# ADMINISTRATIVE REGULATION 37xx

**NAME OF CC DISTRICT** BUSINESS

## INFORMATION SECURITY-ACCEPTABLE USE

### 1. Purpose and Scope

The objective of this administrative regulation is to outline the acceptable use of electronic assets at **NAME OF CC DISTRICT**. Inappropriate use exposes **NAME OF CC DISTRICT** to risks including compromise of network systems and services, human resources or legal issues.

This is one of a series of information security Administrative Regulations maintained by the District Information Technology (IT) department designed to protect **NAME OF CC DISTRICT** information systems.

#### 1.1 Applicability of Assets

The scope of this Administrative Regulation includes all electronic assets that are owned or leased by **NAME OF CC DISTRICT**. Assets may include but are not limited to:

* Desktop and Laptop Computers
* Servers
* Network Infrastructure
* Mobile Computing Devices
* Electronic Media
* Non-electronic media (paper and other)

#### 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 **NAME OF CC 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 **NAME OF CC DISTRICT** business partners, vendors, suppliers, outsource service providers, and other third party entities with access to **NAME OF CC DISTRICT** networks and system resources.

#### 1.4 References and Related Documents

Please refer to the following Administrative Regulations for additional information and references including definitions:

* AR 37xx: Acceptable Use
* AR 37xx: Change Control
* AR 3726: Data Classification
* AR 37xx: Disaster Recovery
* AR 37xx: Information Security Program Overview
* AR 3729: Logging and Monitoring
* AR 37xx: Network Security
* AR 3728: Physical Security
* AR 3730: Remote Access
* AR 37xx: Secure Operations
* AR 37xx: Security Incident Response

### 2. Acceptable Use

#### 2.1 Acknowledgement of User Responsibilities

All users must review and acknowledge their understanding of **NAME OF CC DISTRICT** Acceptable Use Administrative Regulation and other job appropriate information security Administrative Regulations on an annual basis. Human Resources (HR) will provide the Administrative Regulation and acknowledgement links to new staff and contractors upon hire or contract establishment.

#### 2.2 Personal Use

Computers and computer accounts given to users are provided to assist district employees and volunteers in the performance of their jobs. All computer systems belong to **NAME OF CC DISTRICT** and are intended for business and instructional use. Users are expected to exercise good judgment regarding the reasonableness of personal use of **NAME OF CC DISTRICT** information systems and assets. Personal use should not conflict in any way with business objectives or interests, organizational values, or standards of business conduct. **NAME OF CC DISTRICT** reserves the right to limit or prohibit the use of any software not licensed or approved by District IT or Local College IT. If unlicensed software is found to reside on a **NAME OF CC DISTRICT** computer, it must be removed.

**NAME OF CC DISTRICT** considers all information transmitted through or stored in its business system, including e-mail, instant messaging (IM) or chat data, and voice mail messages, as **NAME OF CC DISTRICT** business information. All files and other business information stored on **NAME OF CC DISTRICT** systems, even if considered “personal” by an employee, are and remain the property of **NAME OF CC DISTRICT**. **NAME OF CC DISTRICT** may review or use such business information as it deems appropriate.

Where allowed by law, **NAME OF CC DISTRICT**’s District IT and Local College IT departments reserve the right to monitor activities that occur on its systems in order to troubleshoot system problems, disruptions or outages. For this reason, users should not have an expectation of privacy for anything they store, create, send, or receive on a District or college system. Suspected inappropriate use of systems by individuals may also be investigated in order to protect the organization.

#### 2.3 Confidentiality

**NAME OF CC DISTRICT** has implemented a Data Classification Administrative Regulation 3726 which categorizes different types of information and how it will be protected based on its value and sensitivity. Sensitive, personally identifiable, and customer information are classified as *Restricted*, and must be kept confidential at all times. This information is accessible only to those **NAME OF CC DISTRICT** staff who need such access in order to perform their jobs, or to others who have been expressly authorized by **NAME OF CC DISTRICT** for specific limited purposes. Unauthorized disclosure of information that has been classified as *Restricted* could cause great harm to **NAME OF CC DISTRICT**, and may be protected by law.

*Restricted information* must be protected from disclosure to third parties (non-employees) by default. Third parties may be given access to **NAME OF CC DISTRICT** information only when a demonstrable need-to-know exists. Such disclosure may be authorized by **NAME OF CC DISTRICT** management or by contract, such as with a temporary worker, consultant, or service provider. A non-disclosure agreement may be required as directed by the relationship and **NAME OF CC DISTRICT** legal requirements.

*Restricted* information may be stored in designated locations only andmust be securely deleted when it is no longer required. If stored online, on portable devices or on tape, *Restricted* information requires encryption so that it cannot be read by unauthorized persons. *Restricted* information that is on paper or other media must also be stored securely. Refer to the Data Classification Handling Procedures for additional information on this topic.

