. **Decide whether to permit** people in their department/unit to use their own devices to access or maintain sensitive institutional data in accordance with SPG 601.33.

2. **If Yes, decide whether to impose additional restrictions.**
   - *Example 1:* Only permit people in specific roles to use their personal devices to work with sensitive institutional data.
   - *Example 2:* Require additional specific technical safeguards; require education and awareness.

   **If No, go on to step 3 and communicate the decision.**

3. **Inform those in the department/unit** whether they are permitted to use personally owned devices to access or maintain sensitive institutional data and whether there are additional restrictions.

4. **Document** the decision and any additional restrictions.
This **toolkit** walks you through the risk-based decision-making process of implementing SPG 601.33 in your department/unit.

http://safecomputing.umich.edu/protect-um-data/personal-devices/
1. What sensitive data is used?

• **What sensitive data** does your department/unit use?
  • Is it regulated or unregulated?
  • **How severe is the harm or the penalty** if there is unauthorized disclosure?

• **Decision tools:**
  • [Sensitive Data Guide](#)
  • [Sensitive Data Policies and Regulatory Compliance](#)
  • [Sensitive University Data](#)

**Hypothetical examples:**

<table>
<thead>
<tr>
<th>Unit</th>
<th>Data Type</th>
<th>Regulated?</th>
<th>Potential Harm</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Counsel</td>
<td>Attorney/Client Privileged</td>
<td>No</td>
<td>Low-High</td>
</tr>
<tr>
<td>Registrar</td>
<td>Student Educational Records</td>
<td>Yes - FERPA</td>
<td>Low-Medium</td>
</tr>
<tr>
<td>Health System</td>
<td>Protected Health Information</td>
<td>Yes - HIPAA</td>
<td>High</td>
</tr>
</tbody>
</table>
2. Who works with sensitive data?

• **Who works with sensitive data** in your department/unit?*
  - Almost all users?
  - Only a subset?

• Do all users work with the **same type of sensitive data**?

• Do some work with **more highly regulated sensitive data** than others?

**Hypothetical examples:**

<table>
<thead>
<tr>
<th>Unit</th>
<th>Data Type</th>
<th>Regulated?</th>
<th>User Base</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Counsel</td>
<td>Attorney/Client Privileged</td>
<td>No</td>
<td>All</td>
</tr>
<tr>
<td>Registrar</td>
<td>Student Educational Records</td>
<td>Yes - FERPA</td>
<td>All</td>
</tr>
<tr>
<td>Health System</td>
<td>Protected Health Information</td>
<td>Yes - HIPAA</td>
<td>All (assumed)</td>
</tr>
</tbody>
</table>

*All units have some staff who work with sensitive data (for example, Human Resources data).*
3. Additional restrictions needed?

- Are **additional restrictions** (beyond the minimum) required in your department/unit?
  - Do regulations, level of harm, or number of users call for additional restrictions?

**Hypothetical examples:**

<table>
<thead>
<tr>
<th>Unit</th>
<th>Data Type</th>
<th>Regulated?</th>
<th>Potential Harm</th>
<th>User Base</th>
<th>Additional Restrictions</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Counsel</td>
<td>Attorney/Client Privileged</td>
<td>No</td>
<td>Low-High</td>
<td>All</td>
<td>Only attorneys are allowed to use their own devices with sensitive university data</td>
</tr>
<tr>
<td>Registrar</td>
<td>Student Educational Records</td>
<td>Yes - FERPA</td>
<td>Low-Med</td>
<td>All</td>
<td>None</td>
</tr>
<tr>
<td>Health System</td>
<td>Protected Health Information</td>
<td>Yes - HIPAA</td>
<td>High</td>
<td>All</td>
<td>Must register with Mobile Device Management (MDM) service</td>
</tr>
</tbody>
</table>
• Only work with sensitive institutional data using a personal device if permitted by their unit.

• Follow minimum device management and security expectations.*

• Return/delete sensitive institutional data on request or when role changes.

• Report lost, stolen, or compromised devices that access or store sensitive institutional data to security@umich.edu.

• Allow U-M inspection of their device on request in accordance with U-M policy: Privacy and the Need to Monitor and Access Records (SPG 601.11).

• Produce information as required by FOIA or legal requests.

• Also applies to university-owned devices that are managed by individuals, such as devices purchased with grant funding and managed by researchers.
Device management expectations

• Keep operating system and apps **up-to-date**.

• **Only install trusted market apps**, such as those in the iTunes App Store, Google Play, or the Windows Store, unless required for a job-related purpose.

• **Do not bypass security features** (called “rooting” or “jailbreaking”) unless required for your university work.

• Certain types of data cannot be accessed or maintained **outside the U.S.** (includes Export Control, HIPAA, FISMA).
• **Use secure networks**, such as your cellular carrier network, **MWireless**, or wired connections.

• **Install and use the U-M VPN** if using untrusted networks, such as hotel guest wireless. (UMHS users should use the **UMHS VPN**.)

• **Turn off optional network connections** (for example, Wi Fi and Bluetooth) when not in use.
• **Require a password or PIN** for access to your device.

• **Set auto lock** to 15 minutes or less.

• **Encrypt the device** with built-in encryption (where possible).

• **Turn on the remote tracking/lock/wipe** capability.

• **Secure wipe** the device before selling it or giving it away.
# Implementation support

<table>
<thead>
<tr>
<th>MiWorkspace</th>
<th>Neighborhood IT Service Center</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-MiWorkspace</td>
<td>Unit Desktop Support Service Center</td>
</tr>
<tr>
<td><strong>Web Self-help Resources</strong></td>
<td><strong>Policy &amp; Standard</strong></td>
</tr>
<tr>
<td></td>
<td>• <a href="https://example.com/data-standard">Data Standard: Unit-Specific Expectations for Self-Management of Personally Owned Devices that Access or Maintain Sensitive Institutional Data</a></td>
</tr>
<tr>
<td>For Individuals</td>
<td>• <a href="https://example.com/responsibilities">Your Responsibilities for Protecting University Data When Using Your Own Devices</a></td>
</tr>
<tr>
<td></td>
<td>• <a href="https://example.com/instructions">Instructions for Securing Your Devices and Data</a></td>
</tr>
<tr>
<td>For Departments/Units</td>
<td>• <a href="https://example.com/toolkit">Toolkit: Implementing SPG 601.33 in Your Department/Unit</a></td>
</tr>
<tr>
<td></td>
<td>• <a href="https://example.com/checklist">Checklist for Implementing SPG 601.33</a></td>
</tr>
<tr>
<td><strong>Tips</strong></td>
<td>• Quickest way to get assistance for configuring devices is to call 4-HELP.</td>
</tr>
<tr>
<td></td>
<td>• Neighborhood IT can set up a walk-in session for MiWorkspace units.</td>
</tr>
<tr>
<td></td>
<td>• Departments/Units must determine the types of sensitive institutional data they work with.</td>
</tr>
<tr>
<td></td>
<td>• Questions: Contact <a href="mailto:iia.inform@umich.edu">iia.inform@umich.edu</a></td>
</tr>
</tbody>
</table>