Information Classification & Handling

Information Security Office
(408) 924-1530
Security@sjsu.edu

Mike Cook
Information Security Officer

Hien Huynh
Information Security Program Coordinator

What happens on campus?

Division of Academic Affairs

Information Technology Services

Office of Information Security

One Washington Square
San Jose, CA 95192-0013
Voice: 408.924.1705

Information Security Officer
Mike Cook

January 12, 2017
Notice of Data Breach

We are sending this letter to you as part of San Jose State University's commitment to privacy. We take privacy very seriously at San Jose State University and out of an abundance of caution it is important to us that you are made fully aware of a potential issue.

Last month, personal identifying information about you was disclosed following the theft of a desktop computer from the University Athletic Training Office. The theft was reported December 28th, 2016.

This information stored on the Desktop Computer included your First and Last Name, Social Security Number (SSN), Health Insurance Information and Medical/Injury records.

In response to the theft, San Jose State University is implementing encryption software on all computers used to store confidential data. This will render the information unreadable in the event a computer is stolen in the future.

If you have concerns about potential harm, the references below can explain how to receive a free copy of your credit report either through the Fair Credit Reporting Act or as a result of placing a fraud alert on your credit files:

California Office of Privacy Protection
http://www.privacy.ca.gov/consumers/identity_theft.shtml
Social Security Office http://www.ssa.gov/pubs/10064.html
Free Credit Report https://www.annualcreditreport.com

What happens on campus?

Division of Administration and Finance

Information Technology Services

Office of Information Security

One Washington Square
San Jose, CA 95192-0013
Voice: 408.924.1705

Information Security Officer
Mike Cook

March 22, 2016

I am writing to inform you of a situation that could affect you. On February 29th, 2016 personal identifiable information may have been exposed. Paper files belonging to the San Jose State University (SJSU) Record Clearance Project were stolen from a vehicle belonging to an SJSU employee. The stolen information included the data found on your Criminal Record including First and Last Name, Social Security Number and Criminal Background Check Results. Newark, Ca Police investigated the incident and your records were returned to SJSU's custody on March 3rd.

While we have no reason to believe that anyone viewed this information, we consider any breach a serious matter. We are reviewing our policies and data transport processes in order to prevent this from happening again.

While we cannot advise you on how to proceed, one option you have is to contact one of the credit reporting agencies, each of which has an automated phone-in fraud alert process.

Contact information for the credit agencies is listed below:

- Equifax - 800.525.6285 - http://www.equifax.com/home/
- Experian - 888.397.3742 - http://www.experian.com/

July 22, 2014

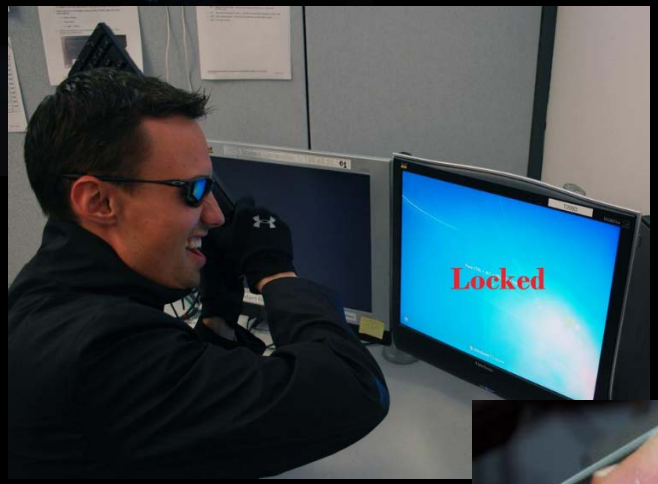
I am writing to inform you of a situation that could affect you. Beginning June 18th, personal identifying information about you was potentially shared. In the process of confirming your identity via video in a proctored exam, your information was available to Canvas Administrators, Blackboard Administrators and 22 of your fellow classmates. The information included the data found on your Drivers' License; First and Last Name, home address, weight, date of birth and drivers' license number. The mistake was reported and the information removed from Canvas and Blackboard on June 20th.

Division of

What do these events have in common?

Every incident which required reporting, credit monitoring or other action at SJSU since 2013 could have been prevented by taking minor precautions.

