OFFICE OF INFORMATION TECHNOLOGY
IT RESOURCE & INFO SYSTEM SECURITY & VULNERABILITY MANAGEMENT

I. PURPOSE AND SCOPE

The purpose of rule is to protect the college's IT resources and information systems, detect and remediate security vulnerabilities, and ensure that IT resources and information systems are available for authorized use.

II. DEFINITIONS

A. **Information Asset:** data or knowledge stored in any electronic manner and recognized as having value for the purpose of enabling the college to perform its business functions.

B. **Information System:** an application or group of servers used for the electronic storage, processing, or transmitting of any College data or Information Asset.

C. **IT Technician:** a college employee who uses industry best practices to develop, administer, manage, and monitor computer resources and assets that support the college's IT infrastructure and ensure compliant IT system security.

D. **IT Resource:** any computer resource used to perform college business operations including, but not limited to, the creation, access, storage, processing, and transmission of information assets. (i.e., server, workstation, mobile device, networking device, web camara, etc.).

E. **User:** any person, including students, staff, faculty, temporary employees, contractors, vendors, research collaborators, and third-party agents, who accesses any college electronic resources, information systems, and/or IT resources.

III. PROCEDURES

A. IT Resource Classifications

1. The Office of Information Technology (OIT) categorizes IT resources by type based on the ownership, function, and physical location.

2. The college analyzes the physical surroundings of IT resources to prevent and preclude unauthorized access and limit the ability of unauthorized persons to view sensitive information.

B. Anti-Virus and Endpoint Security

1. OIT conducts information asset monitoring is conducted on college-owned assets to detect the presence of unapproved files and unauthorized software installations.
2. OIT must configure anti-malware and/or endpoint security scanning to run automatically on college-owned assets.
3. IT Technicians will subscribe to reputable sources to receive notifications for warning bulletins, and notifications to differentiate between hoaxes and verifiable malicious codes.

C. Vulnerability Management

1. The College must monitor vendor and third-party sources for updated vulnerability information and distribute pertinent patch information to responsible parties without unreasonable delay.
2. OIT categorizes vulnerabilities according to the following severity levels, and align these classifications with proprietary vulnerability management tool scores as appropriate:
    a. Critical: vulnerabilities involving a potential leak of sensitive information and local exploits where the risk of compromise is not as high as a critical vulnerability. These include vulnerabilities that may allow an intruder to:
        i. gain control of one or more information systems; or
        ii. gain full read access to files, potential backdoors, or a listing of all the users on the host.
    b. High: vulnerabilities that may allow an intruder to gain access to specific information stored on the host, including security settings or potentially misuse the host, such as:
        i. access to a partial disclosure of file contents;
        ii. access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms; or
        iii. denial of service attacks, and unauthorized use of services, such as mail-relaying.
    c. Medium: vulnerabilities that may allow an intruder to easily exploit known vulnerabilities specific to software versions, such as:

i. information assets stored on an information system; or

ii. sensitive information from the host, such as the precise version of software installed.

d. Low / Informational: vulnerabilities that do not pose an immediate threat to the college information systems. Intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.

3. When a patch cannot be installed due to incompatibility with an IT resource or information system, testing requirements, or other pertinent patching limitations, an exception must be recorded within a risk register by the Information Security Office and periodically reviewed for potential recategorization and/or remediation.

D. Patch Management

1. OIT must take mitigation measures when a vendor releases a patch or update to repair a security-related control, if the release is categorized as a critical vulnerability

2. All patch and update procedures shall be conducted in accordance with the College's Change Management Rule and Procedures.

3. Where available, IT Technicians should install patches on a non-production (or lower impact) system, if available, to verify that the security patch will not adversely impact system functionality.

4. OIT must ensure IT Resources and Information Systems are hardened according to applicable industry best security practices prior to release into the production environments.

5. OIT must implement mitigation procedures must if vulnerabilities are exploitable and/or exploited before they can be removed from the environment.

6. When appropriate, OIT shall conduct security monitoring and scanning with vulnerability scanning tools to verify that remediation activities have been performed.

E. Operating System Access Controls

1. OIT requires the following secured log-on procedures:

a. provide appropriate means for authenticating authorized users;

b. limit the number of unsuccessful log-on attempts;
c. record unsuccessful log-on attempts;
d. auto-lock and/or auto-logoff sessions due to inactivity; and
e. issue alarms when security requirements are breached.