Treasure Valley Community College

Code:	EDCA
Adopted:	6/15/21
Revised/Readopted:	4/18/23

Information Security

Purpose:

The purpose of the Information Security Policy is to clearly establish the College's role in protecting its information assets and communicate minimum expectations for meeting these requirements. Fulfilling these objectives enables the College to implement a comprehensive system-wide Information Security Program. This Policy also assists the College in fulfilling responsibilities relating to the protection of information assets, and compliance with regulatory and contractual requirements involving information security and privacy.

TVCC's Information Security Policy framework consists of separate Policy statements based on guidance provided by the National Institute of Standards and Technology (NIST) Special Publication 800-53.

Although no set of policies can address every possible scenario, this framework, taken as a whole, provides a comprehensive governance structure that addresses key controls in all known areas needed to provide for the confidentiality, integrity, and availability of the institution's information assets. This framework also provides administrators guidance necessary for making prioritized decisions, as well as justification for implementing organizational change.

Scope:

The scope of this policy includes all information assets governed by the College. All personnel and service providers who have access to or utilize information assets of the Institution, including data at rest, in transit or in process shall be subject to these requirements. This Policy applies to all information assets operated by the College and all information assets provided by the College through contracts, subject to the provisions and restrictions of the contracts; and all authenticated users of Treasure Valley Community College information assets.

All third parties with access to the Institutions' non-public information must operate in accordance with a service provider contract containing security provisions consistent with the requirements promulgated under, but not limited to the Gramm-Leach-Bliley Act (GLBA), Family Educational Rights and Privacy Act (FERPA), and the Payment Card Industry Data Security Standard (PCI-DSS).

Implementation:

Treasure Valley Community College needs to protect the availability, integrity and confidentiality of data while providing information resources to fulfill our academic mission. The Information Security Program must be risk-based. Implementation decisions must be made based on addressing the highest risk first. The College's administration recognizes that fully implementing all controls within the NIST Standards is not possible due to organizational limitations and resource constraints. Administration must implement the NIST standards whenever possible, and document exceptions in situations where doing so is not practical.

Roles and Responsibilities:

The College has identified the following roles and responsibilities for IT Security:

1. College President: The President is accountable for the implementation of the Information Security Program including:

    a. Security Policies, Standards, and procedures
    b. Security Compliance including managerial, administrative, and technical controls.

    The President is to be informed of Information security implementations and ongoing development of the Information Security Program design.

2. College Administrative Team: This group is responsible for the oversight and compliance functions of the Information Security Program for Treasure Valley Community College. The group consists of individuals who report directly to the College President who have specific operational responsibilities.

3. Chief Information Security Officer: This role is responsible for the development, implementation, and maintenance of a comprehensive Information Security Program for Treasure Valley Community College. This includes security policies, standards and procedures which reflect best practices in information security. The College currently has designated the Chief Information Officer as its Chief Information Security Officer (CISO), and for the purposes of GLBA compliance, describes this role as its Qualified Individual.

Information and System Classification

The College must establish and maintain security categories for both information and information systems.

Information Security Standards

The Information Security Policy is framed on National Institute of Standards and Technology (NIST) and controls implemented based on the Center for Internet Security (CIS) Critical Security Controls priorities. Treasure Valley Community College must develop appropriate control standards and procedures required to support the College’s Information Security Policy.

This policy is further defined by control standards, procedures, control metrics and control tests to assure functional verification and is based on NIST Special Publication 800-53; this publication is structured into 18 control groupings, herein referred to as Information Security Standards. These Standards must meet all statutory and contractual requirements, including but not limited to the Gramm-Leach-Bliley Act (GLBA), Family Educational Rights and Privacy Act (FERPA), and the Payment Card Industry Data Security Standard (PCI-DSS).

1. ACCESS CONTROL (AC)

The College must limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.

2. AWARENESS AND TRAINING (AT)

The College must: (i) ensure that managers and users of information systems are made aware of the security risks associated with their activities and of the applicable laws, directives, policies, standards, instructions, regulations, or procedures related to the security of College information systems; and (ii) ensure that College personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

3. AUDIT AND ACCOUNTABILITY (AU)

The College must: (i) create, protect, and retain system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity on protective enclave systems, specific to confidential data and confidential networks, at a minimum; and (ii) ensure that the actions of individual information system users can be uniquely traced for all restricted systems.

4. ASSESSMENT AND AUTHORIZATION (AA)

The College must: (i) periodically assess the security controls in College information systems to determine if the controls are effective in their application; (ii) develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in College information systems; (iii) authorize the operation of the College’s information systems and any associated information system connections; And (iv) monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.

5. CONFIGURATION MANAGEMENT (CM)

The College must: (i) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems.

