TREASURE VALLEY
COMMUNITY COLLEGE

AP 3805 Patch and Vulnerability Management

References:

The purpose of the Patch and Vulnerability Management (PVM) procedure is to require all Information Technology (IT) resources connected to the College's networks be routinely reviewed and patched to maintain secure business operations and performance.

The PVM procedure must include the following components:

- An inventory and prioritization of the types of devices which will be reviewed under this procedure
- An inventory of Software-as-a-service solutions that are outside of the IT Department's ability to patch and maintain; this inventory should include documentation about how to contact vendors to report vulnerabilities and other security concerns
- A systematic approach to a college-wide practice of patch and vulnerability management. This approach should include distinct phases for discovery, prioritization, planning, remediation, and validation
- A regular schedule for the review, testing, and application of new security patches
- A listing of identified individuals and their responsibilities associated with patch and vulnerability management
- Processes for addressing proposed exceptions to the policy; all exceptions must be approved by the CISO.

Definitions:

IT Resources include college owned computers, networking, communications, application, and telecommunications systems, infrastructure, hardware, software, data, databases, procedures, physical facilities, cloud-based vendors, Software as a Service (SaaS) vendors, and any related materials and services.

A **patch** is a software update comprised of code inserted (i.e., patched) into the code of an executable program. Typically, a patch is installed into an existing software program. Patches are often temporary fixes between full releases of a software package. Patches include, but are not limited to, the following:

- Upgrading operating systems and/or software applications
- Fixing a software bug
- Installing new drivers
- Addressing security vulnerabilities
- Addressing software stability issues

Remediation is an effort that resolves or mitigates a discovered vulnerability.

Vulnerability is a flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy.

Vulnerability management is the practice of identifying, classifying, remediating, and mitigating vulnerabilities.

Oversight and enforcement of the procedure shall be the responsibility of the CISO as well as identified members of the Information Technology Department. (The College currently has designated the Chief Information Officer as its CISO.)

Adopted: 08/20/24