BP 3805 Patch and Vulnerability Management

References:

The Chief Information Security Officer (CISO) and IT Department shall develop and maintain a Patch and Vulnerability Management (PVM) procedure to ensure all college owned electronic devices connected to the College networks are routinely reviewed and updated with security updates and software patches to maintain a secure and well-performing operational environment.

This policy applies to all IT resources connected to the College networks, and to college employees and contractors who create, deploy or support IT infrastructure, devices or software.

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.

END OF POLICY

Adopted: 08/20/24