Talladega College

Information Security Policy

2020

Last Updated – April 23, 2020

Date	Description of Changes	Updated By:	Approver Title
01/30/2020	Initial version	Quintin Latin	Associate VP of Information Technology
02/18/2020	Reviewed	Quintin Latin	Associate VP of Information Technology
04/23/2020	Reviewed	Quintin Latin	Associate VP of Information Technology

Talladega College Restricted Information
Do Not Distribute without Written Permission from Talladega College

Talladega College Restricted Information
Do Not Distribute without Written Permission from Talladega College

Talladega College Restricted Information
Do Not Distribute without Written Permission from Talladega College

1 INFORMATION SECURITY POLICY PURPOSE & OBJECTIVES

1.1 PURPOSE

Talladega College is committed to protecting the confidentiality of all sensitive data that it maintains, including information about individuals who work or study at the College. Talladega's Information Security Policy (ISP) aims to protect all information assets through their entire lifecycle. The lifecycle includes the creation, collection, processing, dissemination, usage, storage and secure disposal when no longer required.

The Talladega College ISP is intended as a set of comprehensive guidelines and policies designed to safeguard all confidential and restricted data maintained at the College, and to comply with applicable laws and regulations on the protection of Personally Identifiable Information (PII), as those terms are defined below, found in records and in systems owned by the College.

Data - For the purposes of this Policy, "data" refers to any and all information stored, accessed, or collected at the College about members of the College community.

Personally Identifiable Information - Personally Identifiable Information (PII), as defined by the State of Alabama STANDARD 681S2-00, is the first name and last name or first initial and last name of a person in combination with any one or more of the following:

- Social Security number;
- Driver's license number or state-issued identification card number; or
- Financial account number (e.g. bank account) or credit or debit card number that would permit access to a person's financial account, with or without any required security code, access code, personal identification number, or password.
- For the purposes of this Policy, PII also includes passport number, alien registration number or other government-issued identification number.

1.2 OBJECTIVES

Talladega ensures the security and privacy of all Personally Identifiable Information by following the Policy objectives outlined below:

- Establish a comprehensive information security program for Talladega College with policies designed to safeguard sensitive data that is maintained by the College, in compliance with federal and state laws and regulations;
- Establish employee responsibilities in safeguarding data according to its classification level; and
- Establish administrative, technical and physical safeguards to ensure the security of sensitive data.

Talladega College Restricted Information
Do Not Distribute without Written Permission from Talladega College

2 SCOPE

This applies to all Talladega College employees, whether full- or part-time, including faculty, administrative staff, contract and temporary workers, interns, and student employees, as well as to all other members of the Talladega College community (hereafter referred to as the "Community"). This program also applies to certain contracted third-party vendors and/or hired consultants. The data covered by this Policy includes any information stored, accessed or collected at the College or for College operations.

3 GENERAL POLICY CONTROLS

Talladega employs multiple controls in the protection of Information and Information System assets. The controls are based on NIST Special publication 800-53 which in turn maps to best practice ISO 27001 controls. The controls represent a mix of protections, of different types and at different levels using the principle of Defense in Depth. The fundamental focus is preventing undue disclosure, alteration and destruction of information assets; that transactions are genuine and cannot be disputed. Talladega classifies all information assets as is specified in Talladega Information Classification standard. The standard defines the type of information, impact of disclosure, how it should be labeled and handled. Talladega information assets are classified as follows:

Confidential - Confidential data refers to any data where unauthorized access, use, alteration or disclosure of this data could present a significant level of risk to Talladega College or the Community. All PII as defined above is designated as Confidential. Confidential data should be treated with the highest level of security to ensure the privacy of that data and prevent any unauthorized access, use, alteration, or disclosure.

Restricted - Restricted data refers to all other personal and institutional data where the loss of such data could harm an individual's right to privacy or negatively impact the finances, operations, or reputation of Talladega College. Any non-public data that is not explicitly designated as Confidential should be treated as Restricted data. Restricted data includes data protected by the Family Educational Rights and Privacy Act (FERPA), referred to as student education records. This data also includes, but is not limited to, donor information, research data on human subjects, intellectual property, College financial and investment records, employee salary information, or information related to legal or disciplinary matters.

Restricted data should be limited to access by individuals who are employed by or matriculate at Talladega College and who have legitimate reasons for accessing such data, as governed by FERPA, or other applicable law or College policy. A reasonable level of security should be applied to this classification to ensure the privacy and integrity of this data.

