

Security Management at Cal Poly

Ryan Matteson, CISSP

ITS Office of the CIO – Security Assurance

Agenda

Topics I will cover:

- What is security? Why does it matter?
- How can we think about security in a productive way?
- Approaches to implementing security, with examples.
- Question and Answer.

What is security?

- Security is freedom from risk or danger.
- Risk can never be completely removed, but it can be lessened.
- Information systems security: measures to ensure the confidentiality, integrity, and availability of information.

Why does it matter?

- At Cal Poly we have many valuable assets, and some of these are held in or controlled by information systems:
 - Personal information (student, employee, client)
 - Financial information and controls
 - Computational and network resources

Compromises of these assets cost us (time, money, confidence, legal liability)

How do we think about security?

- Security can be:
 - **process**: ongoing effort towards a goal
 - Example: inspection/maintenance of aircraft
 - **enabler**: making things practical by lowering risk (it's not about creating inconvenience).
 - Example: seat belt
 - **risk management**: allocating resources towards the effort, based on analysis of dangers or costs
 - Example: credit card company

All of us share some responsibility for security (for ourselves, for Cal Poly, for the State, ...)

How do we think about security?

- In information systems (InfoSec), the primary goals are C I A (*not* confusion, ignorance, annoyance!)
- Confidentiality: enforce secrecy
- Integrity: protect accuracy/reliability
- Availability: prevent disruption of service

InfoSec Management: The Ten CISSP Areas

- **Access Controls**
- Telecomm & Network Security
- **Security Management**
- Applications Security
- Cryptography
- Security Architecture
- Operations Security
- Business Continuity Planning
- **Law, Investigations & Ethics**
- Physical Security

Security Management

- Catalog organization's information assets
- Documentation/implementation of policies, standards, procedures, guidelines.
- Example: Information Security Program
- Concept: Documentation
- Concept: Risk Assessment

Security Management: Information Security Program

Cal Poly Information Security Program

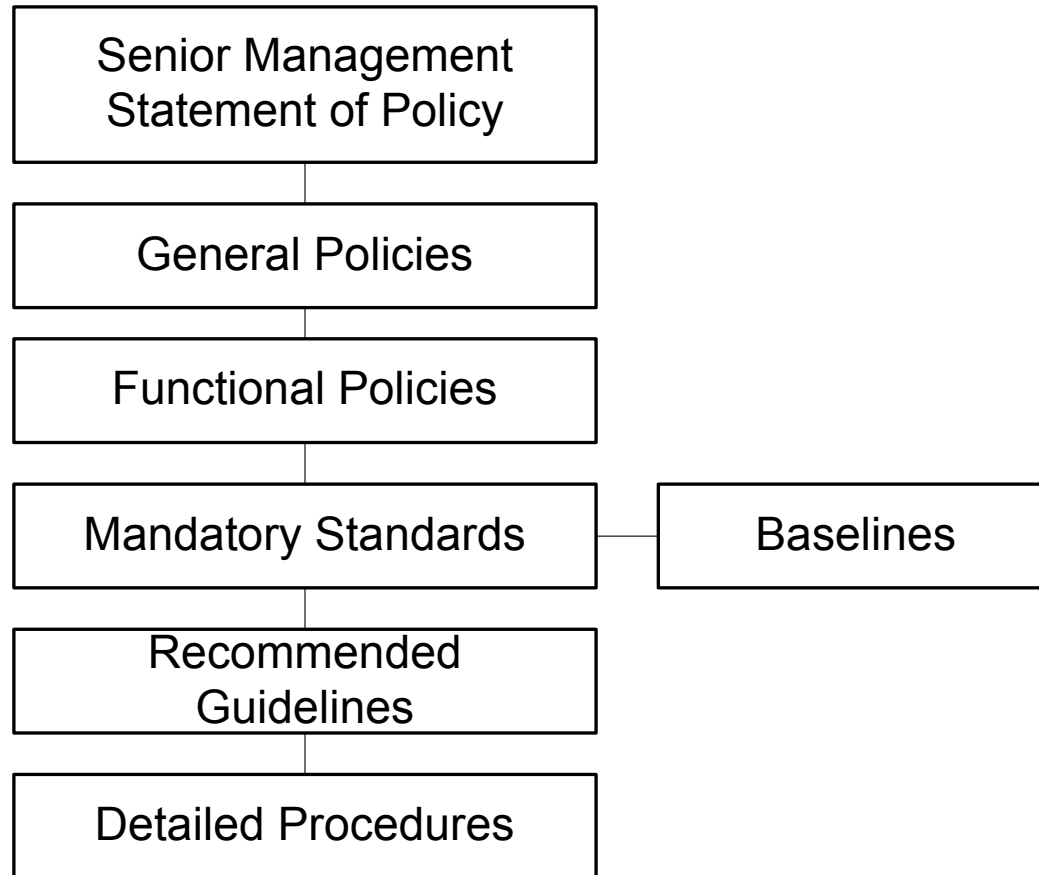
Policy Development History	
October 19, 2004	Amended scope to reflect Unit 4 exception
July 8, 2004	Final approval by President Warren Baker
May 11, 2004	Policy endorsed by Information Resources Management Policy and Planning Committee (IRMPPC)
January – May 2004	Constituency Review
December 8, 2003	Draft policy released

