MONTREAT COLLEGE

Data Protection Policy

Effective:
September 2, 2016

Purpose

The purpose of this policy is to help ensure the protection of the college's sensitive data from unauthorized access, damage, alteration, or disclosure while preserving the ability of authorized users to access and use the data for appropriate college purposes. This policy must be incorporated into the individual handling of hardcopy data and electronically stored data, as well as data access policies and procedures for systems and facilities containing sensitive data. This policy applies regardless of the place of storage and whether used for administration, research, teaching, or other purposes.

Scope

This policy applies to all Montreat College employees, contractors, workforce members, vendors, and agents with a college-owned or personal workstation connected to the Montreat College network.

Policy

- All college employees must have unique and individual user credentials, such as a user id and password. All employees must have passed a background check as defined by the college prior to authorization of access. The granting of access must be documented for future reference.
- Any non-college employee accessing sensitive data must be sponsored by an employee of the college. The approval process for granting such access must follow the policy of the appropriate data trustee. Any non-college individuals accessing college data at Montreat College are required to comply with federal and state laws and college policies and procedures regarding data security of sensitive data, and to exercise discretion with such data. Any non-college individual with access to college data who engages in unauthorized use, disclosure, alteration, or destruction of data in violation of this policy will be subject to appropriate disciplinary action, including possible dismissal and/or legal action.
- The data access request process must be formalized and auditable. The request process must include appropriate approvals, a description of the specific data requested, the level of access requested, and the purpose for accessing the data. Data access requests should be maintained in order to support the need to audit data access permissions at a later time.
- Terminated employees must have their access to all computer, network, and data immediately revoked as of their termination date. The former employee should be

dispossessed of all college-owned property, including technological resources such as laptop computers, mobile devices, portable storage, etc. The revocation of access must be documented for future reference.

- Access and login information must be maintained and monitored. For example, security logs must be enabled to maintain a complete audit trail of all processes initiated by the system. User access information regarding time of day, location, application, and volume of data retrieved must be uniquely attributable to an account of a distinct system user.
- "Clean Desk" practices must be adopted by each user. Paper documents containing sensitive data must not be left unattended and must be protected from the view of any passers-by or office visitors.
- Office doors must be closed when the occupant is away from the office.
- Paper documents containing sensitive data must be stored in locked file cabinets with a controlled key system or in an appropriately secured area.
- A list of individuals having access to the aforementioned file cabinets must be documented.
- File cabinets containing sensitive data must be locked before leaving the office each day.
- The keys to file cabinets containing sensitive data must not be left in unlocked desk drawers on in other areas accessible to unauthorized individuals.
- Paper documents containing information that is critical to the conduct of college business must be kept in secure file cabinets. Backup copies should be kept in an alternate location.
- Paper documents containing sensitive data must be shredded when they are no longer needed following any relevant college retention guidelines, making sure that such documents are secured until shredding occurs. If a shredding service is employed, the service provider should have clearly defined procedures in the contractual agreement that protect discarded information, and ensure that the provider is legally accountable for those procedures, with penalties in place for breach of contract.
- Documents containing sensitive data must be immediately retrieved or secured as they are printed on copy machines, fax machines, or printers.
- Sensitive data must not be discussed outside of the workplace or near/with anyone who does not have a specific "need to know".
- Electronic equipment containing sensitive data must be securely transferred or disposed in a secure manner.
- All workstations must use a surge protector or UPS (Uninterruptible Power Supply).
- Antivirus software must be installed and updated on all workstations and servers.
- If wireless network access is used, the workstation must be connected to the proper Montreat College wireless network.

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: 08/10/2016
Revised: 08/18/2016
Revised 09/02/2016