Sierra College
ADMINISTRATIVE PROCEDURE AP 3722

Electronic Information Security

Date Adopted: 11/2/2018

Date Revised: 12/12/2025

Date Reviewed: 12/12/2025

References: Health Insurance Portability and Accountability Act of 1996 (HIPAA) – 45 CFR Parts 160 and 164. Family Educational Rights and Privacy Act of 1974 (FERPA) - 20 U.S. Code Section 1232g. Breach Notification Law: California Civil Code - 1798.29 (previously SB1386). Security of Personal Information: California Civil Code - 1798.85 (previously SB 25). The Higher Education Opportunity Act (Public Law 110-315).

Suspected security breaches in a District-owned computing system or an emergency situation that may have disastrous consequences to District assets, should be reported to the:

Service Desk at (916) 660-7777 during work hours (published on the District Information Technology Services (ITS) webpage) or the District's Department of Community Safety at (916) 660-7120 after work hours or on holidays.

PURPOSE
The purpose of this procedure is to enhance the security of stored, transmitted, and distributed personal information that could be used to impersonate an individual and cause serious loss of privacy and/or financial damage. This procedure applies to all records, papers, files and communications maintained or possessed by the District.

In addition to this procedure, divisions/departments are urged to establish best practices and procedures that reduce the collection, distribution, and retention of personal data, old files, and other materials, which are not necessary to perform the educational and business needs of the institution.

Legal requirements and local policy, including Administrative Procedure and Board Policy 5040, Student Records, Directory Information and Privacy, require that District personnel take appropriate measures to protect personal information from inadvertent or illegal exposure to unauthorized individuals. Other legal requirements require that if certain personal information is

inadvertently disclosed, the District must notify all individuals whose information was compromised.

DEFINITIONS
Personal Information: Personally Identifiable Information (PII) includes:

Personally Identifiable Information as defined by federal law, refers to specific information about an individual used to trace that individual's identity. Information such as their name, Social Security Number (SSN), date and place of birth, address, mother's maiden name, or biometric records (i.e. fingerprints, DNA sequence, facial characteristics, handwriting, etc.), alone, or when combined with other personal or identifying information is linkable or linked to a specific individual's medical, educational, financial, and employment information.

Stand-alone PII items are:

- Social Security Number
- Driver's License or State ID Number
- Passport Number
- Alien Registration Number
- Financial Account Number

All other personally identifiable information when combined together (two or more) is considered a PII breach. Note: An email address or phone number (non-PII information) when combined with a name is not considered a PII breach.

For students, all personally identifiable information not included as *directory information (see Administrative Procedure and Board Policy 5040)*. This would include the student's name in conjunction with:

- The name of the student's parent(s) or other family members
- The address of the student's family
- A personal identifier, such as a social security number or student identification number
- The race or ethnicity of the student
- The gender of the student
- A list of personal characteristics of the student
- Academic evaluations and grades of the student
- Transcripts and/or other academic records of the student
- Assessment scores
- The student's class schedule

Security Breach: An incident when an individual's unencrypted personal information has been (or is reasonably believed to have been) exposed to or acquired by an unauthorized person.

Good faith acquisition of personal information by an employee or agent for District purposes does not constitute a security breach, provided that the personal information is not further disclosed to unauthorized persons. The theft of a computing system that contains or may contain

personal information will be considered a potential security breach. Inadvertent access to personal information that occurs in the course of performing technical services on a computing system by an authorized technical staff member will not be considered a security breach.

Computing System: Any server, desktop, laptop computer, tablet or other device that contains (or provides network access to) data files.

Computer-Based Information System: Any computing system or device that is used in the acquisition, storage, manipulation, management, movement, control, display, transmission, or reception of data (including software, firmware, and hardware).

Chief Technology Officer (CTO): An administrator who holds responsibility for oversight of data security at the District. The responsibility may be delegated as needed.

Data Resource: Data (information) that is stored on a computer-based information system.

Data Resource Manager or Steward: An individual who controls the use of and access to a data resource within a functional area.

Lead Authority: An administrator who has been delegated responsibility for oversight of data security within the functional business unit they manage for the District.

Control Records: The records contained in a database, spreadsheet, or other electronic file that document system and application level access methods into those computer-based information systems containing personal information. Control records must contain the following for each computer-based information system:

- Name of the computer-based information system
- Physical location of computer-based information system
- Name of the Chief Technology Officer (or designee)
- Name of the data resource manager(s) or Steward who have responsibility for any data containing personal information on the computer-based information system
- Description of logical access methods and security controls (user IDs, passwords, encryption keys, etc.) necessary to gain access to the computer based information systems and its data or, the name of another employee (in addition to the Chief Technology Officer) who has knowledge of logical access methods and security controls (e.g. who can gain access to the system and applications as a systems administrator)

ITS Security Incident Response Team: A team of designated Information Technology Services (ITS) members who initially investigate and respond to security incidents.