Public (or Unrestricted) - Public data includes any information for which there is no restriction to its distribution, and where the loss or public use of such data would not present any harm to Talladega College or members of the Talladega College community. Any data that is not classified as Confidential or Restricted should be considered Public data.

Talladega College Restricted Information
Do Not Distribute without Written Permission from Talladega College

4 GOVERNANCE

Talladega's executive management actively and visibly support an information security culture. Talladega Information Security Team is responsible for the oversight of corporate wide information risks which includes all Information Security and Privacy related affairs. All controls are governed by the required policies that are approved by Talladega's executive management team. Standards and procedures set the right conventions and steps for implemented controls. Specific security roles and responsibilities were established to oversee and manage information security and privacy risks.

5 ROLES & RESPONSIBILITIES

Talladega Executive Management

- Provide Executive Sponsorship/Tone at the top for Information Security and Privacy Policy and activities
- Inform Policy of current and future strategy and vision
- Ensure alignment of Talladega strategy and Information Security & Privacy goals
- Informed of and provide direction in response to Talladega's most significant risks
- Provide management oversight of all aspects of the Information Security & Privacy Policy
- Provide authorization to operate information systems at an acceptable level of risk
- Approve investments and resource allocation to Information Security & Privacy Policy
- Oversee Information Security and Privacy Policy activities
- Monitor execution of the Policy's strategic objectives

Information Security Advisory Board (Subset of Executive Management)

- Provide guidance to Information Security in maintaining alignment between business goals and the Information Security Policy principles and objectives
- Provide guidance to Information Security related to capital investments
- Provide guidance to Information Security related to long term strategic initiatives, execution tactics and operational impacts

Vice President of Technology/Information Security Officer

- Implement and direct a defined Information Security & Privacy Policy
- Provide ongoing guidance and support for the refinement of the overall Policy ensuring best practices are incorporated
- Define the Information Security Strategy
- Communicate status of Information Security Policy to the Board of Trustees and Executive Management
- Synthesize and communicate the latest security & privacy related trends and issues for corporate relevance
- Present relevant Security & Privacy information and trends during Cabinet meetings
- Communicate with auditors and regulators on Information Security management topics as appropriate
- Assist Executive Management with security requirements
- Implement, manage and continuously assess the Information Security and Privacy Policy
- Establish, manage and maintain Talladega's Security profile
- Ensure the appropriate operational security posture is maintained for information systems

Talladega College Restricted Information
Do Not Distribute without Written Permission from Talladega College

- Manage Security Incident Response processes
- Manage annual Security and Privacy training of all Talladega employees
- Manage Security Controls Monitoring
- Perform periodic Security and Privacy Awareness Communications
- Ensure the development and maintenance of the security plan, and that systems are deployed and operated in accordance with the agreed-upon security controls.
- Provide oversight of System Access Management Processes
- Evaluating the ability of service providers to comply with STANDARD 681S2-00 in the handling of Personally Identifiable Information for which the College is responsible, ensuring there are included in the College's contracts with those service providers provisions obligating them to comply with STANDARD 681S2-00 in providing the contracted for services, and obtaining from such service providers written certification that they have a written, comprehensive information security Policy that is in compliance with the provisions of STANDARD 681S2-00.
- Reviewing the scope of the security measures in the Policy at least annually, or whenever there is a material change in College business practices that may implicate the security or integrity of records containing Personally Identifiable Information.
- Responsible for implementation of the business rules established by the Data Security Coordinator.

Vice President of Technology

- Responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of all information systems and data
- Operate and maintain centralized reporting of appropriate information security related activities for formal incident management
- Manage Business Continuity Management processes and Disaster Recovery processes

Type of Data	Data Security Coordinator*
Faculty/Instructional	VP of Academic Affairs
Financial	VP of Finance
Staff/Human Resources	HR Director
Student	Enrollment Management
Alumni/Development	VP of Institutional Advancement

Campus Community

- Handle information and information assets in compliance with this Policy and as defined in Talladega's policies/standards/procedures
- Consult information Security and Privacy on solution(s) implementations
- Escalate suspected incidents to the Helpdesk or Information Security
- Participate in Security and Privacy Awareness Training

Talladega College Restricted Information
Do Not Distribute without Written Permission from Talladega College

6 SECURITY ARCHITECTURE

Talladega's business infrastructure is supported by a multi-layer security architecture. The security architecture enables technical decisions to be made in support of Talladega's business goals and the management of its information assets. The security architecture enables the effective deployment of security resources that include policy, standards, and risk-based decisions.

