CITRUS COMMUNITY COLLEGE DISTRICT
GENERAL INSTITUTION

AP 3724 DATA AND INFORMATION PROTECTION

Purpose

Data and information are some of Citrus Community College District's most valuable resources and require responsible management by all members of the District community. This procedure establishes specific guidelines for the proper protection of these valuable resources and promotes District's maintenance of strict confidentiality in compliance with applicable policies as well as local, state and federal regulations. These policies include but are not limited to Gramm-Leach-Blieliy Act (GLBA), Family Educational Rights and Privacy Act (FERPA) and the US Department of Education regulations. The procedure is also in support of the Citrus College Student Employment FERPA Non-Disclosure/Confidentiality Agreement.

Scope

This procedure addresses the handling of District data, whether communicated orally, in hard copy or electronic format, for all members of the District community, including but not limited to faculty, staff, students, alumni, the Board of Trustees, visitors or external individuals and organizations. This procedure applies to all District information whether stored on centrally maintained servers or storage area networks, employee or staff desktop computer, mobile and cellular devices or moved to media such as CD, tape, flash memory, or paper.

Users shall store only information required for the performance of official District responsibilities on District resources. Many employees, including student employees, generate or are exposed to sensitive District information in the course of their jobs and use it to perform important functions. It is vitally important that all individuals handle District sensitive information properly to protect the individuals whose sensitive information is being processed, as well as those who handle this information. Such information may contain proprietary content, research findings or other intellectual property that cannot be disclosed beyond those who need it. If such information is disclosed to unauthorized parties, the District could be harmed financially, by reputation or both.

Circumventing or attempting to circumvent restrictions on the use and dissemination of District data or information can be considered a serious offense and may result in disciplinary or legal action.

This procedure allows for the release or exchange of District information in accordance with the recommended best practices outlined below. District employees must not divulge confidential information regarding the District to an outside party except for a legitimate business, research, or academic purpose and with appropriate approvals. If such information has not been made public by the District, it should be treated as sensitive.

Procedures

Data Classification

The District will classify its information in three categories: restricted, sensitive or public. These data classes are described in the following table:

	Data Classification		
	Restricted	**Sensitive**	**Public**
Legal Requirement	Protection of data is required by law (e.g. FERPA, HIPPA, GLBA) and data is subject to external audit	The District has a contractual obligation to protect data	Protection of data is at the discretion of the data owner or custodian
Access	Only those individuals designated with approved access and signed agreements	District employees who have a business need to use the data	District employees, students and affiliates and the general public with a need to know
Examples	- Individual student data - Faculty/staff personnel data - Medical information - Credit card information - Management information	- Research results that are not restricted - Financial transactions that do not include restricted data - Information covered by non-disclosure agreements	- Campus maps - Contact information - College Fact Book - Board of Trustee Reports
Institutional Risk	High - Information that provides access to vital resources	Medium - Information that provides access to a restricted set of resources	Low - General District information that can be shared without damage to the District

Recommended Best Practices

Handling Information

Faculty, staff and students should exercise care and judgment to ensure adequate protection of District restricted or sensitive information. It is therefore recommended that they:

- Adopt "clean desk practices." Don't leave unattended paper documents containing restricted or sensitive information; protect them from the view of passers-by or office visitors. It is recommended that confidential documents contain a cover sheet. Close office doors when away from your office.
- Add a "Confidential" watermark to a Word document.
- Store paper documents containing restricted or sensitive information in locked files with a controlled key system (a list of individuals who have access should be documented) or an appropriately secured area.
- Lock file cabinets containing restricted or sensitive information before leaving the office each day.
- Do not leave the keys to file drawers containing restricted or sensitive information in unlocked desk drawers or other areas accessible to unauthorized staff.
- Store paper documents that contain restricted or sensitive information in secure file cabinets. Keep copies in an alternate location.
- Shred paper documents containing restricted and sensitive information when they are no longer needed, making sure that such documents are secured until shredding occurs. If a shredding service is employed, the service provider should have clearly defined procedures in the contractual agreement that protect discarded information, and ensure that the provider is legally accountable for those procedures, with penalties in place for breach of contract.
- Immediately retrieve or secure documents containing sensitive information as they are printed on copy machines, fax machines or printers. Double-check fax messages containing confidential information. Recheck the recipient's number before you hit 'Start.' Verify the security arrangements for a fax's receipt prior to sending. Verify that you are the intended recipient of faxes received on your machine. If you are not, contact the intended recipient and make arrangements for the proper dispatch of the fax.
- Do not discuss sensitive information outside of the workplace or with anyone who does not have a specific "need to know." Be aware of the potential for others to overhear communications containing restricted or sensitive information in offices, on telephones, and in public places like elevators, restaurants, and sidewalks.
- Ensure that electronic equipment containing sensitive information is securely transferred or disposed of in a secure manner, per the District's Electronic Equipment Disposition Policy.
- Immediately report the theft of District electronic computing equipment to a supervisor or manager. Loss or suspected compromise of data containing sensitive information should be immediately reported to the TeCS Department.