RESPONSIBILITIES

1. **The lead authority (or designee) has oversight responsibilities to:**
    - Ensure that data resource managers/stewards are designated and perform their functions as specified in this document.
    - Know where to rapidly locate contact information (email and postal addresses) for individuals of whom personal information is retained or transmitted. (Contact

information on all students and employees is kept in the District's administrative information system.)
- Ensure that the incident response process delineated in these procedures is followed (if a security breach occurs on a computer-based information system or a data resource managed by an individual in this organization).
- Rapidly notify affected individuals whose personal information may have been compromised as the result of a security breach of a computing system or actions of an employee under the jurisdiction of the lead authority as required by this procedure. Current law (as of April 2008) requires that notification be made in the most expedient time possible and without unreasonable delay. (Refer to California Civil Code 1798.29). All breach notifications must first be approved by the District's Risk Manager in the Business Services Office and follow the established ITS Security Incident Response Process below.

2. **The Chief Technology Officer (or designee) has responsibilities to:**
   - Develop security measures, including District published best practices and standards to reduce vulnerabilities of personal information contained in computer-based information systems within their jurisdiction including the use of appropriate encryption strategies for both transmission and storage of personal information.
   - Chair the District Cybersecurity Advisory Group to provide recommendations and procedures, implement them, and update best practices.
   - Create, retain and secure control records for computer-based information systems that contain personal information.
   - Annually update control records as necessary including those kept in the central repository.
   - Implement procedures and tools to monitor access to computer-based information systems that contain personal information and to indicate if unauthorized access occurs.
   - Remove files containing personal information (using an industry standard secure data removal tool) from servers, which are identified to be salvaged or repurposed.
   - Implement procedures, tools, schedules, and best practices that provide data retention for key systems in the data center as specified in the Backup and Data Retention procedures outlined in Administrative Procedure 3721.
   - Know where to rapidly locate contact information (email and postal addresses) for individuals of whom personal information is retained or transmitted. (Contact information on all students and employees is kept in the District's administrative information system.)
   - Ensure that the incident response process delineated in these procedures is followed (if a security breach occurs on a computer-based information system or a data resource managed by an individual in this organization).
   - Rapidly notify affected individuals whose personal information may have been compromised as the result of a security breach of a computing system or actions of an employee under the jurisdiction of the lead authority as required by this procedure. Current law (as of April 2008) requires that notification be made in the most expedient time possible and without unreasonable delay. (Refer to California Civil Code 1798.29).

3. **The data resource manager or steward has responsibilities to:**
    - Identify computer-based information systems within their division/department that contain personal information or that provide to access to personal information.
    - Grant, monitor, and remove access to a data resource or data to individuals/positions based on the documented business need.
    - Inform individuals who have access to the data resource (and any downstream users of distributed data) of their responsibilities to secure and protect personal information as well as to destroy it when no longer needed. Includes applicable:
        - District policies and procedures
        - Best practices
    - Maintain the control records on computer-based information systems that contain personal information within their purview.
    - Additional Data Steward Roles and Responsibilities are shown below in the Data Classification Procedures section.

4. **All employees have responsibilities to:**
    - Abide by the established procedures with regard to accessing, protecting, using, and securing personal information under their control using procedures, guidelines, and best practices provided by the District.
    - Safeguard District data and destroy data containing personal information when no longer needed.
    - Ensure only District owned and approved devices are connected and/or accessing the District's internal network unless approved by the CTO or designee for security.
    - Ensure only District owned and approved software is loaded on District owned systems unless approved by the CTO or designee for security.
    - See also: Board Policy 3720 and Administrative Procedure 3720 - Computer and Network Use: Rights and Responsibilities

5. **Other responsibilities:**
    - The District's Department of Community Safety will act as the point of contact between the District and external law enforcement agencies when external law enforcement agencies are involved.
    - ITS shall remove personal information (using a standard Department of Defense data removal procedure commonly known as "DOD Wipe") from desktop/laptop computers, which are designated to be salvaged or repurposed.
    - System hard drives may be destroyed as an alternate method of removing sensitive information.

