

Security Best Practices Quick Guide**Passwords**

- **Do not** display passwords in your work area.
- **Do not** let others see you type your password.
- **Do not** use the same password more than once or in multiple system/websites.
- **Do not** use: a word, a foreign word, common wildcard replacement @=a, !=I or \$=S in a word, any of the above starting or followed by a 1 or 2 digit number.
- **Do** use a personal phrases to remember passwords (e.g. as a new hire your password could be Isw@CSi12 for “I started work at Sacramento State in December” (Do not use this password.)
- **Do** change your password immediately if you suspect it has been compromised in any way.

Email

- If sending an attachment, notify the recipient of the impending e-mail so they will expect it.
- Do not click on links provided in e-mails unless you trust the source and it is appropriate.
- Do not open spam messages or click on “unsubscribe”, delete it and create a junk mail rule
- Do not e-mail passwords, SSNs, credit card numbers, or other protected data.
- Use BCC (Blind Carbon Copy) for large numbers of recipients. This protects the recipients e-mail address.
- Listen to your instincts when reading and responding to e-mails.

Social Engineering

- Question people in your area whom you do not recognize.
- Call your manager or supervisor to verify if a situation is legitimate.
- Do not give in to artificial pressure. A social engineer may state deadlines, tell you they are going to get in trouble, or that you will lose something or miss a great opportunity.

Internet, Instant Message and Instant Relay Chat

- Assume everything on the Internet is public.
- Do not provide personal, sensitive or confidential information on internet sites, surveys, or forms unless you are using a trusted and secure web page.
- Make sure you are on a secure page before logging in or providing confidential information. Secure pages start with https in the URL, be sure to check for the little lock that appears in the corner on most browser’s windows.
- Do not post confidential information on the Internet.
- Use Internet Explorer with caution. If possible, use a more secure alternative like Firefox and Safari.

Workstation

- Power down your workstation when leaving for the day.
- Password-protect your screen saver and configure to turn on after 10 minutes of inactivity.
- Screen lock your workstation when you leave your work area.
- Physically secure your computer if you are in a public area.
- Run up-to-date virus protection software.
- Update and install security patches as soon as possible (e.g. “Install and shut down”.)

Physical Security

- Check doors, drawers, and windows to make sure they are secure.
- Lock up sensitive materials before you leave your area.
- Never share your access card or key.
- Do not hold secure doors open for unknown people.
- Secure laptops with a lockdown cable, store in locked truck or room.

Protect Confidential Data

- Make sure your department has a data retention policy.
- Do not keep confidential data you no longer need.
- Only allow access to confidential data on a need-to-know basis.

Security Best Practices Quick Guide

Protect Confidential Data

Security of confidential data is of utmost importance at Sacramento State. By law, most student and employee information is confidential and must be handled in a secure manner. No private/confidential data should be stored on your computer or in unlocked areas.

Information kept on your computer can be accessed by someone using your computer or hacking into it from the outside. When the security of personal information is believed to be breached, hundreds of hours of university and outside staff time are involved in investigating and repairing the breach and notifying those affected.

You are responsible for the security of the material that you store, send, or display using the campus computing and communications resources. If you work with confidential information you must be aware of and comply with numerous legal requirements and policies. See <http://www.csus.edu/irt/is>, click on Policies and Procedures.

Confidential data include social security numbers (SSN), drivers license numbers, credit card numbers, grades, birth dates, tax information, marital status, net pay, and so much more. For more information <http://www.csus.edu/irt/is>

Action Items to Safeguard Protected Information

1. Understand what is protected data:

Ask yourself what type of data you are working with and whether it is level 1 or level 3. Level 1 data is the most confidential and are items such as SSNs and Credit Cards. The type of data you work on determines how you should handle it as well what level or protection it should have.

2. Removing confidential data:

If you work with confidential data, you will need to remove the information and files from your local computer and save it to a secure server where the files can be protected and backed-up. Work with your Information Technology Consultant (ITC) to find the best possible solution.

3. Converting confidential information:

If you do not need to use confidential data change it to an acceptable business use format such as SSN being the Employee ID and credit cards only showing the last 4 digits. Work with your ITCs to find the best possible solution.

4. Need to use:

Be aware of who is accessing confidential data. This information should be accessed on a need to know basis. You ITC can help you create security groups in order to set the proper access privileges to your files.

5. Archive

Confidential data that is not longer be accessed but needing to be saved for records reasons should be archived. The Information Security Office (ISO) recommends working with your ITC on encrypting this information for further protection.

6. Question

Are you running more than one system with protected data stored on it? If you have more than one system with protected data, the ISO and your ITC can help consolidate your information to a central location that can be protected and backup.

For information on protecting your data see <http://www.csus.edu/irt/is>, or call the Information Security Office, x81999. For information on security policies, or to set up a training or informational meeting, call Adam Cook, Information Security Analyst, at x81999. For more information see <http://www.csus.edu/irt/is>

It is everyone's responsibility to safeguard our campus community.