Talladega employs active network peripheral and monitoring controls. Encryption is enforced at rest, in all application databases, on portable media, backup media, desktops, laptops and in data transmissions. End-point protection is also enforced.

7 MANAGEMENT CONTROLS

7.1 RISK MANAGEMENT

Addresses: STANDARD 681S2-00

Talladega College recognizes it has both internal and external risks to the privacy and integrity of College information. These risks include, but are not limited to:

- Unauthorized access of Confidential/Restricted data by someone other than the owner of such data
- Compromised system security as a result of system access by an unauthorized person
- Interception of data during transmission
- Loss of data integrity
- Physical loss of data in a disaster
- Errors introduced into the system
- Corruption of data or systems
- Unauthorized access of Confidential/Restricted data by employees
- Unauthorized requests for Confidential/Restricted data
- Unauthorized access through hard copy files or reports
- Unauthorized transfer of Confidential/Restricted data through third parties

This may not be a complete list of the risks associated with the protection of Confidential and Restricted data. Since technology growth is not static, new risks are created regularly. Accordingly, the Talladega's Chief Information Security Officer will actively participate in and monitor advisory groups such as the EDUCAUSE Security Institute and SANS Internet Storm Center for identification of new risks.

7.2 VENDOR MANAGEMENT AND CONTROL

Addresses: STANDARD 681S2-00

Talladega College exercises appropriate diligence in selecting service providers capable of maintaining appropriate security safeguards for PI provided by the College to them. The College Comptroller is responsible for identifying those third parties providing services to the College that have access to PII. All relevant contracts with these third parties are reviewed and approved to ensure the contracts contain the necessary language

Talladega College Restricted Information
Do Not Distribute without Written Permission from Talladega College

regarding safeguarding PII. It is the responsibility of the Data Security Coordinators to confirm that the third parties are required to maintain appropriate security measures to protect PII consistent with this Policy and all federal and state laws and regulations.

7.3 PERSONNEL AND TRAINING

Addresses: STANDARD 681S2-00

Talladega promotes security awareness using email messages, formal instruction, and newsletters to communicate awareness. All employees are required to complete security training upon hire, annually thereafter. Annual training consists of a core security curriculum plus additional materials based on the employee's role. Each employee shall, upon completion of the training, acknowledge in writing that he/she has receipt of completion of the training. Employees must also read and re-sign Talladega's Information Systems Acceptable Use Policy (IT 1.11) annually. The training goals are to ensure that Employees:

- Understand and utilize techniques to minimize security threats
- Know how to respond to security incidents diligently
- Are aware of the policies, standards, and procedures that protect Talladega information assets

Talladega reviews and updates all training content on an annual basis to ensure that it reflects changes to Talladega regulatory and legal environment and policies.

8 TECHNICAL AND OPERATIONAL CONTROLS

8.1 INFORMATION PROTECTION, CLASSIFICATION, HANDLING AND MARKING

Addresses: STANDARD 681S2-00

8.1.1 Talladega Information Privacy Policy

The College has adopted an Information Privacy Policy, which establishes policies and procedures which protect the information it gathers and retains about students, employees, and community visitors. See Information Privacy Policy – IT 1.2.

8.1.2 Access & Storage of Confidential Data

- Only those employees or authorized third parties requiring access to Confidential data in the regular course of their duties are granted access to this data, including both physical and electronic records.
- To the extent possible, all electronic records containing Confidential data should only be stored within approved, secured information systems such as those provided by Jenzabar or ADP.
- Confidential data must not be stored on cloud-based storage solutions that are unsupported by the College (including DropBox, Microsoft OneDrive, Apple iCloud, etc.).

Talladega College Restricted Information
Do Not Distribute without Written Permission from Talladega College

- Paper records containing Confidential data must be kept in locked files or other secured areas when not in use. While storage in a locked office is minimally acceptable, employees should work with their supervisors to find solutions that offer greater long-term security, since many individuals have access to offices that are not their own.
- Upon termination of employment or relationship with Talladega College, electronic and physical access to documents, systems or other network resources containing Confidential and Restricted data is immediately terminated.

8.1.3 Transporting Confidential Data

- Members of the Community are strongly discouraged from storing Confidential data on laptops or on other mobile devices (e.g., flash drives, smart phones, external hard drives). However, if it is necessary to transport Confidential Data electronically, Talladega will provide an authorized asset owned by the college that will be encrypted for transporting data. Personal devices are not permitted to store or transport Confidential Data.
- Under no circumstances are documents, electronic devices, or digital media containing Confidential data to be left unattended in any unsecure location.
- When there is a legitimate need to provide records containing Confidential data to a third party outside Talladega College, electronic records shall be password-protected and/or encrypted, and paper records shall be marked confidential and securely sealed.