SECURITY INCIDENT RESPONSE PROCESS

The incident response process consists of the following steps that must be implemented in the event that a security breach occurs:

1. **Notify Key Persons**
   If a person reasonably believes that a security breach has occurred on a computing system that contains or has network access to unencrypted personal information, the person

identifying the incident must immediately contact the ITS Helpdesk (during work hours) or the District's Department of Community Safety (after work hours). If the security breach is reported after work hours have ended, then the District's Department of Community Safety office will notify the Chief Technology Officer (or designee). The Chief Technology Officer or designee will notify the appropriate Lead Authority and the Chief Technology Officer.

2. **Isolate the System**
   For Computer Based Information Systems: The Chief Technology Officer or designee will disconnect the computing system from the campus network without modifying any settings, files, etc. on the computing system, and leave the system powered up.

   For employee assigned desktop or laptop computers: If the computer is turned on, the employee or ITS Service Desk representative should immediately disconnect the computer from the network (by removing the network cable or disconnecting from a wireless connection). The computer should not be turned on or off or otherwise modified in any way.

   For Stolen Computing Systems: If a District-owned computing system or a computing system containing sensitive District data is stolen, the employee shall notify the District's Department of Community Safety, the Chief Technology Officer (or designee), and their Supervisor of the theft and detail what data was contained on the system.

   If a stolen computing system is recovered, the person gaining possession of the system will first notify the District's Department of Community Safety and then immediately notify the ITS Service Desk, which will arrange for the system to be picked up. The computing system should not be turned on or otherwise modified in any way.

3. **Analyze the Breach**
   The ITS Security Incident Response Team, in cooperation with the District's Department of Community Safety (if involved) and the Chief Technology Officer (or designee), will look for evidence of a security breach to assess the possibility that personal information has been compromised.

4. **Report the Incident**
   If the ITS Security Incident Response Team, in cooperation with the District's Department of Community Safety (if involved) and the Chief Technology Officer (or designee), has sufficient reason to believe that personal information may have been acquired by or exposed to unauthorized individuals, the ITS Security Incident Response Team will submit written notification describing the nature of the security breach and estimated number of affected individuals to the:
   - Superintendent/President (if applicable)
   - Chief Technology Officer
   - Lead authority
   - District Risk Manager and cybersecurity insurance provider if applicable
   - District public information officer
   - District Department of Community Safety or appropriate law enforcement agency

If further expertise is needed the District may request a professional computer forensics team be contacted.

5. **Restore and Reconnect the System**
   ITS may repair and restore system functionality to the computing system when:
   - The computing system is no longer needed for forensic analysis or police investigation and
   - It has been cleaned of all known malware.

   The ITS Security Incident Response Team will work with the Chief Technology Officer (or designee) and the District's Department of Community Safety (if involved) to determine when the computing system can be reconnected to the campus network.

   - Special consideration for rapid restoration and reconnection will be given to computing systems that provide time sensitive functionality to support critical campus services.

6. **Notify Individuals whose Personal Information has been Compromised**
   a. **Decide if Notification is Required and How Notification will be Made**
   The District representatives (as appropriate), the Chief Technology Officer (or designee), the lead authority and the District's attorney or cybersecurity insurance legal advisors (District's legal advisors) will confer to determine whether or not the criteria for notification under California Civil Code 1798.29 and 1798.82 has been met and to determine which means of notification to use (e. g., email, postal mail, or website notice).

   b. **Personal Information Not Involved**
   If information beyond the data elements defined herein as personal information is accessed by an unauthorized person, the appropriate district/college communications coordinator in coordination with the District's legal advisors will determine what notification will be made to affected individuals, if any.

   c. **Required Information**
   If notification is required, the appropriate District communication coordinator shall notify affected individuals of the security breach and include the following information:
   - The date(s) on which the personal information was (or could have been) acquired.
   - A description of the personal information, which was (or could have been) acquired.
   - The name of the department or unit responsible for the information and the relationship that the affected individual has (had) to the department (in such a way that the person receiving the notification will understand why that department or unit had their information).
   - An indication of the likelihood that the personal information was acquired or used.
   - An email address and phone number of a suitable college representative with sufficient knowledge of the incident to be able to handle questions from affected individuals.
   - A list of resources that affected individuals can use to check for potential misuse of their information.