6. CONTINGENCY PLANNING (CP)

The College must establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for the College’s information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.

7. IDENTIFICATION AND AUTHENTICATION (IA)

The College must identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to the College information systems.

8. INCIDENT RESPONSE (IR)

All security incident detections and responses, especially those related to critical systems, will adhere to documented and implemented incident response processes and procedures in order to mitigate risk, reduce costs, and minimize system downtime.

This policy shall be subject to and superseded by applicable regulations and laws.

The CISO shall document and implement incident response plans and procedures that address security incident detection and response.

This shall include standards and procedures for:

a. Incident identification
b. Incident severity & classification
c. Incident declaration & reporting

All TVCC employees shall be responsible for detecting security incidents, notifying appropriate personnel, and facilitating the incident response plan and procedures.

The CISO, or available member of the Information Technology staff, shall be notified immediately of any suspected or confirmed security incidents involving TVCC computing assets, particularly those impacting critical systems.

To assure the integrity of the incident investigation and recovery process, the CISO shall oversee any investigative or corrective action.

9. MAINTENANCE (MA)

The College must: (i) perform periodic and timely maintenance on College information systems; and (ii) provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.

10. MEDIA PROTECTION (MP)

The College must: (i) protect information system media, both paper and digital; (ii) limit access to information-on-information system media to authorized users; and (iii) encryption, where applicable, (iiii) sanitize or destroy information system media before disposal or release for reuse.

11. PHYSICAL AND ENVIRONMENTAL PROTECTION (PE)

The College must: (i) limit physical access to information systems, equipment, and the respective operating environments to authorized individuals; (ii) protect the physical resources and support infrastructure for information systems; (iii) provide supporting utilities for information systems; (iv) protect information systems against environmental hazards; and (v) provide appropriate environmental controls in facilities containing information systems.

12. PLANNING (PL)

The College must develop, document, periodically update, and implement security plans for College information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems.

13. PERSONNEL SECURITY (PS)

The College must: (i) ensure that individuals occupying positions of responsibility within organizations are trustworthy and meet established security criteria for those positions; (ii) ensure that College information and information systems are protected during and after personnel actions such as terminations and transfers; and (iii) employ formal sanctions for personnel failing to comply with information security policies and procedures.

14. RISK ASSESSMENT (RA)

The College must periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information.

15. SYSTEM AND SERVICES ACQUISITION (SA)

The College must: (i) allocate sufficient resources to adequately protect College information systems; (ii) employ system development life cycle processes that incorporate information security considerations; (iii) employ software usage and installation restrictions; and (iv) ensure that third- party providers employ adequate security measures, through federal and Oregon state law and contract, to protect information, applications, and/or services outsourced from the organization.

16. SYSTEM AND COMMUNICATIONS PROTECTION (SC)

The College must: (i) monitor, control, and protect College communications (i.e., information transmitted or received by college information systems) at the external boundaries and key internal boundaries of the information systems for confidential data transmissions; and (ii) employ architectural designs, software development techniques, encryption, and systems engineering principles that promote effective information security within college information systems.

17. SYSTEM AND INFORMATION INTEGRITY (SI)

The College must: (i) identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within the College information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response.

18. PROGRAM MANAGEMENT (PM)

The College must implement security controls to provide a foundation for the organizational information security program.

Enforcement

The College may temporarily suspend or block access to any individual or device when it appears necessary to do so in order to protect the integrity, security, or functionality of institution and computer resources. Violations of this policy may result in penalties and disciplinary action in accordance with the Student Handbook, Employee Handbook and/or rules governing employment at Treasure Valley Community College.

Privacy

The College will make every reasonable effort to respect a user's privacy. However, faculty, staff and students do not acquire a right of privacy for communications transmitted or stored on College resources.

In addition, in response to a judicial order or any other action required by law or permitted by official College policy or as otherwise considered reasonably necessary to protect or promote the legitimate interests of the College and the College community, the President may authorize the Chief Information Officer, or an authorized agent, to access, review, monitor and/or disclose computer files associated with an individual's account.

Disclaimer

Treasure Valley Community College disclaims any responsibility for and does not warrant information and materials residing on non-College systems or available over publicly accessible networks. Such materials do not necessarily reflect the attitudes, opinions or values of Treasure Valley Community College, its faculty, staff, or students.

Related Document and Forms

- The Gramm - Leach Bliley Act (GLBA)
- Family Educational Rights and Privacy Act (FERPA)
- Oregon 2017 ORS 656A.604 Notice of breach of security
- NIST 800-53, FIPS-199
- PCI DSS 3.1
- Information Technology Appropriate Use Policy
- Information Security Training and Awareness Policy END OF POLICY

END OF POLICY