Contents

Document Review Log

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

Formulate, review, and recommend information security policies.
Approve supporting procedures, standards, and guidelines related to information security.
Assess the adequacy and effectiveness of the informati on 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

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