

Electronic Information Security

AP 3260

If you suspect that a security breach has occurred in a district-owned computing system, contact the:	
Call Center at x8324 during work hours	District police at x7313 after work hours / 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.

In addition to this procedure, colleges and departments are urged to establish best practices that reduce the collection, distribution, and retention of personal data, which is 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. Refer to the table below for further details regarding legal, **local policy and contractual** requirements.

Legal and Local Requirements for Safeguarding Personal Information

Reference*	Applies to	Required by Applicable Law	Requires <u>protection</u> of Info?	Requires <u>notification</u> of breach?
M - 1.	All individuals	California Civil Code 1798.85, 1798.29	Yes	**
M - 2.	Students	Family Educational Rights and Privacy Act (FERPA)	Yes	No***
M - 3.	Employees	District procedure	Yes	No
M - 4.	All individuals	PCI-DSS Industry Standards	Yes	Yes

*refer to **Personal Information** definitions below

**Civil Code 1798.29 requires “state agencies, businesses and persons conducting business in California” to notify affected persons in event of a breach. This section of code may not apply to California Community Colleges.

*** FERPA does require the college to make a record of all improper disclosures. It is up to the college to decide if the situation warrants notification of the affected student(s).

DEFINITIONS

A. CHIEF INFORMATION SECURITY OFFICER (CISO):

The role of Chief Information Security Officer is assigned to the Vice Chancellor of Educational Technology Services (ETS).

B. CARD VERIFICATION CODE:

A 3 or 4 digit number printed on the front or the back of a payment card

C. COMPUTER-BASED INFORMATION SYSTEM:

Any computing system that is used in the acquisition, storage, manipulation, management, movement, control, display, transmission, or reception of data (including software, firmware, and hardware), which is used to provide services to persons other than the owner.

D. COMPUTER-BASED INFORMATION SYSTEM MANAGER (CBIS MANAGER):

An individual who maintains and manages an information system, server, or other technology device that stores or transmits data.

E. COMPUTING SYSTEM:

Any server, desktop or laptop computer, or PDA that contains (or provides network access to) data files

F. 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 *CBIS manager*
- name of the *data resource manager(s)* 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 CBIS manager) 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)

G. DATA RESOURCE:

Data (information) that is stored on a *computer-based information system*

H. DATA RESOURCE MANAGER:

An individual who controls the use of and access to a *data resource*

I. 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 sheets, such as for wrestling, showing weight and height of team members

J. ETS INCIDENT RESPONSE TEAM:

A team of designated ETS members who investigate and respond to security incidents

K. LEAD AUTHORITY:

An administrator who has been delegated responsibility for oversight of data security at a college or Central Services. Each president will designate a person to act as the lead authority for their college. The Vice Chancellor of Technology is the lead authority for Central Services.

L. PAYMENT CARD INDUSTRY – DATA SECURITY STANDARDS (PCI-DSS):

Industry developed data security standards that any organization of any size must adhere to in order to accept payment cards, and to store, process, and/or transmit cardholder data.

M. 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 students 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
4. For all individuals, any payment card information (PCI) including
- Primary Account Number (PAN) along with any of the following:
 - Cardholder name
 - Expiration date
 - Service code
 - PIN
 - PIN block used to authenticate cardholders and/or authorize payment card transactions.
 - Magnetic strip data or chip data
 - Card verification code
 - Card verification value

N. PRIMARY ACCOUNT NUMBER (PAN)

A primary account number is the 14 or 16 digit numeric code located on the face (front) of a credit or debit card; this code is also encrypted on the magnetic strip of the card or contained on a chip embedded in the card. This primary account number is used to identify an individual account holder.