8.1.4 Destruction of Confidential Data

- Records containing Confidential data must be destroyed once they are no longer needed for business purposes, unless state or federal regulations require maintaining these records for a prescribed period of time.
- Paper and electronic records containing Confidential data must be destroyed in a manner that prevents recovery of the data. Certified destruction is used for all media that requires disposal. The State Of Alabama STANDARD 681S2-00 specifies the manner in which records containing PII must be destroyed.

8.1.5 Access and Storage of Restricted Data

- Access to Restricted Data is limited to members of the Community who have a legitimate business need for the data.
- Restricted Data can be stored on the College's eLearning learning management system, since this is a primary point of academic interaction between students and instructors.
- Documents containing Restricted Data should not be posted publicly.

8.1.6 College Email Policy

- Talladega College has adopted an Email Policy (IT 1.3) regarding the appropriate use of email, including the limits of sending Confidential and/or Restricted data through unencrypted email communication. It should be understood as a complementary policy to the guidelines contained in this Policy.

Talladega College Restricted Information
Do Not Distribute without Written Permission from Talladega College

8.2 ACCESS CONTROL

Addresses: STANDARD 681S2-00

Talladega manages access control, identification, and authorization through established policies and procedures that grant access using the principle of least privilege as the guiding tenet; the use of strong passwords, and the approval of access by the information owners. Access to information systems and its information usage is further re-enforced by banners. Access to Talladega assets is audited on a user and application level at defined frequencies and criticality. See User Account Review Policy – IT 1.7.

Upon termination employee shall be required to surrender all college assets, keys, IDs, access codes, badges, business cards, and the like, that permit access to the College's premises or information. Moreover, terminated employee's remote electronic access to Personally Identifiable Information will be disabled; his/her voicemail access, e-mail access, internet access, and passwords will be disabled or invalidated. If necessary, terminate employee's access may be extended for 30 days to provide continued access to College e-mail systems, as well as academic systems such as the College's (eLearning) Learning Management System, to facilitate the orderly conclusion of instructional responsibilities.

Talladega College has adopted a Remote Access Policy (IT 1.4) providing guidance for remote access to the College networks and data. It should be understood as a complementary policy to the guidelines contained in this Policy.

Talladega College has provided wireless access to students, and staff and faculty to access information assets while on campus. Access to both wireless networks, Talladega Student and Talladega Faculty, require assigned Active Directory credentials (username and password). For Faculty, all access by non-college assets will be only allowed through remote access, See Remote Access Policy – IT 1.4. Only Talladega College assets will be permitted to directly access the college network.

8.3 USER AUTHENTICATION AND PASSWORD CONTROL

Addresses: STANDARD 681S2-00

Talladega College has adopted a User Authentication and Password Control Policy (IT 1.5), which establishes policies and procedures covering user authentication, password control and network access. It should be understood as a complementary policy to the guidelines contained in this Policy.

8.4 CHANGE CONTROL AND CONFIGURATION MANAGEMENT

Talladega College has adopted a Change Control Policy (IT 1.9) regarding the change controls and documentation associated with changes to IT services. It should be understood as a complementary policy to the guidelines contained in this Policy.

8.5 PHYSICAL SECURITY

Addresses: STANDARD 681S2-00

Talladega College Restricted Information
Do Not Distribute without Written Permission from Talladega College

Talladega's work areas are secured to protect its information assets and ensure privacy. Documents and media are stored in a prescribed manner based on the policies and procedures governing information protection. Clean desk is strictly enforced. The College will ensure that all data centers and network distribution are equipped with automatic door closers and locking hardware to ensure the security of these facilities. Access to keys that will access these facilities will be restricted only to Information Technology Department (IT) staff members, and individuals with College roles which require access to all college facilities – in general, this should be limited to College administrators, plant maintenance staff, and security officers. A record of all individuals with keys granting access to data centers and network distribution facilities will be maintained by the College Security Office. All unauthorized employees, guests and/or vendors entering these facilities will be accompanied by a member of the IT Department staff.

Talladega's work environment is equipped with the required industry safety level controls - temperature and humidity controls, smoke detectors and fire suppression systems. Talladega reviews the appropriateness of the physical and environmental controls on an annual basis. Screen and laptop locks are required and in use. The college shall ensure all computer hardware is secured, either in locked rooms or with other security systems, to prevent loss from theft. The college shall maintain a hardware inventory for identification and retrieval purposes. Filling cabinets and drawers are locked when not in use. Building entry is controlled by security guides. Cameras are in effect and monitored.

