Sierra College
ADMINISTRATIVE PROCEDURE AP 3721

Electronic Information Security and Data Backup Procedures

Date Adopted: 4/13/2012
Date Revised: 5/13/2016
Date Reviewed: 5/13/2016


If you suspect that a security breach has occurred in a district-owned computing system or that an emergency situation that may have disastrous consequences to District assets, contact the:

IIT Helpdesk at x7777 during work hours or District Security at (916) 660-7120 after work hours or on holidays

PURPOSE

The purpose of this procedure is to enhance the security and recoverability 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.

In addition to this procedure, 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 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/college must notify all individuals whose information was compromised.

DEFINITIONS

Sierra College Administrative Procedure 3721 Page 1 of 11
A. Personal Information: *Personal information* includes:

1. For all individuals, an individual's first and last name in combination with any of the following:
   - social security number
   - driver's license number
   - financial account or credit card number in combination with any password that would permit access to the individual's financial account
   - medical information

2. For students, all personally identifiable information not included as directory information. 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 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 other academic records of the student
   - scores on tests required for new students
   - the student's class schedule

3. For employees, an individual's first and last name in combination with the:
   - employee’s ID number

B. Directory Information (FERPA Definition): Information that is generally not considered harmful or an invasion of privacy if released. The primary purpose of directory information is to allow the district/college to include this type of information from a student’s education records in certain school publications. Examples include:

   - A playbill, showing the student's role in a drama production
   - The annual yearbook
   - Honor roll or other recognition lists
   - Graduation programs
   - Sports activity, such as for wrestling, showing weight and height of team members

C. 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 / college 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.

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

E. 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).

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

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

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

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

J. 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)

K. Information Security Incident Response Team: A team of designated Information and Instructional Technology (IIT) members who initially investigate and respond to security incidents.
L. System Backup: A duplicate copy of a server’s applications, data, and operating system files typically preserved both on-site and off-site to allow for system recovery in the event of system failures or disaster scenarios.

M. Data Archives: A copy of application data, user files, emails, and other information that is retained for the purpose of easy access and restoration of historical data.

N. Backup Data Retention: A define period of time that data is maintained in a backup procedure rotation. At the defined retention period the data becomes over-written and/or aged out of the rotation. Once data has exceeded defined retention periods it is unrecoverable from the backup system. Data retention requirements are determined by the Lead Authority as defined above.

RESPONSIBILITIES

A. 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
- assure data retention specifications meet regulatory requirements and are communicated to IIT management
- 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).

B. The Chief Technology Officer (or designee) has responsibilities to:

- develop security measures, including District published best practices 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 security 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 below.

• 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).

C. The data resource manager or steward has responsibilities to:

• identify computer-based information systems under their jurisdiction 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 on a “need to know” basis

• 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. Include applicable:
  • district and college policies and procedures
  • best practices

• Maintain the control records on computer-based information systems that contain personal information within their purview.

D. 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 districts 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: Computer and Network Use: Rights and Responsibilities Policy/Procedures 3720/AP 3720

E. Other responsibilities:

• Sierra District Security Services will act as the point of contact between the district and external law enforcement agencies when external law enforcement agencies are involved

• IIT 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

**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:

A. 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 IIT Helpdesk at 916-660-7777 (during work hours) or district security (after work hours). If during work hours, the IIT Helpdesk will immediately escalate the incident to the Chief Technology Officer (or designee). If the security breach is reported after work hours, district security 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.

B. Isolate the system

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 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. If help is needed with this please contact the Helpdesk.

For Stolen Computing Systems: If a District-owned computing system or a computing system containing sensitive District data is stolen, the employee shall notify District Security, 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 notify the Helpdesk, which will arrange for the system to be picked up. The computing system should not be turned on or otherwise modified in any way.

C. Analyze the breach

The Information Security Incident Response Team, in cooperation with District security (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, or that malicious computer code may be present on the system(s) involved in the breach.

D. Report the incident

If the Information Security Incident Response Team, in cooperation with District security (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 Information Security Incident Response Team will submit written notification describing the nature of the security breach and estimated number of affected individuals to the:

- President of the college (if applicable)
- Chief Technology Officer
- Lead authority
- District and college (as applicable) communication coordinators
- District Security or appropriate law enforcement agency

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

E. Restore and reconnect the System

IIT 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 Information Security Incident Response Team will work with the Chief Technology Officer (or designee) and District security (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.

F. Notify individuals whose personal information has been compromised

1. Decide if notification is required and how notification will be made

The district/college representatives (as appropriate), the Chief Technology Officer (or designee), the lead authority and the district’s attorney 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).

2. 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 attorney will determine what notification will be made to affected individuals, if any.

3. Required information
If notification is required, the appropriate district/college 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.

This list should include the following flyer (either as a link or a hardcopy attachment): “What to Do If Your Personal Information is Compromised” [http://www.privacy.ca.gov/financial/sbfs021205.pdf], produced by the California Office of Privacy Protection.

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

4. 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.)

5. 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 Web site or other commonly used Web site for at least forty-five days.

6. Submit the After Notification Report
The district/college communication coordinator 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:

- President of the college
- Chief Technology Officer
- Lead authority
- District communication coordinators

**BACKUP AND DATA RETENTION**

The District maintains backup copies of critical system data on alternate disk systems and tape media. Backup systems are design to recover from a complete server failure or catastrophic event and are not designed for file restoration and archiving.

It is also necessary for the District to have a formal Policy and Procedure addressing data retention to establish what may or may not be accessible as evidence through e-Discovery.

**Enterprise Resource System (ERP) and Student Information System (SIS):**

The District’s ERP/SIS is critical to the mission of the District and will adhere to following data backup and retention procedures:

1. The District’s Recovery Point Objective for the ERP/SIS system is with a Recovery Time Objective of hours per industry best practices.
2. All ERP production databases will be copied to a redundant and geographically separate database instance multiple times every day.
3. All ERP production databases will be backed up at least nightly in duplicate.
4. All ERP servers and operating systems will be backed up fully every week.
5. All duplicate backup jobs will be maintained in a separate and secure physical location from the primary backup media.
6. All database and server OS backups are for system recovery purposes and disaster recovery (DR), and not for recovery of individual files or version changes.
7. All backup media storing data is to be retained in accordance with legal and regulatory requirements as identified by data stewards with these recommendations factoring into the final process. Backup requirements will be based on industry best practices, resources, and as technology evolves.

**Electronic Mail (email) and other Production Data**

The District’s Email server message stores or email hosting partner servers, along with other production data will adhere to following data backup and retention procedures:
1. The District’s Recovery Point Objective for the ERP/SIS system is with a Recovery Time Objective of hours per industry best practices.
2. All Email and production databases will be copied to a redundant and geographically separate database instance at least every hour.
3. All Email and production databases will be backed up at least nightly in duplicate.
4. All Email and production application server data and operating systems will be backed up fully every week.
5. All duplicate backup jobs will be maintained in a separate and secure physical location from the primary backup media.
6. All database and server OS backups are for system recovery purposes and disaster recovery (DR), and not for recovery of individual files, messages, or deleted database data.
7. All backup media storing data is to be retained in accordance with legal and regulatory requirements as identified by data stewards with these recommendations factoring into the final process. Backup requirements will be based on industry best practices, resources, and as technology evolves.

REFERENCES

Information on privacy laws applicable to California http://www.privacy.ca.gov/

Potential Discipline: Violation of this policy may result in disciplinary action up to and including termination or expulsion.

See Board Policy 3720