Specific information about **NAME OF CC DISTRICT**’s computer network, information system security, security controls, or potential vulnerabilities may not be distributed to persons who do not have a demonstrable need-to-know, and without prior approval from the District Manager of Telecommunications and Security or Local College IT management.

All information systems assets provided by **NAME OF CC DISTRICT** remain the sole property of **NAME OF CC DISTRICT**. Any data or intellectual property created by the user, including voicemail and electronic messages, remain the property of **NAME OF CC DISTRICT** and should not be removed, copied or shared with any person or entity except as part of the user’s normal job responsibilities.

#### 2.4 Electronic Messaging

**NAME OF CC DISTRICT** has an electronic mail (e-mail) network and provides instant messaging (IM) services. Users are responsible for using these technologies responsibly and within the following policies:

* **NAME OF CC DISTRICT**'s e-mail system is not to be used to solicit for commercial ventures, religious or political causes, outside organizations or other non-job-related solicitations.
* Sending unsolicited e-mail messages is prohibited, including the sending of junk mail or other advertising material to individuals who did not specifically request such material.
* Creating or forwarding chain letters or pyramid schemes of any type is prohibited.

* Users must not create any messages that may be considered offensive or disruptive. Examples of messages deemed to be offensive are any which contain sexual implications, racial slurs, gender-specific comments or any other comment that offensively addresses someone's age, sexual orientation, religious or political beliefs, national origin or disability.
* **NAME OF CC DISTRICT** business communications transmitted by e-mail must use the appropriate District or college e-mail address (userid@**NAME OF CC DISTRICT**.edu, userid@ivc.edu, userid@saddleback.edu, or userid@atep.us) and employ the standard e-mail signature for external communications. Falsifying e-mail headers or routing information so as to obscure the origins of the e-mail or identity of the sender is a violation of this Administrative Regulation.
* Because e-mail records and computer files may be subject to discovery in litigation, users must avoid making statements in e-mail that would not reflect favorably on **NAME OF CC DISTRICT** if disclosed in litigation or otherwise. Delete unnecessary e-mail promptly.
* Unauthorized access to others’ e-mail accounts is prohibited.
* Information classified as *Restricted* (sensitive, personally identifiable, or student information) must not be e-mailed over public networks or stored on portable devices without encryption. Refer to the Data Classification Administrative Regulation 3726 for additional information.
* Caution must be used when opening e-mail attachments or following hypertext links received from unknown senders, which may contain malware or viral code.

#### 2.5 Social Networking Technologies

Social networking tools (blogs, online social networks, Facebook, Twitter, etc.) provide an open exchange of information and a means to establish relationships with colleagues and members of the public. These tools represent a communication model where a fine line exists between business and personal statements. Employees who choose to participate in social networking technologies must know and follow **NAME OF CC DISTRICT**’s Employee Handbook and review the Social Networking Guidelines.

**NAME OF CC DISTRICT**’s or another person or company's confidential or proprietary information is not to be shared. Users must ask permission to publish or report on conversations that may have intended to be private or internal to **NAME OF CC DISTRICT**. Check with the appropriate PIO or the Legal department if you have any questions about what is appropriate to publish or say online.

#### 2.6 Use of NAME OF CC DISTRICT Assets

Using **NAME OF CC DISTRICT** electronic assets for abusive, unethical, or inappropriate purposes will not be tolerated and may be considered grounds for disciplinary action, including termination of employment. Unacceptable use of electronic assets includes, but is not limited to:

* Illegal activities
* Revealing or publicizing **NAME OF CC DISTRICT** intellectual property or proprietary information for unapproved or non-business-related reasons
* Use or distribution of unlicensed software
* Unauthorized use of copyrighted materials
* Sharing of user names and/or passwords
* Leaving *Restricted* or any confidential or sensitive materials in plain sight without taking protective measures
* Transferring or storing information on untrusted third party servers. Contact IT for approved locations / services.
* Presenting your own viewpoints or positions as those of **NAME OF CC DISTRICT**, or attributing them to **NAME OF CC DISTRICT**
* Effecting security breaches or disruptions of network communications
* Circumventing user authentication or security of any computer, network or account
* Facilitation of the compromise of **NAME OF CC DISTRICT** information security controls
* Disabling software designed to prevent viruses or malware, or disabling screen savers or encryption methods
* Providing information about, or lists or organizational charts of **NAME OF CC DISTRICT** employees to external parties.

### 3.0 Enforcement

Those detecting violations of this Administrative Regulation must report the violation to their direct manager immediately, who will verify the nature of the violation and report it to District IT or Local College IT and/or Human Resources as appropriate. **NAME OF CC DISTRICT** Management will determine the extent of risk that any non-compliance condition presents and remediation activities that are required.

Users who deliberately violate information security Administrative Regulations will be subject to disciplinary action up to and including termination from employment or association with **NAME OF CC DISTRICT**.