Berry College Information Security Breach Response Policy

I. Purpose

To define the general requirements and responsibilities during and following an information security breach; to ensure that the College community members are informed when there is a breach in the security of their confidential information.

II. Scope

This policy covers all people using Berry College IT resources and those who maintain, create, or store electronic or physical files which include confidential data.

III. Definitions

Breach of security for the purpose of this policy is defined as any unauthorized acquisition, access, use, storage, or disclosure of data maintained by the College that compromises the security and privacy of the data. A breach can be either intentional or accidental and the source may be either internal or external. A breach does not include (1) good faith acquisition, access, or use of private data by an employee, contractor, or agent of the College; (2) incidents involving confidential data that has been rendered unusable, unreadable, or undecipherable (e.g., through valid encryption or redaction) to unauthorized persons; or (3) incidents involving aggregate data.

Confidential Data includes college-owned electronic or paper information that is sensitive in nature and/or protected under applicable state or federal laws (i.e. FERPA, HIPAA, etc.). This data cannot be disclosed externally except in a few specific and highly regulated instances. It may not be shared internally (with other faculty/staff) unless access is required for the completion of official job duties and such sharing should comply with college policies and best practices. For more information, see Berry's FERPA policy.

Data is information collected, stored, transferred or reported for any purpose, whether in electronic or physical form.

Unauthorized acquisition means that a person has obtained confidential College data without statutory authority, authorization from an appropriate College official, or authorization of the person who is the subject of the data.

IV. Responsibilities

All employees and students must promptly report all known or suspected breaches of security regarding confidential data to the Chief Information Officer (CIO), either directly or through the Technical Support Desk. If the CIO is the source of a suspected breach, the report should be made to the Vice President for Finance. If the breach includes student data, the Registrar must be notified. If a computer or mobile device is stolen, Campus Safety must be notified to report the incident. In the case of unauthorized physical access, contact Campus Safety to report the incident.

The Chief Information Officer will make a determination, in consultation with the General Counsel and the Registrar (if student data is included), of whether notification to those affected is required and the responsible departments in complying with notification obligations.

The General Counsel will provide legal advice to the Office of Information Technology and other College staff to ensure compliance with notification obligations under the law.

Public Relations and Marketing will provide guidance during the notification process.

V. Policy

This document provides an overview of the process used to address potential security breaches, including electronic and physical access breaches. It is imperative that the Identification and Verification Phases are categorized as high priority so that the Containment Phase can begin as quickly as possible in order to minimize exposure of confidential data.

Identification Phase

Members of the campus community that suspect an IT system has been compromised in any way must immediately report the situation to the CIO or, if the CIO is the source of a suspected breach, the report should be made to the Vice President for Finance. If the breach includes student data, the Registrar must be notified. In the case of unauthorized physical access, contact Campus Safety to report the incident.

Types of Data Security Incidents:

Computing Devices Compromised by Malware
Desktops, laptops, mobile devices, and servers are often infected with malicious software (e.g., viruses, malware). If the infected device contains confidential data, this may constitute a data security incident. Discontinue use of the computer immediately and contact the Technical Support desk for assistance.

Computing Devices Accessed without Authorization
These include college-owned devices accessed without permission – stolen or compromised credentials (e.g., user names and passwords), credentials lost to phishing scams, and other attempts to access a device without authorization (e.g., former employees). Discontinue use of the computer immediately and contact the Technical Support desk for assistance.

Lost or Stolen Computing Devices
These include any device, whether college-owned or personal, that may contain confidential data. **Immediately** contact both the CIO and Campus Safety to report the theft/loss.

Physical Access Breach
Includes unauthorized access to physical documents that may contain confidential data. Contact Campus Safety to report the situation.

Verification Phase

Electronic Records: The CIO, with input from the Director of the compromised system, will determine if the reported incident poses a risk that warrants investigation.

Physical Records: The Assistant Vice President (AVP) for Campus Security and Emergency Management Response, with input from the Director of the compromised records, will determine if the incident requires further investigation.

This investigation will have one of two outcomes:

1. The incident is determined to be without merit and the Director of the compromised system will write a brief summary of the events for the record. The reporting member of the community will be contacted with information that an investigation was conducted, along with the findings which will close the incident.
2. A security breach or unauthorized physical access is determined to have occurred and the incident is moved to the containment phase below.

