TENNESSEE STATE UNIVERSITY

Information Security Policy

Policy No. 10.01

Contents

Document Change Control

Date	Version	Tech. Writer	Change/Review
05/31/2018	0.91		First Draft
01/07/2019	0.92		Section 5.1 and 5.3 revised for currency
02/12/2019	0.93		Added section 5.15 to address SaaS and email use
02/14/2019	0.94		Added FERPA
06/01/2020	1.0		Adopted
06/23/2022	1.1	bli@tnstate.edu	Formated consistently; Added network security administration policy fixed broken links.
08/28/2023	1.2	bli@tnstate.edu	Added the requirements of account passwords
09/12/2023	1.2	bli@tnstate.edu	Added a section to state standard for cybersecurity controls.

I.Overview and Purpose

Tennessee State University (TSU, TSU) has established this information security policy to provide security guidance and directive to its users, including students, faculty and staff, and vendor / third party personnel. Information security can be defined as the measures that protect the confidentiality, integrity, and availability of organization's data and information systems. TSU intends to implement security measures that protect the data of students and employees, as well as ensure the ongoing success of its mission.

As a policy, this document defines high-level mandates critical to reducing security risks across TSU but does not proscribe specific controls or procedures (which can be found in TSU's Security Standards). While the Office of Technology Services (OTS) will audit and facilitate validation for compliance with policy, TSU users and data owners are ultimately responsible and accountable for upholding the mandates described herein.

II.Roles and Responsibilities

A. Data Owner – The individual granted administrative control over a data or information asset. The data owner is typically a senior leader who understands how the data is used in the organization. Data owners are charged with classifying the data based on sensitivity, value, and confidentiality. This judgement determines who can view or manipulate the data, and well as the type of controls implemented to protect it.

B. Data Custodian – The individual charged with administering the data, the systems that support it, and the security controls requested by the data owner. They may help guide the data owner to an appropriate level of access and controls for a data asset. At TSU, most data custodians work in the Office of Technology Services (OTS).

C. Data User – An individual authorized by the data owner to access a data asset. Almost all students, employees, and vendor / third party workers at TSU are data users. Data users play a critical role in keeping TSU secure and TSU expects them to comply with policy as well as report suspicious events that could indicate a security incident or breach.

III.Scope

This policy applies to:

a. All data owned or managed by TSU.
b. All systems and infrastructure processing or storing TSU data.
c. All TSU students, employees, third party / vendor workers, and visitors accessing TSU data, systems, or infrastructure, whether electronically or physically.

IV.Policy Maintenance

The Chief Information Officer (CIO) and the Chief Information Security Officer (CISO) must review and approve information security policy at least once every year.

V.Standard for Cybersecurity Controls

TSU hereby adopts the current National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) as our standard for cybersecurity controls, with a commitment to follow any future amendments or updates.

VI.Data Classification

TSU classifies all data based on its value, sensitivity, and regulatory considerations. Classification determines how data is collected, stored, protected, and destroyed or wiped. TSU defines four categories of data:

Category	Description	Examples
Public	Data made available (intentionally) for public consumption.	• Brochures for prospective students, alumni, or parents • Marketing materials • Phone and email of customer / student facing university employ • Materials whose release to the public would not harm TSU's mi

Protected	Data that should be kept private, but which would not severely and directly endanger TSU's mission, student / employee privacy, or violate regulatory or compliance restrictions if released.	• Emails and phone numbers of faculty or staff who should not be • Departmental procedures or diagrams (not containing restricted • Academic materials (papers, PowerPoints, etc.) produced by a T • Employee or user IDs
Sensitive	Data that when released or lost could damage TSU's standing among other universities or otherwise result in a less competitive collegiate profile.	• Proprietary research • Strategic plans • Student transcripts • Audit results
Highly Sensitive	Data uniquely identifying students or employees and endangering their privacy or financial well-being.	• Protected Health Information (PHI)* • Financial data (including bank numbers and credit / debit card r • Personally Identifiable Information (PII)* • Data that when disclosed in an unauthorized manner would sub compliance standards, including HIPPA, PCI DSS, and GDPR • Passwords to TSU systems

PII – Any combination of data that could uniquely distinguish or trace an individual's identity, including (but not limited to): name, social security number, date and place of birth, mother's maiden name, or biometric records. (*Source: NIST Special Publication 800-122*).