Introduction

As part of its educational mission, the University acquires, develops, maintains and archives information. University information is found throughout the campus community in various forms, including paper documentation, electronic form, and verbal communication. Therefore, this program is widespread and relies on employees to use reasonable judgment in its application.

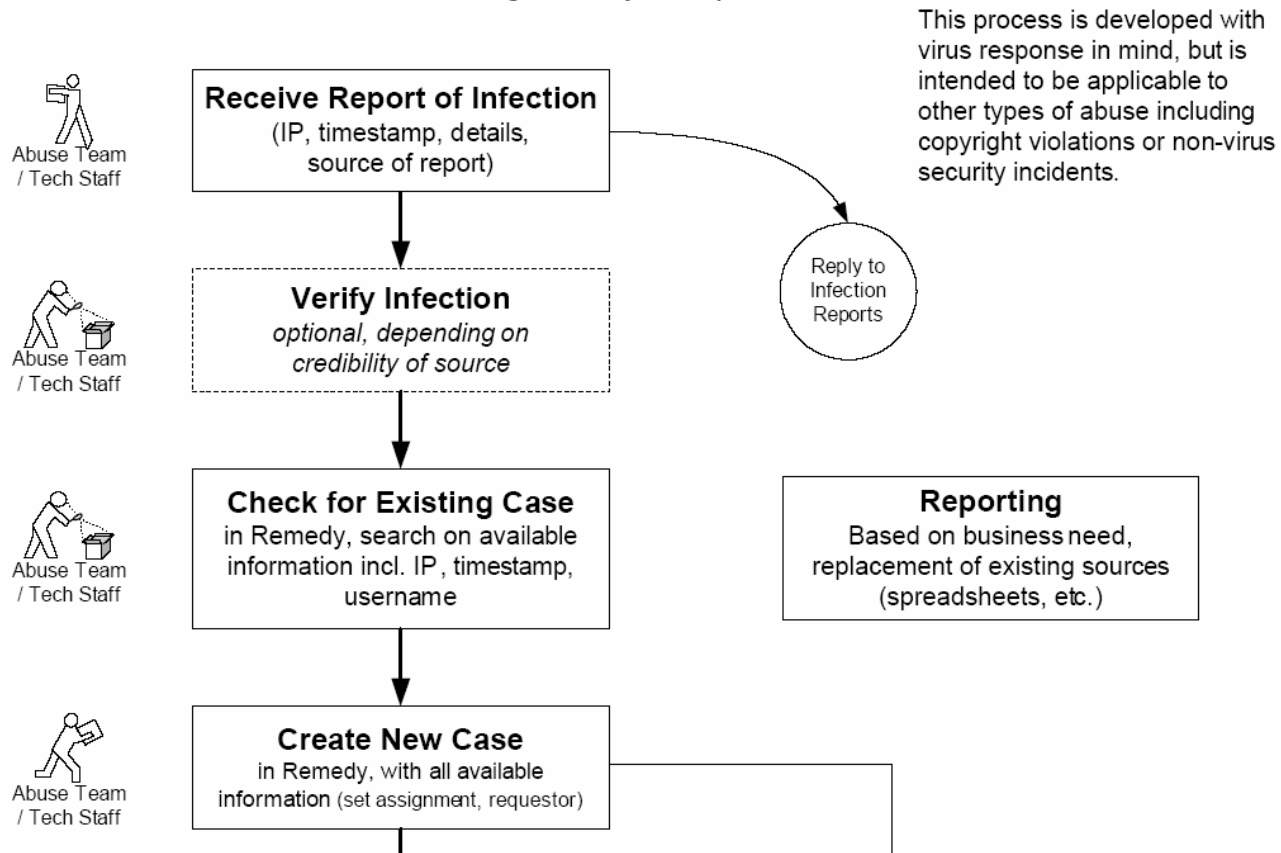
This program, along with campus processes, is designed to ensure that Cal Poly meets the generally recognized standards known as the “fair information practice codes” and its core principles of: (1) Notice/Awareness; (2) Choice/Consent; (3) Access/Participation; (4) Integrity/Security; and (5) Enforcement/Redress and is in compliance with the Gramm-Leach-Bliley Act.

