INFORMATION TECHNOLOGY SECURITY POLICY

Division: Information Technology

Policy Statement

Terra State Community College (TSCC) recognizes the critical importance of information security in the digital age. This Information Technology (IT) Security Policy outlines the principles, guidelines, and responsibilities for safeguarding the College's information assets and technology infrastructure. The policy is designed to protect the confidentiality, integrity, and availability of data and systems, ensuring compliance with applicable laws and regulations.

Policy Details

This policy is applicable to all members of the Terra State Community College community and applies to all locations and operations of the institution. Specifically, the scope of this policy includes:

- All faculty, staff, students, contractors, consultants, temporary, and other workers or guests using Terra State Community College's network and/or systems, and/or any other persons who are acting on, for, or on behalf of Terra State Community College;
- All institutional data, whether individually controlled or shared, stand-alone or networked, including but not limited to administrative, teaching and learning, licensed, or any other data related to Terra State Community College;
- All computer and communication facilities owned, leased, operated, or contracted by Terra State Community College and all devices that access or maintain institutional data, including but not limited to personal digital assistants, cell phones, personal computers, workstations, minicomputers, other wireless devices such as tablets, and any associated peripherals and software, regardless of whether used for administration, research, teaching or other purposes; and
- Third-party vendors who collect, process, share, transmit or maintain Terra State Community College institutional data, whether managed or hosted internally or externally.

Procedures

Information Classification and Handling

Information assets shall be classified based on their sensitivity and criticality into categories such as public, internal use, and confidential. Users must handle information in accordance with its classification and follow appropriate procedures for data storage, transmission, and disposal.

Data classifications:

- Public: Information intended for unrestricted access.
- Internal: Information intended for college personnel only.
- Confidential: Highly sensitive information, including student records, financial data, and intellectual property.

Handling and Storage

- Public data should be handled with care but can be stored on standard systems.
- Internal data should be stored on secure systems and shared on a need-to-know basis.
- Confidential data requires special handling, encryption, and access controls.

Access Control

Access to IT resources shall be granted on a need-to-know basis. User access is only granted to a system containing sensitive data upon an initial request from the user's supervisor and subsequent approval by an authorizing authority. Each system will have a designated authorizing authority that manages end user access to the system. More specifics can be found in the procedures that pertain to each specific system.

User Authentication

- Users must authenticate using strong, unique passwords.
- Multi-factor authentication (MFA) is mandatory for access to sensitive systems with confidential data.

Account Management

- User accounts must be created, modified, and terminated promptly following established procedures.
- Accounts with unused access must be reviewed and deactivated regularly.

Data Protection

Data privacy laws and regulations, as well as Terra State's data protection policies, shall be strictly adhered to. Personally identifiable information (PII) and sensitive data shall be collected, processed, and stored securely and only for legitimate purposes.

- Data in transit must be encrypted using secure protocols.
- Regular backups of critical data must be performed and tested.
- A disaster recovery plan must be in place.

Acceptable Use

All users are expected to use IT resources responsibly and ethically. This includes refraining from unauthorized access, distribution of malicious software, harassment, copyright violations, and other activities that may compromise the security and functionality of the IT environment as outlined in the Acceptable Use Policy.

Security Awareness and Training

Regular security awareness programs and training sessions shall be conducted to educate users about IT security best practices, phishing prevention, and other relevant topics to enhance their understanding of potential risks and mitigation strategies.

Physical Security

All equipment must be maintained in a secure environment. Physical access to IT infrastructure, including server rooms and data closets, shall be restricted to authorized personnel only. Appropriate physical security measures, such as access controls, surveillance, and environmental controls, shall be implemented to safeguard the equipment. Access must be authorized by job function only and revoked immediately upon job termination.

Hardware Security

The Information Technology department will establish and maintain a system that ensures that all pieces of equipment are properly accounted for and configured.

Incident Reporting and Response

Any suspected or confirmed IT security incidents, including breaches, unauthorized access, malware infections, and data loss, must be promptly reported to the IT department by submitting a help ticket to the IT Help Desk. The college will follow a defined incident response plan to mitigate and manage such incidents effectively.

Compliance

Terra State Community College will adhere to all applicable federal, state, and local laws and regulations regarding information security.

Remote Access and Mobile Devices

Remote access to college resources and the use of mobile devices shall follow secure protocols and practices. Devices used to access college systems remotely must adhere to security configurations and encryption standards.

Network Security

Firewalls must be implemented to protect the network from unauthorized access and threats. Regular firewall rule reviews are mandatory to identify and mitigate security risks.

Wi-Fi networks must be secured to current best security practices. Guest networks will be isolated from internal networks, and guest access will be granted for a limited duration.

All users accessing the network, both wired and wireless, must agree to the College's Acceptable Use policy each time a connection is established.

Software and Patch Management

All software must be obtained from legitimate sources and properly licensed. Regular security patches and updates must be applied to operating systems, applications, and devices to address known vulnerabilities.

Third-Party Security

Third-party vendors and contractors who have access to Terra State's IT resources must adhere to security requirements outlined in their contracts and agreements. The college reserves the right to assess the security practices of third parties.

Responsibilities:

All Terra State Community College faculty, staff, students, and contractors are expected to:

- Follow Terra State Community College's Acceptable Use Policy.
- Understand this IT Security Policy.
- Understand the type of information they store, transmit or process and protect the information in compliance with this policy.

Enforcement

Any violation of this Policy may result in actions as defined in the Progressive Action Policy as well as:

- Revocation of access privileges.
- Academic penalties.
- Responsibility for remediation costs associated with a security incident.
- Regulatory non-compliance penalties.
- Disciplinary action up to and including termination of employment or contractor status with Terra State Community College.
- Other penalties including but not limited to financial penalties, civil or criminal proceedings, legal fees, and other costs.

Review and Revision

This policy will be reviewed on an annual basis to ensure its relevance and effectiveness in addressing emerging IT security threats and challenges. Revisions will be made as necessary and communicated to all relevant stakeholders.

Adherence to this IT Security Policy is vital to maintaining the confidentiality, integrity, and availability of Terra State Community College's information technology resources. All members of the Terra State community are expected to understand and follow the guidelines outlined in this policy.

Resources

Acceptable Use Policy

Documentation

Definitions

Term	**Definition**

*Personally Identifiable Information (PII_*	Any data element that can be used to unequivocally identify a person such as, but not limited to, Social Security Number, Driver's License Number, face, credit card number, digital identity.
Multi-Factor Authentication	An electronic authentication method where an end user is granted access only after presenting two or more factors of identification to an application or website. Factors typically are something you know (i.e., password), something you have (i.e., token), or something that you are (i.e., biometrics)

Approval History

Date	Policy/Procedure or Entire Document	Notes (Types of Actions)	**Approved by
5/25/2005	Policy	Issued	Unknown
2/5/2024	Entire Document	Transferred to new template, updated policy and procedure	Wayne Yerdon, CIO

**Full name of CASA Committee Chair, signatory, or designee

Effective Date: 5/25/2005

Next Review Date: 2/28/2025