Treasure Valley Community College

Code: EHBA
Adopted: 4/18/23

Information Incident Response

In the event of an information security incident, it is critical to respond and resolve the issue as quickly and effectively as possible. TVCC shall maintain documented procedures, processes, roles, and responsibilities so that TVCC may respond promptly. Procedures and processes are accessible through the Chief Information Security Officer (CISO) or Office of Public Information.

Any information security related incident, breach, or compromise affecting critical data for which TVCC upholds or causes disruption to TVCC's normal operation 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This policy shall be subject to and superseded by applicable regulations and laws.

1. 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

2. All TVCC employees shall be responsible for notifying appropriate personnel of any security incident.

Violations of TVCC Information Incident Response may result in, but not be limited to:

- Deactivate any User's access rights when necessary to preserve the integrity of resources.
- Disciplinary Action in accordance with TVCC Human Resources and/or Student Conduct guidelines.
- Violations may include reporting to Federal, State, and/or Local authorities regulating computer and network use.
- Be held liable for damages, including but not limited to the loss of information, computer software/hardware, lost revenue, and fines and judgments imposed as a direct result of the violation.

Governing standards, policies, and guidelines:

- US Dept of Education: Guidance Letter – Protecting Student Information
- US Dept of Education: Family Educational Rights and Privacy Act (FERPA)
- US Dept of Homeland Security: Federal Information Security Management Act (FISMA)
- Gramm-Leach-Bliley Act (GLBA)
- FTC Red Flags Rule
- Health Insurance Portability and Accountability Act (HIPAA)
- International Organization for Standardization (ISO)

- National Institute Standards and Technology (NIST)
- Payment Card Industry Data Security Standard (PCI DSS)
- Sarbanes-Oxley (SOX) for Colleges and Universities

END OF POLICY