PHI – Any element of a patient's medical record or payment history that can be uniquely linked to a specific individual. HIPPA identifies 18 record types that, when linked together so as to identify a specific individual, constitute PHI. Please refer to https://www.hipaajournal.com/what-is-considered-protected-health-information-under-hipaa/ for a complete list of identifiers.

VII.ACCEPTABLE USE

Users are expected to operate TSU assets and data for approved work-related purposes. The following is not meant as an exhaustive list of acceptable and unacceptable behaviors but a broad example of activities falling into these categories. Clarification should be sought from the Information Security Office if a particular activity is not certain.

1. General Acceptable Use

- Using resources only for authorized purposes.
- Accessing only information to which they have been given authorized access or that is publicly available.
- Using only legal versions of copyrighted software in compliance with vendor license requirements.
- Being considerate in the use of shared resources. Refrain from monopolizing systems, overloading networks with excessive data, degrading services, or wasting computer time, connection time, disk space, printer paper, manuals, or other resources.
- Restricting personal use of the TSU's information resources and technology to incidental, intermittent and minor use that is consistent with applicable law and TSU Policy.
- Storing confidential data only in TSU approved secured locations.
- Transmitting / transporting confidential data, information, and information assets only via TSU approved secured mechanisms.
- Using Bring Your Own Device (BYOD) in only TSU approved means.
- Reporting identified or suspected security incidents to the Information Security Office or OTS Support/Help Desk.

2. Unacceptable Use

The following uses of TSU assets and data are not approved and can result in punishment up to criminal charges and termination of employment:

- Engaging in any activity that is illegal under local, state, federal or international law, Effective Rules and Regulations of the State of Tennessee, and Polices and Guidelines of Tennessee Board of Regents.
- Browsing websites with inappropriate content (pornography or illegal activity such as drugs or gambling).
- Performing network or software scans without the approval of the Office of Technology Services
- Downloading software or tools that are not approved by OTS.
- Modifying system, computer, or application settings without prior approval from the owners or OTS.
- Attempting to access systems for which authorization has not been given, whether they are TSU

owned or owned by an external party.

- Downloading and / or using key loggers, password crackers, sniffers, or any other tool to compromise or crack passwords without explicit approval from OTS.
- Using TSU technology for inappropriate or abusive communication.
- Setting up servers, applications, or networks without explicit approval from OTS.
- Using TSU assets, data, or systems for personal profit or commercial purposes.
- Uploading TSU data to external, unapproved applications, websites (e.g., Dropbox, Google Drive, etc.), or using personal email accounts to conduct business.
- Taking action to deny services for TSU users (i.e., denial of service attacks).

VIII.AUTHENTICATION

Access to TSU's private networks, technology, and software must be secured with a username and password unique to each user. Accounts should never be shared among users, since shared use inhibits attribution. Software and device default passwords should be changed as quickly as possible. Multiple factors authentication (key fob, biometrics, smart card, etc.) is required to be used by all users with critical access and remote users.

IX.ACCESS AND ACCOUNT MANAGEMENT

A. Access to TSU networks and systems must be granted via a unique account(s) linked to a specific user. Access to TSU networks and systems should be granted on a least privilege model, wherein users are granted only the access required to perform their job duties. Wherever possible, system and network permissions should be bundled into "roles" mapping to job duties. This model of access provisioning, known as role-based access control (RBAC), allows for easier access administration and standardization of access across similar jobs.

B. All network and system access must be approved by the user's supervisor and the data owner. Access must be terminated in a timely manner upon employee termination, change of job role, end of contract or service with vendor, or any other event that renders any part of the user's access unnecessary. Permissions assigned to individual accounts, as well as groups / roles with permissions assigned to them, should be reviewed periodically by the user's supervisor or data owner to determine if the access remains appropriate and modified as needed.

C. Password Requirements
In line with the recommendation from NIST SP 800-63B Section 5.1.1.2 paragraph 9, which states, "Verifiers should not require memorized secrets to be changed arbitrarily (e.g., periodically). However, verifiers shall force a change if there is evidence of compromise of the authenticator." TSU does not mandate regular password resets. Instead, we emphasize a 16-character minimum password length, enforce MFA authentication, and promptly monitor and reset account passwords whenever compromised is detected.