O. 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*.

RESPONSIBILITIES

A. THE CHIEF INFORMATION SECURITY OFFICER HAS RESPONSIBILITIES TO ENSURE THE FOLLOWING FUNCTIONS ARE COMPLETED:

- create, update and distribute security policies and procedures
- monitor, analyze and distribute security alerts as appropriate
- create, update and distribute security incident response and escalation procedures
- appoint *Data Security Managers* for each key area of stored data within the Banner ERP system
- administer user account and authentication system controls for the Banner ERP system

B. THE LEAD AUTHORITY HAS OVERSIGHT RESPONSIBILITIES TO:

- identify *computer-based information systems* under their jurisdiction that contain *personal information* or that provide to access to *personal information*
- ensure that *data resource managers* and *CBIS managers* perform their functions as specified in this document
- create a secure central repository to contain *control records* on *computer-based information systems* that contain *personal information*
- 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 his / her organization [college or Central Services]).
- 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. MANAGERS WHOSE EMPLOYEES PROCESS CREDIT CARD INFORMATION HAVE RESPONSIBILITIES TO:

- ensure that employees comply with this procedure (AP3260) in its entirety for all card processing activities and related technologies
- give access to cardholder data only to those employees whose job requires them to have this access
- ensure that manual swipe transactions are to be conducted by authorized employees only
- conduct periodic assessments to ensure continued compliance to these policies and procedures, which may include review of records, systems and equipment.
- ensure records of these assessments are maintained as part of Foothill-De Anza Community College District's compliance records

D. THE CBIS MANAGER 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*
- 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

E. THE DATA RESOURCE MANAGER HAS RESPONSIBILITIES TO:

- grant 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

F. ALL EMPLOYEES HAVE RESPONSIBILITIES TO:

- abide by the established procedures with regard to accessing and using *personal information*

*Foothill-De Anza Community College District
Administrative Procedures*

- protect and secure *personal information* under their control using best practices as outlined in the publication: *Information Security Best Practices* which is available on the FHDA Website
- destroy data containing *personal information* when no longer needed
- See also: *Computer and Network Use: Rights and Responsibilities Policy / Procedures 3250 / AP 3250*
- Comply with an employee's duty to cooperate with any internal investigation associated with an incident / data breach.
- secure their own passwords and accounts.
- never share their passwords, PINs, or passphrases with anyone
- never use the same password for Foothill-De Anza Community College District accounts that are used for personal access.
- choose passwords that are difficult to guess.
- never insert passwords in email messages or other forms of electronic communication.
- never write passwords down, store online, or store in a .pda document without encryption.
- never reveal passwords over the phone, in questionnaires or in security forms.
- never talk about a password in front of others, nor hint at the format of a password.
- never use the 'Remember Password' feature of applications (e.g., Eudora, Outlook, Internet Explorer, etc.).
- immediately report a suspected compromise of an account or password has been compromised to their manager and the CSO and change all system passwords.

G. EMPLOYEES HANDLING CREDIT CARD INFORMATION HAVE RESPONSIBILITIES TO:

- ensure that the debit and credit card information is kept safe and secure at all times during the transaction
- accurately enter the payment information into Point of Sale (POS) terminals
- secure student's or customer's payment cards so that cards are not left unattended or to be given to any other person other than an approved employee for processing the payment
- notify a manager immediately should problems arise with any credit card transaction
- do not copy credit card information by any means including, but not limited to, written copies, spreadsheets / electronic formats, PDAs, laptops, manual impressions, magnetic, photos, etc.
- sign an acknowledgement that they have read, understood and agree to the Foothill-De Anza Community College District Policies and Procedures for PCI DSS compliance
- attend annual training on the payment card policies and procedures to review and maintain knowledge of the requirements of the payment card policies and procedures

- ensure that sensitive authentication data such as the card verification code, personal identification number (PIN) and the full magnetic stripe data are not stored at any time
- store, if needed, only the last four digits of the payment card account number when manually entering any transaction into electronic databases
- never send PAN data by end user messaging technologies such as instant messaging, email, SMS texting. (Users within the Cashier's Office are authorized to use hosted secure encrypted email and fax service, but must adhere to the Veritape Peepsafe Security Training Guidelines.)
- immediately notify their manager and the CISO if this policy has been violated. [deleted ...]
- mask PAN data If necessary to display it. (Only the first six and last four digits of a PAN number can be displayed.)
- never allow unauthorized employees or contractors to store or view full PAN data

