Information Security Program

Issue Date: 2018-12-13
Expiration Date: N/A
Category: ITS Standard

1.0 – Overview

Yavapai College (YC) participates in financial activities related to students ("customers") potentially including making, acquiring, brokering, or servicing loans and engaging in collection agency services either directly or via contracted third parties. As a result, YC is required to comply with the Gramm-Leach-Bliley Act (GLBA). YC is presumed to be in compliance with the privacy provisions of the GLBA due to its compliance with the Family Educational Rights and Privacy Act (FERPA). However, the GLBA subjects institutions to additional provisions related to administrative, technical, and physical safeguarding of customer information.

2.0 – Purpose

This document provides a basic overview of YC's formal information security program, formal and informal efforts to protect sensitive information, roles and responsibilities, and contact information for reporting purposes.

3.0 – Scope

This program applies to all YC employees, contractors, and volunteers and to all College-owned data, including data subject to regulatory compliance under FERPA, GLBA, or because of an FSA Program Agreement.

4.0 – Program Overview

YC's information security program focuses on the confidentiality, integrity, and availability of data, both in electronic and physical form. The program conducts formal and informal risk assessments, facilitates internal and external audits, coordinates departmental information management and protection efforts, and supports delivery of security and phishing awareness training and related efforts.

4.1 – Program Ownership / Coordination

The Information Security Program is managed by the Information Security group, part of YC's Information Technology Services Department. The Chief Information Security Officer (CISO) is principally responsible for program implementation and is the Security Program Coordinator.

Yavapai COLLEGE

4.2 – Employee Training and Responsibilities

Employees are required to complete an information security awareness training annually. Additionally, employees with access to data classified as sensitive or restricted according to YC's Information Security Data Classification Standard are required to complete a supplemental training addressing the handling and protection of sensitive or regulated data. Pursuant to this training, it is the responsibility of employees to be aware of and promptly report any known or suspected information security incident. Reports should be made to the Information Security group – 928-717-7722 or email infosec@yc.edu.

4.3 – Information Management – Physical and Electronic

It is the responsibility of each employee and department that creates or handles sensitive or regulated data to properly protect that data, regardless of its form. The Information Security group, in concert with Information Technology Services staff, work to ensure the confidentiality, integrity, and availability of electronic data in order to make sure it is available only to those with a legitimate business purpose.

Employees are encouraged to securely delete data no longer necessary for business purposes, subject to records retention policies and procedures. Guidance on proper handling and destruction of electronic media can be found in the ITS Media Protection Procedure. Employees are additionally reminded of their responsibilities related to the secure storage and handling of physical records addressed within policy 5.30 – Clean Desk and Clear Screen.

4.4 – Third Party Access to Data, Selection of Service Providers

YC routinely works with third parties to deliver products and services to its customers. Some of these third parties create, share, store, or receive access to sensitive or regulated data directly from or on behalf of YC. Handling of sensitive and/or regulated data by third parties is addressed in YC's purchasing terms and conditions, specifically in the "Data Security Addendum". Third parties are required to promptly inform YC of any breach to their systems involving YC data and are not permitted to share, transfer, or sell that data or derivative works to others without YC's explicit written permission.

4.5 – Incident Handling / Incident Response

YC routinely engages in proactive threat assessment to minimize the risk of security incidents. When incidents occur, YC has defined policies and procedures related to incident handling and response. Employees, contractors, or volunteers who suspect they have observed an information security incident should contact YC Information Security at 928-717-7722 or infosec@yc.edu promptly to report all relevant details related to the incident.

4.6 – Risk Assessment

Formal and informal risk assessments are conducted annually and throughout the year to address reasonably foreseeable risks to security or privacy identified through internal efforts, from affiliated third parties, and from local, state, and national information sharing groups. Risk assessment focus areas include employee information security awareness, sensitive data management, system and service availability, border and internal technical protections, incident response, and vendor management.

4.7 – Continuous Evaluation

Elements of the Information Security Program are continuously reviewed for efficacy and relevance to the institution and to the threats targeted to the institution and its customers. Material changes to the Program are reviewed and approved by the CISO and CIO and will be noted in this document and/or in the Yavapai College Information Security Playbook.

5.0 – Revision History

Author	Date	Version	Reason
S. Hagan	12/12/18	1.0	Initial Creation
S. Hagan	12/14/18	1.1	Added Section 4.7, clarified Section 4.6

6.0 – Inquiries

Direct inquiries about this procedure to:

Patrick Burns
Chief Information Officer – Yavapai College
E-mail: Patrick.burns@yc.edu
Voice: (928) 776-2055

Yavapai COLLEGE