X.DISASTER RECOVERY

A. OTS must work with TSU officials to maintain the Disaster Recovery Plan (DRP) to ensure the availability of systems supporting critical processes in the event of natural or man-made disaster. The DRP should be derived from the Business Continuity Plan and must list the IT systems and infrastructure supporting critical processes (as identified by TSU). The DRP must then detail how these systems will be made available within TSU-designated Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO). Further, the DRP must designate roles and responsibilities for disaster scenarios and include the contact information of responsible parties. Finally, an offsite, dedicated disaster recovery center must be maintained.

B. The DRP must be tested periodically. The results of the test must be recorded and used to modify the plan and/or TSU's recovery capabilities to ensure adherence to TSU's RTO and RPO.

XI.CHANGE MANAGEMENT

Changes to TSU applications must go through a formal change management process that ensures sufficient testing and approvals before implementation to a production environment. Separation of duties (SoD) should also be enforced between testers, approvers, and implementers.

XII.COMPUTER SECURITY INCIDENT RESPONSE

All TSU users are expected to report suspected indicators of compromise (IoC) to OTS. In addition, OTS must monitor TSU's systems, networks, and electronic data for IoCs. OTS must triage suspected IoCs; confirmed IoCs – known as incidents - must be contained and remediated as soon as feasible. If an incident meets a defined risk threshold, OTS will initiate TSU's Incident Response Plan, which may result in the involvement of one or more stakeholders (media relations, legal, HR, law enforcement, Ellucian Global Information Security, etc.) based on remediation and legal requirements. OTS' incident responders are required to document both potential and confirmed incidents and provide the results to the CISO.

XIII.ELECTRONIC DATA RETENTION AND DESTRUCTION

Requirements for the retention and destruction of digital data must be driven by TSU's broader data retention and destruction policies, standards, and guidelines. Using these guidelines, and with the assistance of Legal and HR, OTS shall develop and maintain requirements for retaining and disposing electronic data.

XIV.PHYSICAL SECURITY AND CLEAN DESK

TSU users and workers are expected to exercise precaution to protect TSU facilities, data, and IT assets from unauthorized physical access. Achieving these ends requires:

a. University campus guests to follow the established guest access policy.
b. Entry ways to non-public areas be locked and accessible only to authorized personnel.
c. Keys or cards not to be shared among employees.
d. Securing and supervision of workstations and other hardware hosting University data.
e. Locking away sensitive data when leaving the work area, whether it is on paper or stored on an electronic device.
f. Physically protecting IT assets, devices, cabling, and other infrastructure from tampering or theft and (as necessary) augmenting protection with monitoring capabilities, like security cameras.

XV.THIRD PARTY MANAGEMENT AND SYSTEM ACQUISITION

All purchases of software or IT services must follow the Procurement Department's formal purchasing process. In addition, OTS must be informed when any University department is considering contracting with an external organization to provide IT services or process TSU data. During the procurement process, OTS will assess the organization's ability to comply with TSU security standards and identify mitigating controls that TSU must implement to ensure the security of TSU data or system availability. Whenever possible, TSU must include security-specific service level agreements (SLAs) and right to audit clauses in contracts with third parties.

XVI.NETWORK SECURITY

Principle

TSU networks must be architected to isolate traffic and systems based on criticality, confidentiality, and regulatory considerations. Isolation techniques include, but are not limited to, firewalls rules, ACLs, VLAN, and network access control (NAC) software. Network devices (routers, switches, access points, etc.) should be configured to provide only required functions and secured based on vendor and leading practice guidelines. Firmware updates addressing security vulnerabilities should be promptly applied and unsupported network devices / software must be phased out in as soon as feasible. Finally, changes to device configurations, rulesets, and ACLs must be approved via the formal change management process.

Firewall and Router Security Administration

1. Responsibilities

- OTS network service is responsible for implementing and maintaining TSU firewalls, maintaining documentation of implemented rule sets including reference to ticket numbers, and for activities related to this policy.
- The TSU Information Security Office is responsible for review and approval/denial of all submitted firewall change requests and for coordinating periodic review of firewall rule sets and documentation.

2. Change Requests

- All firewall change requests must contain the following information: Source IP/network or hostname; Destination IP/network or hostname; Service name or port(s) required; and Business Reason for Change.
- Implementing a new system must include firewall port requirements as part of implementation planning and submit a firewall change request to support this effort.
- Firewall changes must be approved by the Information Security Office prior to being implemented unless the change is considered an emergency or necessary for the immediate resolution of a system/network outage.
- System or application administrators are responsible for submitting a change request upon the decommissioning of any system, service, or application.

