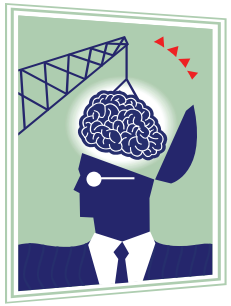
Resources

Want to learn more about security and privacy?

These resources provide guidance and information

- California State Information Security Office—www.infosecurity.ca.gov/
- California Office of Privacy Protection—www.privacy.ca.gov/
- California Department of HIPAA Implementation—www.calohi.ca.gov/
- California Highway Patrol—www.chp.ca.gov/html/computercrime.html
- Multi-State Information Sharing and Analysis Center (MS-ISAC) —www.msisac.org/
- United State Computer Emergency Readiness Team (US-CERT) —www.uscert.gov/
- SANS Institute—www.sans.org/



References used to create this Brochure:

- CalSTRS Information Security Awareness Booklet (October 2006)
- Multi-State Information Sharing and Analysis Center (MS-ISAC) —www.msisac.org/
- United State Computer Emergency Readiness Team (US-CERT) —www.uscert.gov/

CA State Information Security Office

You will find other useful Brochures, Guides, and Checklists available on our Web site at www.infosecurity.ca.gov/ including:

- Information Security Incident Notification Roadmap for Information Security Officers
- Information Technology Security Program Guideline
- Information Technology Security Risk Assessment Checklist

Contact Us:

CA State Information Security Office

Phone: (916) 445-5239

Email: security@oispp.ca.gov

Web: www.infosecurity.ca.gov

November 2008

CA State Information Security Office

Top Ten Information Security Practices You Should Know

Sound Security Practices for All Employees to Consider

Security is Everyone's Business!

Top Ten Security Practices for State Employees.....

Information Security—You Are The Key!

Information Security is about protecting your department's information and its assets from intentional or accidental misuse or disclosure. That means knowing about threats and vulnerabilities, practicing security-minded work habits, and making sure everyone follows your department's information security policies and practices.

There are many aspects to Information Security. Most people think of Information Security as computer passwords and locking up laptops. But it means much more, and includes things like properly identifying a caller, remembering not to leave personally identifiable information (like social security numbers) in printers, and storing procedural manuals for safe keeping.

Since you have access to your department's information and assets, you are responsible for taking a proactive approach to Information Security. This means practicing good Information Security work habits every day, reporting possible Information Security issues, and keeping up on the latest Information Security policies and practices.

This Brochure is a good way to educate all employees. We hope you find it valuable and will share it with others.

What is the key to Information Security?

YOU!

Executives

1. Promote Information Security. It starts at the top!
2. Designate an Information Security Officer (ISO).
3. Place your ISO at the right level in your organization.
4. Be familiar with security and privacy laws, regulations, and policies.
5. Develop, update, and review policies annually.
6. Implement training and awareness programs.
7. Make security and privacy training mandatory for all employees and contractors.
8. Conduct risk assessments routinely.
9. If a security breach occurs, know who to contact and what to do.
10. Recognize that security is a business enabler.

Train Your Employees!

Managers and Supervisors

1. Inform contractors of security requirements.
2. Develop and use non-disclosure agreements.
3. Protect information in any format (electronic, paper).
4. Know how to recognize a security problem and when to contact your ISO.
5. Involve your ISO in all IT projects.
6. Ensure your employees follow policy and good security practices.
7. Don't allow untrained staff to take responsibility for securing important systems.
8. Understand the relationship of information security to the business process.
9. Realize the value of your department's information and its reputation.
10. Follow through with the operational aspects of security. Ensure the problems stay fixed.

IT Staff

1. Report security incidents to your ISO immediately!
2. Update anti-virus, spyware, and operating software daily (automate, if possible).
3. Complete incremental backups daily, full backups and off-site storage weekly.
4. Change staff access control when duties change or staff leave.
5. Review hardware/software inventory annually.
6. Review information assets and applications as acquired.
7. Notify users of alerts and advisories.
8. Test your Disaster Recovery Plan at least annually.
9. Take steps to securely sanitize storage media and equipment before disposal or reuse.
10. Protect essential hardware and software.

Report incidents immediately!

Employees

1. Report security incidents to your ISO immediately!
2. Read and comply with your department's security and privacy policies.
3. Do not e-mail confidential information.
4. Secure your workspace.
5. Use encryption software on your mobile devices, like laptops and personal assistance devices.
6. Lock your computer before you leave your seat.
7. Create passwords that are not easy to guess.
8. Do not share your passwords.
9. Secure paper that contains personal or confidential information.
10. Physically protect equipment assigned to you.