TERRA STATE COMMUNITY COLLEGE

RED FLAG POLICY

Division: Information Technology

Policy Statement

The purpose of the Red Flag Policy is to establish an Identity Theft Prevention Program for TSCC designed to detect, prevent, and mitigate identity theft pursuant to the Federal Trade Commission's (FTC) Red Flags Rule for the security of sensitive information and maintaining the trust of those we serve.

Policy Details

Terra State Community College (TSCC) is committed to safeguarding the personal and financial information of our customers, employees, and stakeholders. Identity theft poses a significant risk to individuals and our business

The College creates, obtains, and stores personally-identifiable financial and other sensitive information, and desires to ensure appropriate measures are taken to prevent identity theft involving such information. Therefore, the College shall maintain an active identity theft program in accordance with Federal Trade Commission regulations enacted at 16 C.F.R. 681 et. seq. (often referenced as the "red flag rule").

This policy applies to all employees, contractors, vendors, and third parties who have access to personal or financial information within our organization.

Red Flag Indicators

The following are examples, but not a complete list, of red flag indicators that require heightened attention and prompt action:

1. Unauthorized access or attempts to access sensitive systems or data.
2. Unexplained discrepancies in customer, employee, or vendor information.
3. Alerts or notifications from credit reporting agencies regarding potentially fraudulent activities.
4. Suspicious account activity, such as unauthorized withdrawals or transfers.
5. Requests for changes in account information without proper documentation.
6. Multiple failed login attempts on user accounts.
7. Lost or stolen company-issued identification or access cards.
8. Unauthorized changes to billing or payment information.
9. Sharing of personally identifiable information through an insecure medium such as regular email

Procedures

Prevention Measures

a. Secure Access: The College will implement strong access controls and authentication methods to ensure only authorized personnel can access sensitive information.

b. Employee Training: The College will offer regular training sessions to educate employees about identity theft risks, prevention techniques, and how to recognize red flag indicators.

c. Data Protection: Encrypt sensitive data both in transit and at rest to minimize the risk of unauthorized access. When encryption is not feasible, data will be secured by using effective alternative controls approved by the program's compliance officer.

d. Document Management: Establish secure document storage and disposal procedures to prevent unauthorized access to physical records.

Detection and Reporting

a. Monitoring: Implement monitoring of systems and accounts to detect unusual or suspicious activities.

b. Reporting: Encourage employees to promptly report any red flag indicators or suspected identity theft incidents to the designated point of contact.

c. Incident Response: Establish a clear incident response plan detailing steps to be taken in the event of a suspected identity theft incident. This includes immediate containment, investigation, and communication protocols.

Compliance and Oversight

a. Periodic Reviews: Conduct regular reviews of this policy and associated procedures to ensure their effectiveness and relevance.

b. Compliance Officer: Designate an individual responsible for overseeing the implementation and enforcement of the policy.

Consequences of Non-Compliance

Failure to comply with this policy may result in disciplinary action, up to and including termination of employment or contractual relationships, as well as legal consequences if applicable.

Communication

This policy shall be communicated to all relevant parties and made accessible through TSCC's internal communication channels and official website.

Resources

Red Flags Rule = https://www.ftc.gov/business-guidance/privacy-security/red-flags-rule

Part 681 – Identity Theft Rules = https://www.ecfr.gov/current/title-16/chapter-I/subchapter-F/part-681

Documentation

Definitions

Term	**Definition**
Red Flag	A pattern, practice, or specific activity that would indicate the potential for, or existence of, possible identity theft.
Identity Theft	A fraudulent act that is committed or attempted using the identifying information of another person without that person's authority.
Personal Identifying Information (PII)	Any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including: name, address, telephone number, social security number, date of birth, bank account or credit card numbers, government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number, or student identification number.
Covered Account	An account that Terra State Community College offers or maintains and is designed to permit multiple payments or transactions for which there is a reasonably foreseeable risk to the account information from identity theft, including financial, operational, compliance, reputation, or litigation risks. Examples include, but are not limited to, deferred payment plans, student loans, emergency loans, institutional

	loans, federal work study programs, student billing and receivables, student refunds, accounts in collection, and student records.

Approval History

Date	Policy/Procedure or Entire Document	Notes (Types of Actions)	**Approved by
11/01/2009	Entire Document	Issued	Unknown
10/17/2023	Entire Document	Revision of Policy Transfer to new policy template	Wayne Yerdon, Chief Information Officer

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

Effective Date: 11/01/2009

Next Review Date: 10/31/2026