Security Management: Documentation

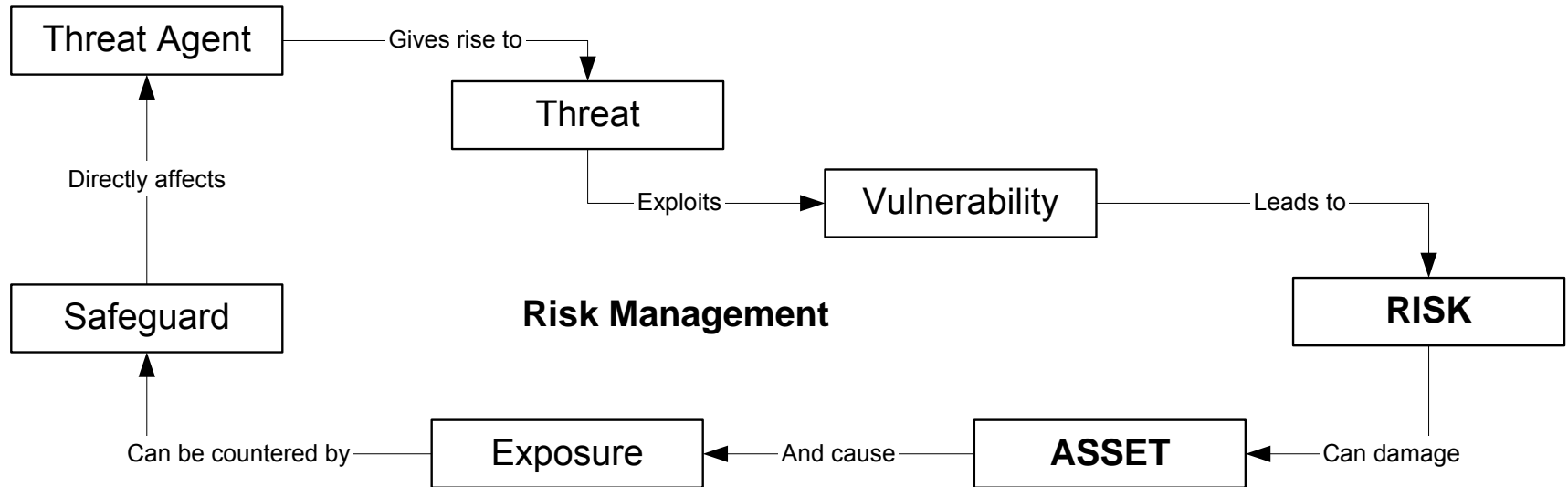


Security Management: Documentation

Cal Poly - Campus Desktop Abuse Response with ITS and Housing as Key Responders

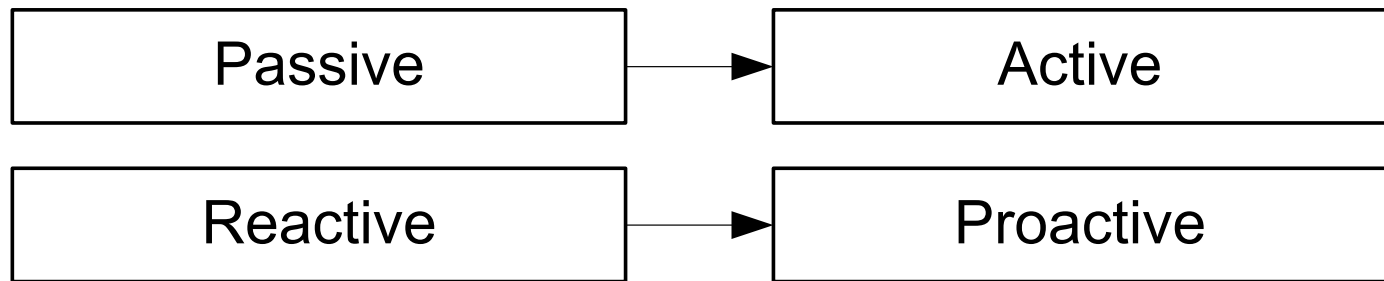
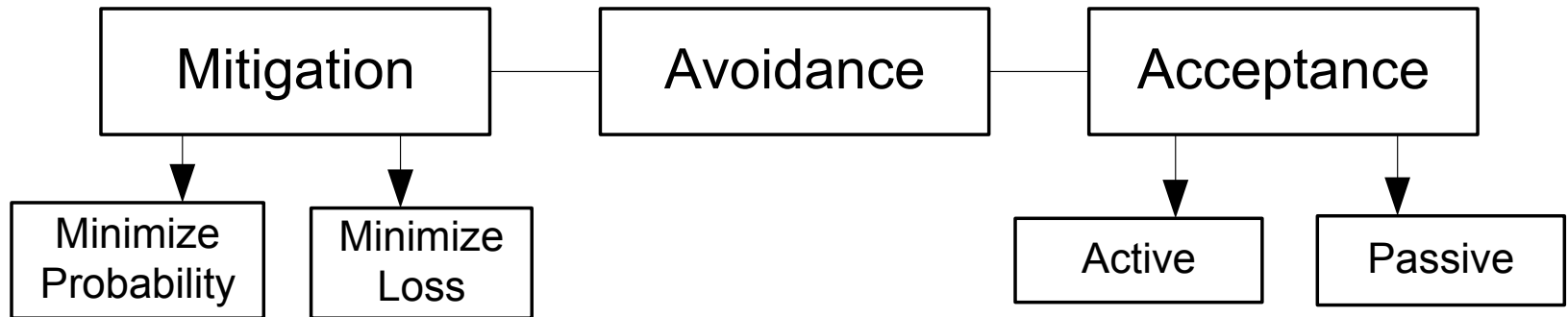