The appropriate District communications coordinator will also determine what additional advice or assistance will be given to the affected individuals.

d. **Timeliness of Notification**
Notification must occur without unreasonable delay, except when a law enforcement agency has determined that notification will impede a criminal investigation. (In this case, notification must occur as soon as the law enforcement agency determines that it will not compromise the investigation.)

e. **Substitute Method of Notification**
If sufficient contact information is not available for direct hard copy or e-mail notice for some affected individuals, a substitute method of notice may be used. The substitute notice should include a prominent display on the campus website or other commonly used public communications medium for at least 45 days.

f. **Submit the After Notification Report**
The District Chief Technology Officer will provide a written report describing the number of individuals successfully notified, the number of individuals for unsuccessful notifications, and which methods were used for notification, along with any issues that have arisen as a result of the breach such as press coverage, complaints from affected individuals, etc. The report will be sent to the following individuals:
- Superintendent/President
- Chief Technology Officer
- Lead authority
- District public information officer

DATA CLASSIFICATION PROCEDURES
Users of Sierra Community College District systems need to understand the importance of securely handling the information they are able to access and the standards that have been created to ensure data protection. For the purposes of this Administrative Procedure, data includes both electronic and paper.

Specific protection requirements are mandated for certain types of data, such as credit card information, personally identifiable information, student grades, or financial data. Where information is entrusted to us by our students, employees, or business partners, their expectations for secure handling must be met. Consistent use of this Data Classification AP will help to ensure that we maintain adequate data protection.

1. **Classification of Data Assets**
Sierra Community College District classifies information regardless of medium (electronic or paper) according to its sensitivity and the potential impact of disclosure.

In general, information is disclosed to employees or others when there is a business need-to-know. Information must be consistently handled according to its requirements for confidentiality and disclosure.

The role of the Data Stewards, as defined below, are responsible for determining the appropriate classification level for data for which they are responsible or for the same information maintained on paper documents.

If the classification level is set too high, the cost of protection will be excessive in relation to the value or sensitivity of the data. If it is set too low, the risk of compromise could be increased.

Downgrading to a lower classification at a future date is appropriate should conditions warrant.

a. **Data Stewardship Roles and Responsibilities for Data Classification and Security**
Every business application or file on a Department District File Server must have one or more designated Data Stewards. The Data Steward is the person responsible for (or dependent upon) the business process associated with an information asset. The Data Steward is knowledgeable about how the information is acquired, transmitted, stored, deleted, or otherwise processed, and is therefore best suited to make decisions about the information on behalf of the organization.

The Data Steward is ultimately responsible for security decisions regarding the data. The Data Steward will work with the appropriate campus or District ITS department personnel to ensure that minimum security standards are met. The District and College ITS departments will provide appropriate security technology solutions (such as system or application security controls or encryption methods) based on classification level.

If the Data Steward has chosen to outsource processing or storage of information at a location outside of Sierra Community College District's control, such as on a cloud-based service, the Data Steward retains full accountability for security of the information. Security controls that are required to be performed by the third party service provider must be detailed in the contract with that provider, and monitored by the Data Steward. All contracts to outsource processing or storage of District Information must be approved by the District's Chief Technology Officer (CTO) in additional all standard contract approval procedures.

The Data Steward's responsibilities include:

- Classifying data for which they are responsible. This includes determining the level of confidentiality that should be assigned to information, which will dictate its level of protection.
- Working with ITS to select security controls that are appropriate to the level of sensitivity, value or confidentiality of the application or data it processes.
- Working with ITS to ensure that third parties to whom data has been entrusted meet Sierra Community College District security requirements.
- Establishing and maintaining response plans which identify actions to be taken for their area of control, such as Security Incident Response processes and defined Business Continuity Plans.
- Provide District ITS management with administrative access in order to

maintain continuity of access to systems and services.

b. **Data Classification Categories**

Information that is owned, used, created or maintained by Sierra Community College District must be classified into one of three categories:

- Public
- Internal
- Restricted

i. **Public**

Data classified as Public is suitable for routine public disclosure and use. Security at this level is the minimum required by Sierra Community College District to protect the integrity and availability of this data. Examples of this type of data include, but are not limited to, data routinely distributed to the public such as publicly accessible web pages, marketing materials, and press statements.

ii. **Internal**

Internal data is information about Sierra Community College District or internal processes that must be guarded due to proprietary or business considerations, but which is not personally identifiable or otherwise considered confidential. This classification may apply even if there are no regulatory or contractual requirements for its protection.

