Title – IT Security Policy

Policy Abstract – In the event of information security breach, availability of service attack, or unauthorized physical access Birmingham-Southern College will follow appropriate steps to identify, contain, analyze, recover and report such incidents.

Responsible Office – Information Technology

Official – Anthony Hambey

Contact(s) – Anthony Hambey, 226-4849, ahambey@bsc.edu
Applies To – Information Technology
Effective Date – 2/2014
Revision Dates – 8/31/2021

1. **Introduction/Background –** An information technology security incident is an event involving an IT resource at Birmingham-Southern College that has the potential of having an adverse effect on the confidentiality, integrity, or availability of that resource or connected resources. Resources include individual computers, servers, storage devices, media, and mobile devices such as phones and tablets, as well as the information, messages, files, and/or data stored on them. This includes incidents that originate externally from outside sources as well as internally from students, employees or others either maliciously or from being used unknowingly through falling victim to scams from phishing, spam or other means such as but not limited to viruses, malware, Trojan horses, key loggers, root kits etc. Physical access such as but not limited to server rooms, equipment closets, underground conduit accesses and wireless access points are also defined as IT resources covered by this policy. Prompt detection and appropriate handling of these security incidents is necessary to protect Birmingham-Southern College's information technology assets.

2. **Purpose –** The purpose of this policy is to provide general guidance to BSC staff and supervisors who manage IT resources to:

   - Enable quick and efficient recovery from security incidents.
   - Respond in a systematic manner to incidents and carry out all necessary steps to correctly handle an incident.
   - Prevent or minimize disruption of critical computing services.
   - Minimize loss or theft of sensitive or mission critical information.

3. **Applicable Regulations –** SACSCOC, Principles of Accreditation 2018

4. **Policy Statement** – This document provides an overview of the process used to address potential security, availability of service attacks and physical access breaches. Detailed technical procedures may vary depending on the systems impacted and will be addressed within the framework of this document.

- Identification Phase
  1. Any member of the campus community may identify a potential security incident though external complaint/notification, or other knowledge of impermissible use or disclosure of restricted data or physical access to areas where IT resources are present. System owners or Directors of the compromised system may do so by observing suspicious system behavior or evidence of physical access by unauthorized personnel.
  2. Members of the campus community that suspect an IT system has been accessed without authorization or is under an availability of service attack must immediately report the situation to the Help Desk.

- Verification Phase
  1. The Vice President for IT or the AVP for IT with input from the Director of the compromised system such as the ERP (Colleague, CBORD, TheSIS), LMS (Moodle), Active Directory (network credential management and email), backup systems, VPN, firewall, packet shaper, Network Storage systems, LAN, WAN, Telephony or Cable TV systems, etc. is to determine if the reported incident poses a unique risk that warrants investigation.
  2. If the above authority determines that the report warrants an investigation, the Director of the compromised system will conduct one. This investigation will have one of two outcomes:
     - The incident is determined to be false positive 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 with a false positive outcome which will close the incident.
     - A security breach, availability of service attack or unauthorized physical access occurred and the incident is moved to the containment phase below.

- Containment Phase

  This is the most time-sensitive and also the most contextually dependent phase of the investigation. 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 rare cases, this is done via the Director of the compromised system unplugging the network cable. 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, secure the unsecure area.
  2. Assess the scope of the incident by:
     - Creating a preliminary list of compromised systems.
     - Creating a preliminary list of storage media that may contain evidence.

        - Creating a preliminary attack timeline based on initially available evidence.
        - In the case of unauthorized physical access contact campus police and report the incident.
    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 work with campus police to preserve any physical evidence to identify the intruder.

- Analysis Phase

    The analysis phase is where in-depth investigation of the available network-based and system-based evidence occurs. 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 police. 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 was the data encrypted in a way that would have prevented reading? In the case of unauthorized physical access was a terminal or 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 "drive-by" 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 to its normal business function in a safe manner. The Director of the compromised system will remediate the immediate problem and restore the system to normal function. The Director of the compromised system will make short-term system, application, and business process changes to prevent further compromise and reduce operating risk.

- Reporting Phase

    The final report serves two main purposes.

1. A recommendation is made to the President and the President's Council as to whether the Director of the compromised system and the Vice President for IT or AVP for IT feel there is a reasonable belief that restricted data was disclosed impermissibly without authorization and the degree of probability that the security or privacy of the data has been compromised. The report must be made in sufficient time to allow notification, if appropriate, within any legally-mandated time period. Although at the time of this policy creation Federal laws defer to state regulations outside of specific banking and health care industries and the State of Alabama has no security breach laws.
2. 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.

5. **Detail**s – An annual financial audit of the College contains a technology component whereby this is verified each year. Non-compliance with this policy would be reported in the form of comments in the management letter of the audit.

6. **Definitions** –

- SACSCOC is the Southern Association of Colleges and Schools, Commission on Colleges.
- System owners are managers or directors in areas outside of IT that operate and are the responsible party for entering and maintaining the data in a system.
- Director of the compromised system is the respective director or system administrator within IT responsible for the operation and security of the system.
- ERP is a term meaning Enterprise Resource Planning. This is an industry standard term referring to software applications used to operate the business function of an organization.
- Colleague is the system name of the ERP from the vendor Ellucian used by the College.
- CBORD is the campus meal plan and campus card system used by the College.
- TheSIS is the system name of the web access to the Colleague system used by the College.
- LMS is a term meaning Learning Management System whereby content is housed for the distribution of course materials.
- Moodle is the system name of the LMS used by the College.
- Active Directory is the Microsoft developed credential and network access system used by the College.
- VPN is a virtual private network allowing access from off-campus to on-campus systems used by the College.
- LAN is the local area network for the College.

- WAN is the wide area network including systems outside the physical premises of the campus.

7. **References** – IT Security Incident Form and SACSCOC, Principles of Accreditation 2018 https://sacscoc.org/app/uploads/2019/08/2018PrinciplesOfAcreditation.pdf