INFORMATION SECURITY-SECURE OPERATIONS

1.0 Purpose and Scope

The objective of this Administrative Regulation is to describe policies for secure operations of Yosemite Community College District (YCCD) information and systems. The following topics are covered:

- Operations Processing
- Malware Management
- Patches and Updates
- Backups and Media
- Third Party Management

This is one of a series of information security Administrative Regulations maintained by the District Information Technology Services (ITS) department designed to protect YCCD information systems.

1.1 Applicability of Assets

This Administrative Regulation applies to all electronic assets that are owned or leased by YCCD, including but not limited to:

- Desktop and Laptop Computers
- Mobile Devices
- Servers
- Network Infrastructure

1.2 Applicability to all Employees and Volunteers

This Administrative Regulation applies to all Board of Trustees authorized/ratified full-time and part-time regular Academic and Classified employees, Substitutes, Short-term (Temporary) staff, Professional Experts, College Work Study students, Student Help and Volunteers who are employed in the Yosemite Community College District for the purpose of meeting the needs of students.

1.3 Applicability to External Parties

This Administrative Regulation applies to all external parties, including but not limited to YCCD business partners, vendors, suppliers, outsource service providers, and other third party entities with access to YCCD networks and system resources.

2.0 Secure Operations

2.1 Operations Processing

All system scheduling, jobs, and dependencies must be documented. This documentation must include job start times, latest job completion times, delay procedures and handling procedures in case of failure or error.

Operating system and application processing, restart and shutdown procedures must be documented.

Application back out, restart and shutdown procedures with emergency contact information must be provided by the Applications Development team and made available to District ITS operations personnel.

Refer to Physical Security ITS-AR-1510 for data center access and other physical security controls.

2.2 Malware Management

All applicable systems must be configured with District ITS-approved anti-Malware software. The software must be configured to scan for malware in real-time. Anti-malware programs must be capable of detecting, removing, and protecting against all known types of malicious software.

All systems with anti-malware software must be configured to update malware signatures on a daily basis.

End users must not be able to configure or disable the software.

All anti-malware mechanisms must generate audit logs to aid District ITS in detecting and responding to malware outbreaks.

All YCCD employees may obtain approved anti-malware software to install on YCCD assets from District ITS.

2.3 Patches and Updates

YCCD must ensure that all system components and software are protected from known vulnerabilities by installing the latest vendor-supplied firmware, security patches, hot fixes and service packs found to be applicable to YCCD computing resources.

District ITS system administrators must keep up with vendor changes and enhancements. New or modified non-urgent patches must be scheduled and installed within one month of release. Urgent patches that address security

vulnerabilities must be installed as soon as is feasible without introducing instability or impacting service availability.

Where feasible, patches must be tested in a test environment prior to production deployment. Testing must ensure that systems function correctly.

Changes to servers and networks should be tested prior to implementation and follow normal change control management procedures.

District ITS must be alert to identifying new security vulnerabilities by monitoring available vendor or industry security sources. Hardening and configuration standards must be updated as soon as practical after new vulnerabilities are found.

2.4 Software and Asset Management

The Computer Use policy BP/AP 3720 sets forth usage policies for critical technologies that include e-mail usage and Internet usage and define proper use of these technologies. District ITS may also issue mobile devices (such as laptops or removable storage devices), and will maintain a list of issued devices and personnel with access to assist in determining owner, contact information and purpose.

District ITS will maintain a list of company-approved products and software.

2.5 Backups and Media

Users must store all critical files on the local area network so that they can be properly backed up. If an end-user chooses to store essential data elsewhere, it must be approved by District ITS management the user is responsible for ensuring the data can be recovered.

Any media containing backup data that is stored onsite must be classified so that operations personnel can determine the sensitivity of the data stored on tape or other formats.

Any backup media that must be transferred that contains *Restricted* information must be sent by secured courier or other delivery method that can be accurately tracked. Management must approve any and all media that is moved from a secured area (especially when media is distributed to individuals).

Strict control must be maintained over the storage and accessibility of backup media. Inventory logs of all media must be maintained and reviewed at least annually.

Media must be destroyed when it is no longer needed for business or legal reasons. Data retention requirements must be documented.

2.6 Third Party Management

A third party user is a non-YCCD employee or entity that is authorized to access YCCD systems and networks. Examples of third party users include consultants, contractors, temporary employees, interns, vendors, business partners, service providers, and suppliers of products, services, or information.

A process for engaging service providers must include proper due diligence prior to beginning the engagement. A list of all third party providers must be maintained.

Network connections between the YCCD environment and third parties must follow agreed-upon security procedures and/or confidentiality requirements. Such connections and other third-party access to YCCD's systems must be governed by formal written agreements or contracts.

These agreements may require signed Confidentiality and Non-Disclosure statements restricting the subsequent usage and dissemination of YCCD information.

Vendors or other third parties with access to YCCD-owned or leased equipment or systems housed in YCCD data center are restricted to only the specific equipment and systems they are authorized to maintain or monitor.

2.7 PCI Third Party Requirements

YCCD maintains a program to monitor its PCI DSS service providers' compliance status at least annually.

Payment Card Industry Data Security Standard (PCI DSS) requires that shared hosting providers protect each entity's hosted environment and cardholder data. These providers must meet specific requirements as detailed in Appendix A of the PCI DSS.

A written agreement that includes an acknowledgement from any PCI service providers must be maintained to ensure that the third party accepts responsibility for the security of cardholder data the service providers possess.

All service providers providing PCI services must be monitored at least annually to ensure their continued compliance with PCI DSS.