MONTREAT COLLEGE

Clean Desk Policy

Effective:
September 2, 2016

Purpose

The purpose of this policy is to ensure that all sensitive and/or confidential information is removed from an end user's workspace and properly locked away when not in use, or when the end user leaves his or her workstation. This policy is intended to reduce the risk of security breaches and the loss of, or damage to, information during and outside of normal business hours.

Scope

This policy applies to all Montreat College employees and affiliates.

Policy

- Users are required to ensure that all sensitive, restricted, and/or confidential information in hardcopy or electronic form is removed from the desk and locked in a drawer when their desk is unoccupied, at the end of the work day, and when they expect to be gone for an extended period.
- Computer workstations must be locked when the workspace is unoccupied.
- File cabinets containing restricted, confidential, or sensitive information must be kept closed and locked when not in use or when unattended.
- Keys used for access to restricted or sensitive information must not be left at an unattended desk.
- Laptops and other portable devices must be either locked with a locking cable or locked away in a drawer.
- Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.
- Printouts containing restricted, confidential, or sensitive information should be immediately removed from the printer.
- Upon disposal restricted, confidential, and/or sensitive documents must be shredded.
- Whiteboards containing restricted, confidential, and/or sensitive information must be erased.
- Storage devices such as CDs, DVDs, or USB drives containing restricted, confidential, and/or sensitive information must be locked in a drawer.

Policy Compliance

Compliance Measurement

Campus Technology will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to the policy must be approved by Campus Technology in advance.

Non-Compliance

The responses for violation of this policy will include, but are not limited to, the following:

- Notification: alerting a user to what appears to be an inadvertent violation of this policy in order to educate the user to avoid subsequent violations.
- Warning: alerting a user to the violation, with the understanding that any additional violation will result in a greater penalty.
- Loss of computer privileges: limitation or removal of computer privileges, either permanently or for a specified period of time.
- Restitution for damages: requiring reimbursement for the costs of repairs to or replacement of computer related material, equipment, hardware, software, data, and/or facilities, which reimbursement shall include, but not be limited to, the cost of additional time spent by college employees due to the violation.

In addition to the aforementioned, violators may be subject to disciplinary action – which may include termination – as may be prescribed by other rules, regulations, handbooks, procedures, or policies applicable to the violator. Furthermore, the violator may be subject to civil suits or ordinances, laws, statues, or regulations of the applicable local government, the State of North Carolina, or the United States of America.

Definitions of Terms

Sensitive Data: Data such as social security numbers, personal health information (PHI), personal identity information (PII), financial data, proprietary data, graded papers, etc. that must be handled with the utmost care, stored securely, and be protected to the greatest possible extent.

Contact Information

Campus Technology
Phone: 828-669-8012 Ext. 3663
Email: support@montreat.edu

Revision History

Initial Draft: 08/09/2016
Revised: 08/18/2016
Revised: 09/02/2016