3. Access Control

- Administrative access to TSU firewall(s) must be limited to only employees responsible for the maintenance and administration of the device(s).
- Administrative accounts should be created for each individual responsible for the maintenance and administration of the device(s). Generic accounts should not be used.
- Any Administrator accounts must be carefully protected.
- Default SNMP strings may not be used.
- Access to devices should be made using encrypted methods (SSHv2 or SSL if using a web interface).

4. Firewall Rule Review

- TSU firewalls will be reviewed annually by the Information Security Office to identify “stale rules” and excessive privileges allowing ‘any’ access, appropriateness of access.
- The Information Security Office will, upon consultation with appropriate application and system owners, submit tickets to have stale rules removed and/or excessive privileges reduced to apply least privilege principles.
- The Information Security Office will produce a “Firewall Rule Review” report after each review session to TSU OTS.

XVII.SYSTEMS SECURITY

Systems, including operating and database management systems, should be secured according to their respective hardening baseline, as created by OTS leveraging best practices and vendor recommendations. All systems should be configured to use the minimum number of services, modules, or packages to meet business requirements. System updates/patches addressing security vulnerabilities should be promptly applied and unsupported systems must be phased out in as soon as feasible. Based on data classification, data owners and custodians must consider augmenting system security with encryption, whether for data in-transit or at-rest. Finally, changes to critical system configurations or images must be approved via the formal change management process.

XVIII.RISK AND SECURITY ASSESSMENT

OTS (or a qualified third party) must conduct periodic security assessments to determine if users are following IT policies and standards, TSU applications, systems, and infrastructure are secured to meet TSU standards, and if existing TSU policies and standards address technology risks.

XIX.INFORMATION SECURITY AWARENESS

OTS is responsible for administering TSU’s information security awareness program. The program must include multiple methods for teaching users their role in identifying and preventing threats to the confidentiality, integrity, and availability of TSU’s systems and data. Methods for training users may include, but are not limited to posters and brochures, presentations and seminars, simulations, and video-based trainings.

XX.SECURE COMMUNICATION, EMAIL, AND SOFTWARE AS A SERVICE (SaaS)

A. TSU data must be transferred in accordance with data classification standards (see data classification above). Email is **not** a secure method of transmission and therefore should not be used for restricted or highly sensitive data. In addition, personal email accounts (Gmail, Yahoo, etc.) are not subject to OTS security controls or visibility and should never be used to conduct university business.

B. Hosted (internet-based) software solutions, also known as SaaS, such as Dropbox, DocuSign, and Google Drive are permitted **if reviewed and approved by OTS**. Uploading TSU data to unapproved SaaS applications is never permitted because TSU cannot validate if data is protected in accordance with university policy, regulations (FERPA, GDPR, etc.), and respect for student privacy.

XXI.NON-COMPLIANCE

University employees and contractors found to be violating this policy may be subject to recourse, up to and including termination. Third parties found to be violating this policy may be found in breach of contract and subject to recourse as defined therein.

XXII.TERMS AND DEFINITIONS

A. Confidentiality – Security rules and settings that restrict data and system usage to appropriate individuals.
B. Integrity – Security rules and settings that ensure data remains accurate and systems are used as intended.
C. Availability – Security rules and settings that ensure data and systems remain accessible.
D. Third Party – Any external entity involved in TSU's relationship with its students. This includes, but is not limited to, vendors, government agencies, and contractors.
E. IT assets - TSU-owned data, systems, and hardware.
F. Indicator of Compromise – Anomalous system or network activity that could indicate a computer intrusion. Includes, but is not limited to: loss of system functions, high traffic volume, downed or unresponsive sites, virus signatures, and pop ups claiming that your PC is infected.
G. Recovery Time Objective - the duration of time within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity.
H. Recovery Point Objective - the maximum period of data that can be lost from an IT service without unacceptable consequences regarding business continuity.

APPROVAL AND VERSION INFORMATION

2023-09-12 - Added a section to state standard for cybersecurity controls

2019-02-14 - Added FERPA considerations.

2019-02-12 - Added section 5.15 to address SaaS and email use.

2019-01-07 - Sections 5.1 and 5.3 revised for currency.

2018-05-31 - First draft