Containment Phase

The actions that need to be taken will depend on the uptime requirements of the compromised system, the suspected level of attacker privilege, the nature and quantity of data at risk, and the suspected profile of the attacker. The most important goals of this phase are to:

1. Eliminate attacker access: Whenever possible, the Director of the compromised system may request that Network Operations staff implement a port-block to eliminate attacker access. In cases where the impact of system downtime is very high, the Director of the compromised system will work to determine the level of attacker privilege and eliminate their access safely. In the case of physical access, the Director should secure the unsecure area.
2. Assess the scope of the incident by:
   - Creating a preliminary list of compromised systems/files.
   - Creating a preliminary list of storage media that may contain evidence.
   - Creating a preliminary attack timeline based on initially available evidence.
3. Preserve forensic evidence: The Director of the compromised system will capture disk images when possible for all media that are suspected of containing evidence, including external hard drives and flash drives. In the case of unauthorized physical access, the Director will work with Campus Safety to preserve any physical evidence to identify the intruder.

Analysis Phase

In this phase, an in-depth investigation of the available network-based and system-based evidence will occur. The primary goal of analysis is to establish whether there is reasonable belief that the attacker(s) successfully accessed restricted data on the compromised system electronically or through unauthorized physical access. Secondary goals are to generate an attack timeline and ascertain the attackers' actions. All analysis steps are primarily driven by the Director of the compromised system, who coordinates communications between other stakeholders, including system owners, and other Directors, and, in the case of unauthorized physical access, Campus Safety. Questions which are relevant to making a determination about whether data was accessed without authorization include:

1. Suspicious Network Traffic: Is there any suspicious or unaccounted for network traffic that may indicate data extraction occurred?
2. Attacker Access to Data: Did attackers have privileges to access the data or were the data encrypted in a way that would have prevented reading? In the case of unauthorized physical access, was a computer station available to allow access to systems?
3. Evidence that Data was accessed: Are file access audit logs available that show whether the files have been accessed during the compromise period?
4. Length of Compromise: How long was the system accessed by the attacker?
5. Method of Attack: Was a human involved in executing the attack, or was an automated method used?
6. Attacker Profile: Is there any indication that the attackers were data thieves or motivated by different goals?

Recovery Phase

The primary goal of the recovery phase is to restore the compromised system or physical location to its normal business function in a safe manner. This phase will very often begin during the Analysis Phase and run simultaneously. The Director of the compromised system will remediate the immediate problem and restore the system to normal function. The Director of the compromised system, in consultation with the CIO and other Berry College administrators as needed, will make short-term system, application, and business process changes to prevent further compromise and reduce operating risk. If the breach involved physical records, the Director, along with Campus Safety personnel, will be responsible for making sure the location is properly secured if temporary measures were taken during the Containment Phase.

Reporting/Notification Phase

The final report serves two main purposes.

1. A report is made to the President and the Cabinet as to whether the Director of the compromised system/location and the CIO/AVP conclude there is a reasonable belief that a breach of security has occurred and the degree of probability that the security or privacy of the data has been compromised. The report shall be completed within a time frame that ensures compliance with any applicable federal and/or state data security laws; if no such laws exist or apply, then the report shall be completed as soon as practical and reasonable under the circumstances.
2. If the results of the investigation conclude that there is a reasonable expectation that confidential data was viewed or taken, the department must notify those affected whose information is at risk. The department will work with its Dean's or Vice President's office, the General Counsel, and the Office of Public Relations and Marketing to provide notification. Notices must be given in writing by US Mail, email, or other appropriate electronic means. The final text that is used in any breach notification must be reviewed and approved by the Office of Public Relations and Marketing and the General Counsel.

Notifications will vary depending on the circumstances of each system breach and could include the following elements:

- purpose of the letter;
- identity of the college department;
- what happened in general terms, including the dates of the security breach and of its discovery;
- what kind of personal information was involved;
- what they should do to protect themselves;
- where to go for more information;
- what the institution is doing, if anything, to investigate further;
- who to contact for more info

3. A series of mid-term and long-term recommendations are made to the owners of the compromised system, including responsible management, suggesting improvements in technology or business processes that could reduce operating risk in the future.

VI. References

Educause Library, www.educause.edu

HEISC 2014 Information Security Guide, https://spaces.internet2.edu/display/2014infosecurityguide/Home

UMass Amherst, http://www.it.umass.edu/support/security/data-security-incidents-prevention-response-procedures-umass-amherst

Birmingham Southern College, http://www.bsc.edu/policies/it/IT%20Security%20Policy.pdf

VII. Approval and Review

This policy is periodically reviewed by Information Security Advisory Committee and Information Technology staff. Recommendations for changes or additions to this policy will be referred to the President's Cabinet. The college reserves the right to amend this policy at any time.

Date issued: August 5, 2015

Review Date: