Alvernia
University

Information Technology Policy
9.3600
IT Security Incident Response

Contents

Document Review Log

Date Reviewed	Description of Changes
8/17/2023	Initial Draft approved by Senior Leadership Team

Introduction

Information security is a holistic discipline, meaning that its application, or lack thereof, affects all facets of an organization or enterprise. The goal of the Alvernia University Information Security Program is to protect the Confidentiality, Integrity, and Availability of the data employed within the organization while providing value to the way we conduct business. Protection of the Confidentiality, Integrity, and Availability are basic principles of information security, and can be defined as:

- Confidentiality – Ensuring that information is accessible only to those entities that are authorized to have access, many times enforced by the classic "need to know" principle.
- Integrity – Protecting the accuracy and completeness of information and the methods that are used to process and manage it.
- Availability – Ensuring that information assets (information, systems, facilities, networks, and computers) are accessible and usable when needed by an authorized entity.

Alvernia University has recognized that our business information is a critical asset and as such our ability to manage, control, and protect this asset will have a direct and significant impact on our future success.

This document establishes the framework from which the enterprise can efficiently and effectively manage, control and protect its business information assets and those information assets entrusted to Alvernia University by its stakeholders, partners, customers and other third parties.

The Alvernia University Information Security Program is built around the information contained within this policy and its supporting documents.

Purpose and Scope

The purpose of the Alvernia University Information Security Policy is to describe the actions and behaviors required to ensure that due care is taken to avoid inappropriate risks to Alvernia University, its business partners, and its stakeholders. The Alvernia University Information Security Policy applies equally to any individual, entity, or process that interacts with any Alvernia University Information Resources.

Leadership recognizes that intrinsic to an effective incident response plan, the incident response team has:

A) Explicit authorization to monitor networks, systems, and storage as required.
B) An understanding that end users have no expectation to privacy and consent to such monitoring.

These two key preconditions to this policy are addressed in 9.2000, End User Responsibilities.

Responsibilities

Senior Leadership Team

Responsibilities of the Senior Leadership Team include:

- Ensure that an appropriate risk-based Information Security Program is implemented to protect the confidentiality, integrity, and availability of all Information Resources collected or maintained by or on behalf of Alvernia University.
- Ensure that information security processes are integrated with strategic and operational planning processes to secure the organization’s mission.
- Ensure adequate information security financial and personnel resources are included in the budgeting and/or financial planning process.
- Ensure that the Security Team is given the necessary authority to secure the Information Resources under their control within the scope of the Alvernia University Information Security Program.
- Designate an Information Security Officer and delegate authority to that individual to ensure compliance with applicable information security requirements.
- Ensure that the Information Security Officer, in coordination with the Information Security Committee, reports annually to the Senior Leadership Team on the effectiveness of the Alvernia University Information Security Program.

Information Security Officer

Responsibilities of the Information Security Officer include:

- Chair the Information Security Committee and provide updates on the status of the Information Security Program to Executive Management.
- Manage compliance with all relevant statutory, regulatory, and contractual requirements.
- Participate in security related forums, associations, and special interest groups.
- Assess risks to the confidentiality, integrity, and availability of all Information Resources collected or maintained by or on behalf of Alvernia University.
- Facilitate development and adoption of supporting policies, procedures, standards, and guidelines for providing adequate information security and continuity of operations.
- Ensure that Alvernia University has trained all personnel to support compliance with information security policies, processes, standards, and guidelines. Train and oversee personnel with significant responsibilities for information security with respect to such responsibilities.
- Ensure that appropriate information security awareness training is provided to company personnel, including contractors.
- Implement and maintain a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of Alvernia University.
- Develop and implement procedures for testing and evaluating the effectiveness of the Alvernia University Information Security Program in accordance with stated objectives.
- Develop and implement a process for evaluating risks related to vendors and managing vendor relationships.
- Report annually, in coordination with the Information Security Committee, to Executive Management on the effectiveness of the Alvernia University Information Security Program, including progress of remedial actions.

Information Security Committee

Responsibilities of the Information Security Committee include:

- Ensure compliance with applicable information security requirements.

- Formulate, review, and recommend information security policies.
- Approve supporting procedures, standards, and guidelines related to information security.
- Assess the adequacy and effectiveness of the information security policies and coordinate the implementation of information security controls.
- Review and manage the information security policy waiver request process.
- Identify and recommend how to handle non-compliance.
- Provide clear direction and visible management support for information security initiatives.
- Promote information security education, training, and awareness throughout Alvernia University, and initiate plans and programs to maintain information security awareness.
- Educate the team and staff on ongoing legal, regulatory and compliance changes as well as industry news and trends.
- Identify significant threat changes and vulnerabilities.
- Evaluate information received from monitoring processes.
- Review information security incident information and recommend follow-up actions.
- Report annually, in coordination with the Information Security Officer, to Executive Management on the effectiveness of the Alvernia University Information Security Program, including progress of remedial actions.

All Employees, Contractors, and Other Third-Party Personnel

All individuals have the following responsibilities:

- Understand their responsibilities for complying with the Alvernia University Information Security Program.
- Formally sign off and agree to abide by all applicable policies, standards, and guidelines that have been established.
- Use Alvernia University Information Resources in compliance with all Alvernia University Information Security Policies.
- Seek guidance from the Information Security Team for questions or issues related to information security.

Policy

Alvernia University maintains and communicates an Information Security Program consisting of topic-specific policies, standards, procedures, and guidelines that:

- Serve to protect the Confidentiality, Integrity, and Availability of the Information Resources maintained within the organization using administrative, physical, and technical controls.
- Provide value to the way we conduct business and support institutional objectives.
- Comply with all regulatory and legal requirements, including:
  - GLBA
  - HIPAA
  - FERPA
  - PCI Data Security Standard
  - Information Security best practices, including NIST 800
  - State breach notification laws
  - All other applicable federal and state laws or regulations

The information security program is reviewed no less than annually or upon significant changes to the information security environment.

Enforcement

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

Exceptions

Exceptions from certain policy provisions may be sought following the Alvernia University Exception Process.

References

This section contains any 3rd party standards, guidelines, or other policies referenced by this policy.

1. NIST Special Publication 800-61 R2, Computer Security Incident Handling Guide, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
2. SANS Institute InfoSec Reading Room, Incident Handler's Handbook, https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901
3. SANS Institute InfoSec Reaching Room, An Incident Handling Process for Small and Medium Businesses, https://www.sans.org/reading-room/whitepapers/incident/incident-handling-process-small-medium-businesses-1791
4. SANS SCORE: Law Enforcement FAQ, https://www.sans.org/score/law-enforcement-faq/
5. NIST special publication 800-86, Guide to Integrating Forensic Techniques into Incident Response, http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf
6. Information Technology Standard Operating Procedures located on the IT SharePoint site
    a. SOP - IT Security Incident Response Plan
    b. SOP - IR Severity and Response Quick Reference
    c. SOP - Information Security Incident Response Report

Exhibits

None