Data in this category is generally available to employees, contractors, students, or business associates, but is not routinely distributed outside Sierra Community College District. Some Internal data may be limited to individuals who have a legitimate business purpose for accessing the data, and not be available to everyone. Examples of Internal data may include:

- Sierra Community College District procedures and manuals
- Organization charts
- Data which is on the internal Intranet (SharePoint), but has not been approved for external communication
- Software application lists or project reports
- Building or facility floor plans or equipment locations

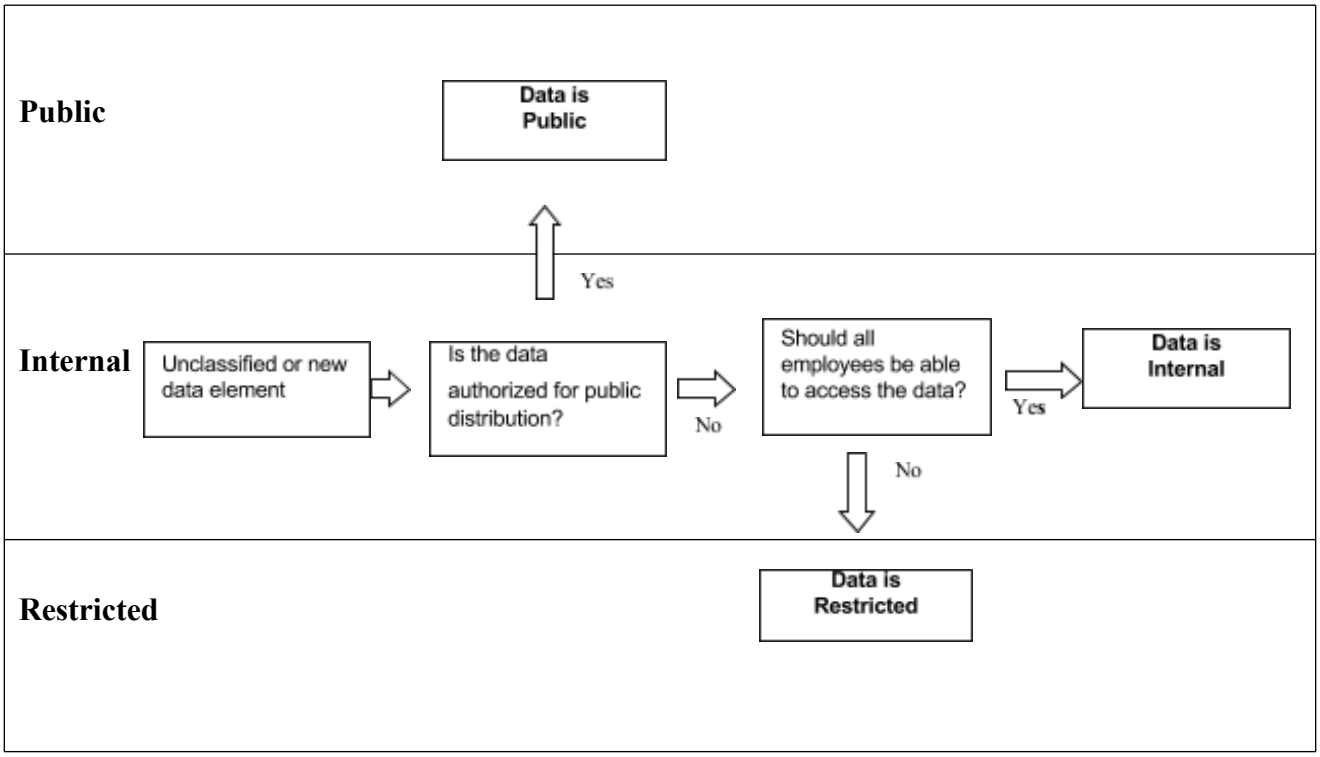
iii. **Restricted**

Restricted data is information that is sensitive in nature, and may be proprietary, personally identifiable, or otherwise sensitive. Unauthorized compromise or disclosure of the information would be likely to cause serious financial, legal, or reputation damage to Sierra Joint Community College District, as well as its employees or students. Restricted data may be protected by statutes, regulations, or contractual requirements. All HIPAA, FERPA and Personal Information is restricted. Disclosure is limited to those within Sierra Joint Community College District on a “need-to-know” basis only. Disclosure

to parties outside of Sierra Joint Community College District must be authorized by law and by appropriate data steward and covered by a binding confidentiality or non-disclosure agreement.

c. **Minimum Classification**
All information should be assumed Internal unless classified otherwise.

d. **Classification Flow Chart**
The Classification Flow Chart on the following page is intended to assist a Data Steward, document creator or user to assist in quickly determining the classification of a data element or document.



e. **Information Access**
The Data Steward makes access decisions regarding information they are responsible for, and must be consulted when access decisions are to be made, extended, or modified.

2. Periodic Review
Information asset classifications must be reviewed by the Data Steward at least every two years, or when necessary based on business need. Review records must be maintained by Data Stewards documenting the review processes took place, for audit purposes.

See Board Policy 3720.