H. OTHER RESPONSIBILITIES

- FHDA District Police will act as the point of contact between the district and external law enforcement agencies when external law enforcement agencies are involved
- ETS shall remove personal information (using an industry standard secure data removal tool) 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
- The vice chancellor of Business Services will ensure that appropriate employees are trained annually on payment card policies and procedures and keep records of all employees who are trained for a minimum of five (5) years.
- The purchasing / contracting manager will require external organizations (vendor, etc.), whose contracts with the district provides them access to personal data, sensitive electronic systems, or sensitive facilities, undergo a Vendor Security Review, prior to entering any agreement.
 - The purchasing / contracting manager must notify ETS in the event there are any material changes to the services, connectivity or type and content of data exchanged with the third party.
 - ETS will make a determination as to whether the changes require the department to request that the vendor undergo a new Vendor Security Review.

INCIDENT RESPONSE PROCESS

Incidents / data breaches cover the unintended, improper or fraudulent use, storage or release of personal information. This can be as a result of an external hack into the system, introduction of malware, theft of equipment, intentional or unintentional fraudulent activities by any person (external or internal).

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 suspects 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 ETS Call Center (during work hours) or the district police (after work hours). If the security breach is reported after work hours have ended, then district police will notify the Vice Chancellor of Technology. The Vice Chancellor of Technology or designee will notify the appropriate Lead Authority.

B. ISOLATE THE SYSTEM

For Computer Based Information Systems:

The *CBIS manager* 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.

For Stolen Computing Systems:

If a stolen *computing system* is recovered, the person gaining possession of the system will notify the Call Center, who 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 ETS Incident Response Team, in cooperation with District Police (if involved) and the CBIS manager, will look for evidence of a *security breach* to assess the possibility that *personal information* has been compromised.

D. REPORT THE INCIDENT

If the ETS Incident Response Team, in cooperation with District Police (if involved) and the CBIS manager, has sufficient reason to believe that *personal information* may have been acquired by or exposed to unauthorized individuals, the ETS Incident Response Team will submit written notification describing the nature of the *security breach* and estimated number of affected individuals to the:

- Chancellor
- President of the college (if applicable)
- Vice Chancellor of Technology (CISO)
- Lead authority
- District and college (as applicable) communication coordinators
- District Police

The CISO will notify the affected Credit Card Company within 24 hours if the incident involves the compromise of credit card information:

- Visa Fraud Control Group at (650) 432-2978
- MasterCard Compromised Account Team at (636) 722-4100
- Discover Fraud Prevention at (800) 347-3102
- American Express Merchant Services at (800) 528-5200

E. RESTORE AND RECONNECT THE SYSTEM

The CBIS manager 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 ETS Incident Response Team will work with the CBIS manager and District Police (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 communication coordinators (as appropriate), the Vice Chancellor of Technology, 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.

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 or Central Services 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:

- Chancellor
- President of the college (if applicable)
- Vice Chancellor of Technology
- Lead authority
- District communication coordinators

REFERENCES

- Information on privacy laws applicable to California
<http://www.privacy.ca.gov/lawenforcement/laws.htm#twelve>
- Important legislation governing the security of confidential information
 - 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)
- FHDA - AP 3410 Guidelines for Classification, Retention and Destruction of Records
<http://fhdafiles.fhda.edu/downloads/aboutfhda/3410ap.pdf>

*Foothill-De Anza Community College District
Administrative Procedures*

- FHDA - Policy 3250 / AP 3250 Computer and Network Use: Rights and Responsibilities
<http://153.18.96.19/downloads/etac/Policy3250.doc%20>
- FHDA – Policy 5050 Furnishing Information Concerning Students
- FHDA – Policy 4150 Personnel Files
- Information Security Best Practices www.fhda.edu/security
- PCI-DSS Industry Standards
https://www.pcisecuritystandards.org/security_standards/

See Board Policy 3260

Updated 12/1/11
Reviewed by Chancellor's Advisory Council 11/28/08, 12/1/11