Office of the Vice President for Communications

Electronic Data Disposal and Media Sanitization Policy

There are two SPGs that apply to this topic: 601.27 Information Security and 601.33 Security of Personally Owned Devices That Access or Maintain Sensitive Institutional Data. It is the policy of OVPC to comply with all university SPGs.

ITS has a policy page (http://cio.umich.edu/policy/electronic-data-disposal) which details procedures for Electronic Data Disposal and Media Sanitization. There is a separate guidance page to assist in assessing the classification level of data: (https://www.safecomputing.umich.edu/protect-the-u/safely-use-sensitive-data/classification-levels). In our communications work, it can be assumed that all of our data can be classified as *at least* **Moderate,** meaning that**:**

- Disclosure could cause limited harm to individuals and/or the university with some risk of civil liability.
- The data may be subject to contractual agreements or regulatory compliance, or is individually identifiable, confidential, and/or proprietary.

Due to this assessment, it is the policy of OVPC to treat all devices as needing the more rigorous sanitization methods. Our ITS support staff already follow these procedures when decommissioning university-owned devices. It is the responsibility of the supervising manager of any departing employee to ensure that this is done.

Employees who have used personally owned devices to store or view personally owned data are also required to comply with these rigorous sanitization methods. It is the responsibility of the supervising manager to ensure that university accounts and data are removed from personally owned devices when an employee leaves OVPC. This includes notifying system owners to remove access to university resources (websites, online tools, etc.) and verifying that employees delete university accounts from their phones, tablets, and other personally owned devices.

Shared document repositories can be problematic for maintaining access and control. Two methods offer greater control, and should be considered standard and preferable to others. As a result, we now require that when documents are created to be shared by a work group, they not be created in an individual account, but rather in one of these:

1. Team Drive in Google Drive
2. University file storage servers (sometimes call a letter drive for Windows users)

Both of these storage solutions offer a way to remove access to document shares without losing the documents. Documents shared from *individual* Google drive accounts do not offer this safeguard.