Physical Security In the Office



Lock your Screen

Lock your Cabinets

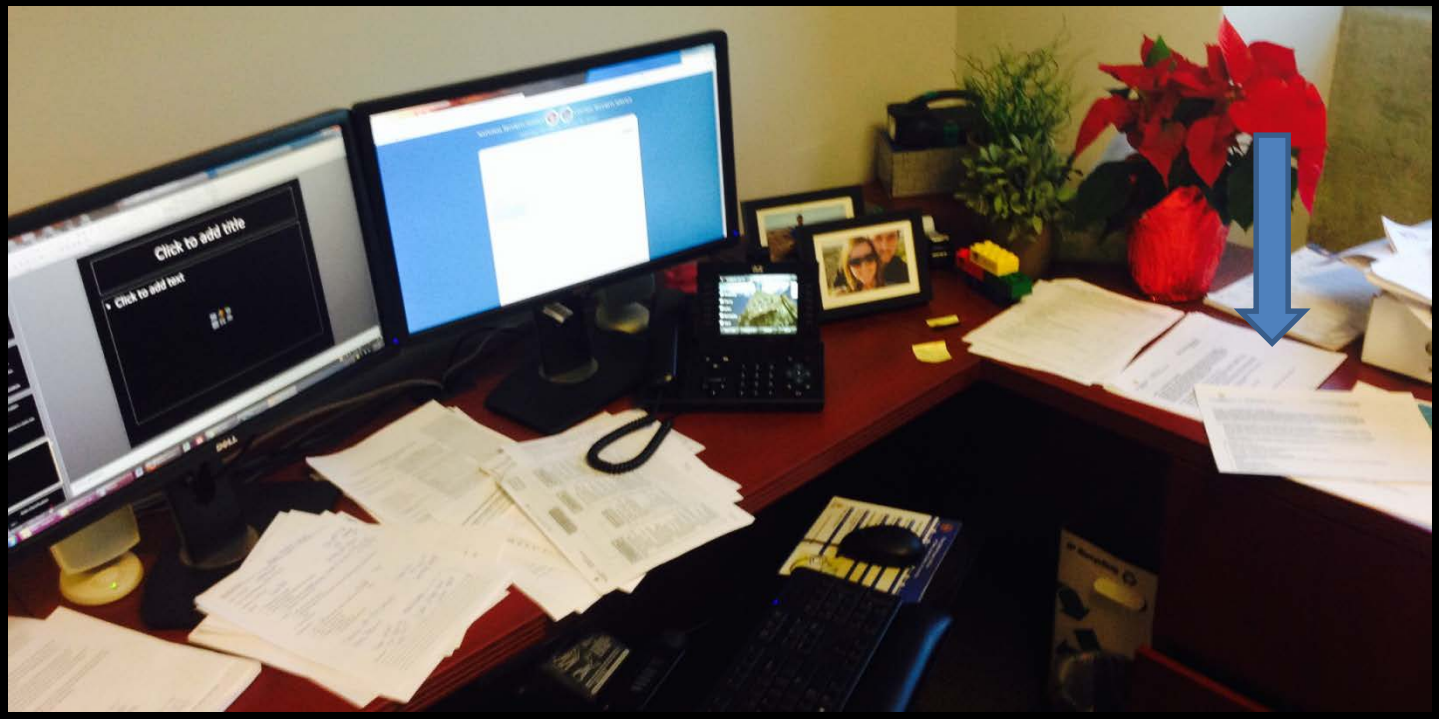
Don’t let people tailgate.

Don’t prop open doors to secure facilities.

Don’t share door codes.

Keep a Clean Desk

Lock up confidential data when you are away



Data Classification

At SJSU, we use 3 categories to classify Data

Data Classification

FERPA
HIPAA
PCI
Federally Protected
CSU Protected

Level 1

- Passwords
- PIN Numbers
- Birth Dates
- Credit Card Numbers
- Driver's License Numbers
- SSNs
- Health Insurance Information
- Medical Records
- Psychological Counseling Records
- Employee Home Addresses

Data Classification

FERPA
HIPAA
PCI
Federally Protected
CSU Protected

Level 2

- Identification Photos
- Student Information (Grades, courses, schedule)
- Library Circulation Information
- Linking a User to a Subject Area
- Bids
- Intellectual Property
- Information Under NDA
- Maps of Campus Utilities
- Construction Drawings
- Licensed Software
- Accident Reports
- Personal phone numbers, addresses, salaries
- Donor Information

Data Classification

FERPA
HIPAA
PCI
Federally Protected
CSU Protected

Level 3

- SJSU ID
- Employee Email Address, Title, Department
- Budget
- Student Information
  - Name
  - Major
  - Sports Information
  - Weight and Height
  - Dates of Attendance
  - Full-Time Status
  - SJSU Email Address

Protection of Electronic Data by Classification

What can I do where?

	Network File Share	C: Drive (Documents, Desktop, etc.)	Google Drive	Personal Dropbox, Box.Com, etc.	SJSU Email	Thumb Drive
Level 1	Yes	Requires Encryption	No	No	Requires Encryption*	Requires Encryption
Level 2	Yes	Best Practice, No or Use Encryption	Yes	No	Best Practice, No	Best Practice, Erase when Finished
Level 3	Yes	Yes	Yes	Yes	Yes	Yes
FERPA	Yes	Yes	Yes	No	Best Practice, No	Best Practice, Erase when Finished

Protection of Electronic Data by Classification

Types of controls we need to put in place depend on the sensitivity of the data.

Level 1 – Must not be viewable by an outside party. Encrypted in flight. Encrypted at rest or other compensating controls. Systems patched. Data centers secure. Employee background checks. Follow password standards. Change Management. Secure applications.

Protection of Electronic Data by Classification

Types of controls we need to put in place depend on the sensitivity of the data.

Level 2 – Must not be viewable by an outside party as part of normal operations (Google). Encrypted in flight. Systems patched. Data centers secure. Follow password standards. Change management. Secure Applications

Level 3 – Public information, no controls needed UNLESS student has requested a FERPA hold.

Protection of Electronic Data by Classification

EVERY application, every database, every system we touch is unique.

Ask yourself, what type of data am I handling?

http://security.sjsu.edu/ - Policies and Standards –
Data Classification Levels Cheat Sheet

If you have questions, ask me. We are here to help!