Data Stewardship Responsibilities

The District has four roles for proper data stewardship: data owner, manager of policies and procedures for access to that data, manager of the infrastructure

and account access, and data user. All information should have an identified owner. Anyone who has been entrusted with restricted or sensitive information has a responsibility to the data's owner for its proper use and protection.

Non-Disclosure and Non-Use

Sharing District information directly with other colleges and universities may violate anti-trust laws. Particular care should be shown in disclosure of financial aid data, faculty salaries, and fees that are not yet final. Violations of antitrust laws may have serious consequences for the District and individuals. Certain general information may be shared in surveys conducted by other colleges and universities.

Individuals should not disclose any District information that they obtain as a result of their employment at the District to unauthorized persons, nor should they use it for their own personal benefit, or for the profit of others. This obligation continues after an individual's association with the District ends.

Individuals may be asked for information about the District by the media, outside groups, consultants and others collecting information for various purposes. No one should make public statements on behalf of the District in response to external inquiries unless he/she has been authorized to do so. Refer all employment verification and reference requests to the Human Resources Department. When legal requests are made concerning wages, wage garnishments, and employee records Payroll and/or Human Resources should also be notified so they may coordinate the release.

Proper Disclosure and Release of Information

Confidential information concerning individual students or employees may be released only if the release of such information has been properly authorized. Some individuals must disclose District information as a part of their job responsibilities. Individuals should be certain that they understand what they have been authorized to disclose and to whom, prior to disclosing any Citrus Community College District sensitive information.

Examples of situations in which such information might properly be disclosed are:

- Disclosure of operational data to vendors or consultants in connection with their formal engagement to provide services to the District. A Non-Disclosure Agreement must also be signed by vendors who have access to sensitive information. Vendors must also comply with all applicable federal, state, and local laws/regulations in the production of goods or performance of services.
- Participation in legitimate and authorized surveys.
- Providing data to government agencies as part of required filings.
- An authorized individual responding to media or financial analyst inquiries.

Computing Requirements

Data Storage and Transmission

Strict control must also be maintained over District information that is stored on personal computers, external media (such as CDs, tapes, or memory sticks) or centrally on servers, as well as transmitted across District's network. The following guidelines should be applied for the storage and transmission of District data:

- Storage
  - Whenever possible, District data should be stored on a centrally managed server and not on a workstation or locally managed server.
  - A local machine storing District data must be in a physically secure location and require a unique logon with a strong password for each individual authorized to use it (i.e. shared accounts and passwords are not permitted).
  - Whether District data is housed on a server or workstation, the machine must meet current operation system, hardware and software support levels.
- Transmission
  - Restricted and sensitive data should never be transmitted over the Internet "in the clear." It should always be transmitted using an encryption mechanism (as listed in section 3.5.2 below).
  - Restricted and sensitive data should not be transmitted via email.
- Backups
  - It is the responsibility of all employees entrusted with District data to back it up and store in a secure location.
  - Backup of District information should be encrypted, whenever technically feasible.
  - Unencrypted backups should be physically secured and not subject to unauthorized personnel at any time.
- Access
  - Access controls to all restricted and sensitive information must be documented.

Encryption and Certification

The transmission of District restricted or sensitive data over the network should be protected by an approved encryption mechanism to ensure its proper protection. Any method of encryption or transmission system other than those listed below should be reviewed and approved by the TeCS Department before being utilized.

- Transport Encryption
  - Hypertext Transfer Protocol Secure (HTTPS)
  - Secure Shell (Secure Copy Protocol (scp)/ SSH File Transfer Protocol (sftp))
  - Secure Socket Layer (SSL)/Transport Layer Security (TLS)
  - File Transfer Protocol Secure (FTPS) (TLS wrapped FTP)
- File/Email Encryption

- Secure/Multipurpose Internet Mail Extensions (S/MIME) signed and encrypted email
- PGP (Pretty Good Privacy)/ GNU (Privacy Guard) GnuPG encrypted email and files
- Password-protected zipfiles
- Password-protected Microsoft Office documents

Access

The District shall maintain strict control over access to work locations, records, computer information and other items of value. Individuals who are assigned keys, given special access or assigned job responsibilities in connection with the safety, security or confidentiality of such records, materials or equipment value should use sound judgment and discretion in carrying out their duties and will be held accountable for any wrongdoing or acts of indiscretion. Furthermore, information may not be divulged, copied, released, sold, loaned, reviewed, altered or destroyed except as properly authorized within the scope of applicable federal, state or local laws.

Unauthorized access to any District restricted or sensitive information by students, faculty or staff will be cause for disciplinary and possible legal action. Unauthorized access in situations, which indicate that privacy, copyright, anti-trust, or other laws may have been broken, may be referred to legal authorities.

Anyone who may become familiar with another District's or person's confidential information should take care to respect the proprietary nature of this information and not use it or reveal it without authorization.

Board Approved 05/04/10
Board Revised 05/03/16