8.6 Systems and Communication Protection

Addresses: STANDARD 681S2-00

Talladega has implemented key controls which are used to assure secure information transmission using the security principle of defense in depth. Talladega's system and communications protection strategy focuses on perimeter and boundary protections, network, gateways and application level malware and virus protections, public access protection and the use of encryption of information. The protections are governed by strict rules-based standards and processes of administration. Audit trail reviews are proactively conducted on a regular basis to alert on anomalies.

To combat external risks to the security, confidentiality, and/or integrity of any electronic records containing PII, the College has implemented, and will maintain, the following technical systems and processes:

- Redundant network firewall systems which are regularly updated with malware protection and operating system security patches.
- Antivirus and malware software that has been installed on all College servers and computer workstations. These software systems refresh their virus signature database files daily.
- Encryption software for College desktops, laptops and other portable devices, to prevent any loss of Confidential or Restricted data that might be inappropriately stored locally on these devices. Encryption here means the transformation of data using an algorithmic process, or an alternative method at least as secure, into a form in which meaning cannot be assigned without the use of a confidential process or key.

Talladega College Restricted Information
Do Not Distribute without Written Permission from Talladega College

- Virtual Private Networks have been established between the College and vendors providing critical hosting services for the College's Student Information Management System. These VPNs are encrypted to prevent external interception of Confidential or Restricted data.
- Operating system patches and security updates are installed to all servers on a regular basis.

8.7 Incident Reporting and Response Planning

Addresses: STANDARD 681S2-00

Any incident of possible or actual unauthorized access to or disclosure, misuse, alteration, destruction, or other compromise of PII, or of a breach or attempted breach of the information safeguards adopted under this Policy, must be reported immediately to the CISO, who will coordinate the College's response. Talladega ensures that all employees, contractors, and temporary workers are trained to report suspected incidents expediently.

Talladega College has adopted an Information Security Incident Response Policy (IT 1.6) regarding the response and reporting to any Information Security Incident. It should be understood as a complementary policy to the guidelines contained in this Policy.

8.8 Regular Monitoring and Detection of Security Failures

Addresses: STANDARD 681S2-00

The College's Information Technology staff will ensure regular internal network security audits are performed to all server and computer system logs to discover, to the extent reasonably feasible, possible electronic security breaches, and to monitor the system for possible unauthorized access to or disclosure, misuse, alteration, destruction, or other compromise of College data. Additionally, centralized logging systems are configured to look for anomalous behavior or unauthorized access to Confidential or Restricted data and provide alerts and regular reports to the CISO.

8.9 Contingency Planning

Talladega actively maintains a Business Continuity & Disaster Recovery Plan (IT 1.10), and an incident management process. The plans prioritize critical business applications and the infrastructure required to recover the business environment in the event of a disaster. The prioritization is determined using a Business Impact Assessment (BIA) which identifies the overall recovery objectives – recovery time objective (RTO), recovery point objective (RPO) and a maximum tolerable outage (MTO). Table top exercises are conducted once a year. Lessons Learned sessions are conducted after every activity and corrective action is taken with uncovered gaps. Talladega maintains both co-location and recovery sites to ensure availability. Talladega College has also adopted a Network Backup Policy (IT 1.8) regarding planning for information backups and network disaster recovery. It should be understood as a complementary policy to the guidelines contained in this Policy.

9 Enforcement

Addresses: STANDARD 681S2-00

Talladega College Restricted Information
Do Not Distribute without Written Permission from Talladega College

Any employee or student who willfully accesses, discloses, misuses, alters, destroys, or otherwise compromises Confidential or Restricted data without authorization, or who fails to comply with this Policy in any other respect, will be subject to disciplinary action, which may include termination in the case of employees and expulsion in the case of students.

10 POLICIES CROSS-REFERENCED

The following Talladega College policies provide advice and guidance that relates to this Policy:

- Information Privacy Policy – IT 1.2
- Email Policy – IT 1.3
- Remote Access Policy – IT 1.4
- User Authentication and Password Control Policy – IT 1.5
- Information Security Incident Response Policy – IT 1.6
- User Account Review Policy – IT 1.7
- Network Backup Policy – IT 1.8
- Change Control Policy – IT 1.9
- Business Continuity & Disaster Recovery Plan – IT 1.10
- Information Systems Acceptable Use Policy – IT 1.11

Talladega College Restricted Information
Do Not Distribute without Written Permission from Talladega College