MONTREAT COLLEGE

Incident Response Policy

Effective:
September 2, 2016

Purpose

The purpose of this document is to provide some general guidelines and procedures for dealing with computer security incidents. The document is meant to provide Montreat College support personnel with some guidelines on what to do if they discover a security incident. The term incident in this document is defined as any irregular or adverse event that occurs on any part of the Montreat College Network. Some examples of possible incident categories include: compromise of system integrity; denial of system resources; illegal access to a system (either a penetration or an intrusion); malicious use of system resources, or any kind of damage to a system.

Scope

This policy applies to all Montreat College employees.

Policy

- All members of the University community are responsible for reporting known or suspected information or information technology security incidents. All security incidents at Montreat College must be promptly reported to the Director of Technology.
- Incident response will be handled appropriately based on the type and severity of the incident in accordance with the Incident Response Table below.
- All individuals involved in investigating a security incident should maintain confidentiality, unless the Director of Technology authorizes information disclosure in advance.

Incident Response

- Incident response will be managed based on the level of severity of the incident. The level of severity is a measure of its impact on or threat to the operation or integrity of the institution and its information. It determines the priority for handling the incident, who manages the incident, and the timing and extent of the response. Four levels of incident severity will be used to guide incident response: high, medium, low, and NA (Not Applicable).

Incident Response Table

Incident Severity	Characteristics (one or more condition present determines the severity)	Response Time	Incident Manager	Who to Notify	Post-Incident Report Required*
High	Significant adverse impact on a large number of systems and/or people Potential large financial risk or legal liability to the College Threatens confidential data Adversely impacts a critical enterprise system or service Significant and immediate threat to human safety High probability of propagating to a large number of other systems on or off campus and causing significant disruption	Immediate	Director of Technology	Director of Technology System Administrator Helpdesk Administrator	Yes
Medium	Adversely impacts a moderate number of systems and/or people Adversely impacts a non-critical enterprise system or service Adversely impacts a departmental	4 hours	Appointed by Director of Technology	Director of Technology System Administrator Helpdesk Administrator	No, unless requested by the Director of Technology or other appropriate administrator

	scale system or service Disrupts a building or departmental network Moderate risk of propagating and causing further disruption				
Low	Adversely impacts a very small number of non-critical individual systems, services, or people Disrupts a very small number of network devices or segments Little risk of propagation and further disruption	Next business day	Helpdesk Administrator	Director of Technology System Administrator Helpdesk Administrator	No
N/A	"Not Applicable" - used for suspicious activities which upon investigation are determined not to be an IT security incident.				

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