Treasure Valley Community College

Code: EDCAA
Adopted: 6/15/21

Information Security Training and Awareness Policy

Purpose:

The purpose of the Information Security Training and Awareness Policy is to clearly establish the College's role in protecting its information assets and communicate minimum expectations for meeting these requirements. This Policy also assists the College in fulfilling responsibilities relating to the protection of information assets, compliance with regulatory and contractual requirements involving information security and privacy and preventing cybercrimes.

Policy

TVCC's information security awareness, training and education program strives to ensure that the College community achieves and maintains at least a basic level of understanding of information security matters, such as general obligations under various information security policies, standards, procedures, laws, regulations, contractual terms and generally held standards of ethics and acceptable use of information resources.

Security awareness and training activities are initiated as soon as practical after faculty, staff and/or a student worker has been employed. The training and awareness activities are conducted on a continuous basis thereafter in order to maintain a reasonably consistent level of awareness.

All authorized users with access to Institutional Data and IT Resources receive sufficient training to allow them to adequately protect Institutional Data and IT Resources.

Additional and specific training are required for personnel with responsibilities related to programming, administering, and securing systems and for specific College community members with access to Controlled Sensitive Data in accordance with compliance laws and regulations.

Training Program

The IT Department and the Human Resources Department are responsible for developing and maintaining a program to provide:

- Initial and ongoing security awareness training on acceptable use of IT resources to the College community.
- Proper information security training as related to functional responsibilities.
- Educational opportunities to ensure information security personnel are equipped with the necessary security skills, knowledge, and competencies.
- All employees' acknowledgement in writing that they have read and understood TVCC's Information Security Policy.

- Information security training that is incorporated into the new hire and new contractor orientation processes. Access to systems may not be provided until training is completed and a signed acknowledgment of security training has been received by the IT Department.
- Annual information security awareness refresher training that must be completed by all administrators, faculty, staff, student workers and authorized users.
- Specialized security training applicable to their functions for information system security personnel with responsibilities related to administering and securing systems. Acknowledgment of having received specialized security training must be submitted to CIO before administrative access can be given to any TVCC's systems.

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.

Definitions:

Authorized Users: Includes faculty, administrators, staff, student workers, graduate/technical assistants, alumni, interns, guests or agents of the administration, external individuals and organizations accessing who have access to or utilize information assets of the college, including data at rest, in transit or in process.

Chief Information Officer (CIO): Senior manager of the Information Technology (IT) Department and a member of TVCC's Administrative Team.

College Community: Includes faculty, administrators, staff, student workers, graduate/technical assistants, alumni, interns, guests or agents of the administration, external individuals and organizations accessing St. John's network services, and other authorized users.

Controlled Sensitive Data (CSD): A general categorization that is used in TVCC's Information Technology (IT) policies (primarily the Information Security Policy and the Acceptable Use Policy) to represent all confidential and private information governed by those policies. CSD includes: PII, PHI, HIPAA, FERPA, regulated, private, personal, or sensitive information for which TVCC is liable if publicly disclosed.

Cybercrime: Criminal activity or a crime that involves the Internet, a computer system, or computer technology.

Data Breach: Generally, an incident in which sensitive, protected, or confidential data has potentially been viewed, stolen, or used by an individual unauthorized to do so. Note: Although "breach" is a commonly used term in the information security community, legally, the term "breach" tends to only be used when a security event reaches the threshold of regulatory reporting. TVCC will use the terms "incident" or "compromise" until it can be determined whether an event satisfies the legal definition of a breach.

Information Technology Resources: (At TVCC) All Information Technology (IT) resources that are the property of TVCC and include, but are not limited to, all network-related systems; business applications; network and application accounts; administrative, academic and library computing facilities; college-wide data, video and voice networks; electronic mail; video and web conferencing systems; access to the Internet; voicemail, fax machines and photocopiers; classroom audio/video; computer equipment; software and operating systems; storage media; Intranet, VPN, and FTP.

IT Resources include resources administered by IT, as well as those administered by individual departments, college laboratories, and other college-based entities.

Institutional Data: All data owned or licensed by TVCC.

END OF POLICY
