Protecting Your Gear, Your Work & Cal Poly

Information Security Office

Sharif Sharifi, CISSP, CRISC
Kyle Gustafson, Information Security Analyst
Jon Vasquez, Information Security Analyst
What is Information Security?

- Is the practice of defending information from unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction.

  Source: http://en.wikipedia.org/wiki/Information_security
Why Is Information Security Important?
Cost of Data Breach

– **Direct Cost**
  - Notification
  - Call Center
  - Identity Monitoring
  - Identity Restoration
  - Forensics
  - Loss of Employee Productivity

– **Indirect Cost**
  - Restitution
  - Additional Security and Audit
  - Lawsuits
  - Regulatory Fines
  - Loss of Consumer Confidence
  - **Loss of Funding**

Reported average total cost of $214 per record
Laws & CSU Policies

• Breach Notifications (SB-1386)
• FERPA – Family Educational Rights & Privacy Act
• HIPAA – Health Insurance Portability Accountability Act
• PCI – Payment Card Industry standards
• CSU policies
CSU & Cal Poly

- CSU and Cal Poly have policies and procedures to protect the privacy and security of information
  - security.calpoly.edu
- As a Cal Poly workforce member, you are responsible to follow these policies and procedures to protect the privacy and security of information
- Ask your Supervisor or Manager for guidance
- Remember that privacy applies to ALL verbal, written, and electronic information
Data Classification and Handling (Level 1)

- **Personal Identifiable Information (PII):**
  - Passwords or credentials
  - PINs (Personal Identification Numbers)
  - Birth date combined with last four digits of SSN and name
  - Credit card numbers with cardholder name
  - Tax ID with name
  - Driver’s license number, state identification card, and other forms of national or international identification (such as passports, visas, etc.) in combination with name
Information Requiring Special Protection (Level 1)

- **Medical Information:**
  - Health insurance information
  - Medical records related to an individual
- **Financial Information:**
  - Bank account or debit card information in combination with any required security code, access code, or password that would permit access to an individual's financial account
Data Classification and Handling (Level 2)

- Identity Validation Keys (name with)
  - Birth date (full: mm-dd-yy)
  - Birth date (partial: mm-dd only)
  - Photo (taken for identification purposes)
- Student Information - Educational Records not defined as “directory” information, typically
  - Grades
  - Courses taken
  - Schedule
  - Test Scores
  - Advising records
  - Educational services received
  - Disciplinary actions
  - Student photo
- Library circulation information
- Trade secrets or intellectual property such as research activities
- Location of critical or protected assets
- Licensed software
Email & Phishing

– Never provide your username and password to an email request
  • ITS will never ask you to provide this information via email or phone

– Delete spam and empty the “Deleted Items” folder regularly
Data Security & Secure Shredding
Best practices for Level 1 & Level 2 data

- Only use or store Level 1 and Level 2 data **when necessary**.
- Whenever possible, minimize or eliminate the use of sensitive information.
- Do not leave paper documents that contain sensitive information **unattended**.
- When printing or scanning sensitive documents, retrieve them immediately from the printer/scanner.
- Store paper documents with sensitive information in **locked file cabinets** that are kept in a secure location.
- Ensure the keys to the file cabinets storing sensitive information are **properly secured** as well and that only approved faculty or staff have access to keys for the file cabinets.
- This should be limited to only faculty and staff that **need to know** the information for their duties at Cal Poly.
- **Shred sensitive paper documents** or dispose of them through Cal Poly’s secure disposal service when they no longer need to be retained.
Top 10 Best Security Practices

1. Install anti-virus
2. Keep your computer updated
3. Log off public computers
4. Back up important information
5. Lock your computer
6. Download files legally
7. Create strong passwords
8. Keep personal information safe
9. Secure your phone
10. Limit social network sharing
Report Incidents

- Immediately report lost or stolen electronic devices
- Immediately report any unusual or suspected information security incidents

security@calpoly.edu
abuse@calpoly.edu
Thank you

security@calpoly.edu
abuse@calpoly.edu

security.calpoly.edu