MiWorkspace Migration Code of Conduct

Overview

A common desktop operating environment or centralized core imaging is an important component of MiWorkspace-supported workstations. The core image includes a specific hardware set, software suite, and configuration supported by MiWorkspace staff. Tier-1 (Transition Desk/Service Center), Tier-2 (Neighborhood IT/Depot), and Tier-3 (Infrastructure) staff will be responsible for implementing the common desktop operating environment, resulting in a more effective and efficient desktop and asset management system for campus.

As this core image deployment is executed, it is very important that all appropriate steps be taken to ensure protection from unauthorized disclosure, as well as the privacy and confidentiality, of the files and contents on workstations, with the exception described below.

It is the policy of U-M to take all appropriate steps to protect the confidentiality, integrity, security, and privacy of both personal and institutional data and records maintained within the university environment. Privacy and the Need to Monitor and Access Records is the primary U-M SPG (601.11) that provides the underpinning for this standard. SPG 601.11 also provides the authority to access records of employees when there is reasonable cause to believe that the employee has engaged in misconduct and may have used University resources improperly.

ITS Staff Member Responsibilities

Staff whose computers will be migrated to the new core image will receive advance notification and instructions sufficient to allow them to organize, move or delete files or records—both personal and work-related—prior to the deployment of the core image on existing or new computers and workstations. This notification will specify the necessary actions for support staff deploying the core image on the workstation as well as those that are non-permissible.

Desktop Support Staff Responsibilities

Ethics, Privacy, and Reporting Requirements

All staff that provides desktop support related to the implementation of core images on MiWorkspace workstations are required to be knowledgeable of and follow this standard. Employees who fail to exercise appropriate ethical and professional conduct may be subject to disciplinary action up to and including termination.¹

¹ Section IV, Sanctions, SPG 601.11, Privacy and the Need to Monitor and Access Records.
Specific responsibilities of desktop support staff include:

- Not monitoring or inspecting the content on workstations being transitioned to the core image, including all information in folders labeled as private or personal.
- Only accessing or reviewing the minimum amount of files, applications, or operating systems necessary to deploy the core image on any workstation.
- Not sharing, copying, transmitting, deleting, or in any way altering information in workstations except when required in deploying the core image.
- Handling sensitive data appropriately as expected of an employee and steward of university information resources.
- Not disclosing such information to other employees unless they have a job-related or legal need to know.
- Being familiar with the provisions of the U-M Statement of Stewardship related to Information and Technology Resources (http://hr.umich.edu/stewardship.html#4).

In the course of deploying core images on staff workstations, support staff members may be exposed to or inadvertently observe confidential, personal, sensitive, or privileged information. This information may not be disclosed to others except where there is an obligation to report suspicious or illegal activity or computer content, including:

- When there is the reasonable expectation that not reporting the information might result in harm to individuals or university property (e.g., threats of workplace violence against members of the U-M community; suspicion of possessing a weapon on campus);
- When the information pertains to possession, distribution, or transmission of child pornography, which should be immediately reported to the U-M Department of Public Safety;
- When the information pertains to acts, conduct, or activities that are violations of University of Michigan policies or illegal.

The responsibility of the staff member ends with reporting the suspicious or illegal activity to an appropriate authority. Under no circumstances should the desktop support staff member confront the staff member or conduct any kind of investigation.

**Reporting Violations or Inappropriate Conduct**
Staff should immediately report potential violations of, or noncompliance with, this standard to the ITS User Advocate, abuse@umich.edu. Instances of suspected child pornography must be reported to the U-M Department of Public Safety.

Staff members who do not feel comfortable reporting concerns to the User Advocate can report their concern, suspicion of a violation of U-M policies, or illegal activity—annonymously if so desired—via the U-M Compliance Hotline (compliance.umich.edu/report.html, 866-990-0111). No staff should experience harassment or retribution when acting responsibly by reporting what they believe to be a legitimate and serious concern. Staff that feels they have been harassed, punished, or retaliated against for reporting a compliance concern should report this immediately to ITS HR, UHR, or the Compliance Hotline.

**Training and Attestation Requirements**
Staff engaged in re-imaging activities are required to complete the Access and Compliance 101 course in MyLinc, and sign the ITS code of conduct attestation.

---

1 The U-M Statement on Stewardship notes the responsibility of U-M staff to determine that “prior to sharing data with others [that] the recipient is authorized to access/view such information and understands his/her responsibility as a user.”

2 SPG 601.16, Policy and Guidelines Regarding Electronic Access to Potentially Offensive Material
Contact: IT Policy and Compliance Lead, Information and Infrastructure Assurance, ajlevy@umich.edu, 647-5357.