Security Management: Risk Assessment



Security Management: Risk Assessment

Risk Response



Law, Investigations & Ethics

- Policy must be aligned with and support law.
- Organizations must show due diligence:
 - Roles of Vicki and Me
 - Effort to follow industry standards, ISO17799
- It's a growth area.
- Example: California SB1386
- Example: U.S. FERPA

Law: California SB1386

Effective on July 1, 2003, amending civil codes 1798.29, 1798.82 and 1798.84:

Agency, person or business that conducts business in California and owns or licenses computerized 'personal information' must disclose any breach of security to any resident whose unencrypted data is believed to have been disclosed.

Remember: Sec Mgmt Info Classification

Example: State Controller's Office

Law: California SB1386

Example: State Controller's Office



THE CALIFORNIA STATE UNIVERSITY

BAKERSFIELD • CHANNEL ISLANDS • CHICO • DOMINGUEZ HILLS • FRESNO • FULLERTON • HAYWARD • HUMBOLDT
LONG BEACH • LOS ANGELES • MARITIME ACADEMY • MONTEREY BAY • NORTHRIDGE • POMONA • SACRAMENTO
SAN BERNARDINO • SAN DIEGO • SAN FRANCISCO • SAN JOSE • SAN LUIS OBISPO • SAN MARCOS • SONOMA • STANISLA

OFFICE OF THE
UNIVERSITY AUDITOR

July 21, 2004

I am writing to inform you that a hard drive from a laptop computer belonging to the California State University systemwide Office of the University Auditor was either inadvertently discarded or stolen sometime over the weekend of June 26-27, 2004. This hard drive contained personal information, including your name and Social Security Number. While there is no indication that your private information was accessed for the purposes of identity theft, we are sending this notification to you as required by California Civil Code 1798.29, commonly referred to as SB 1386. Please accept our sincere apologies. This is a very serious issue for us, and we know that it is a very serious concern for you.

Law: California SB1386

Example: Berkeley Research Program

Law: FERPA

Family Educational Rights and Privacy Act:

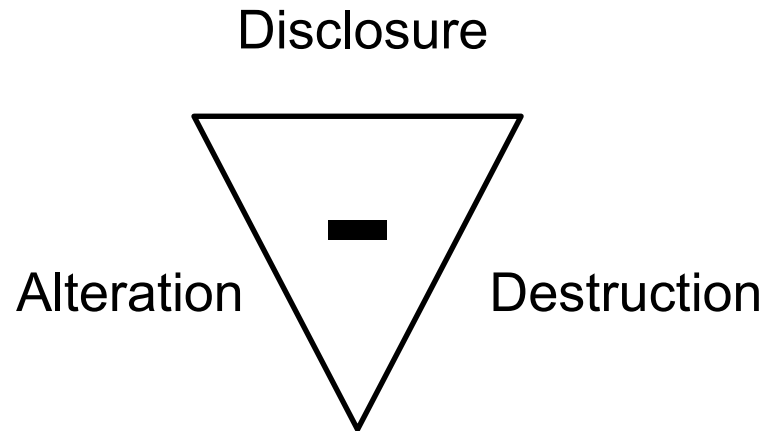
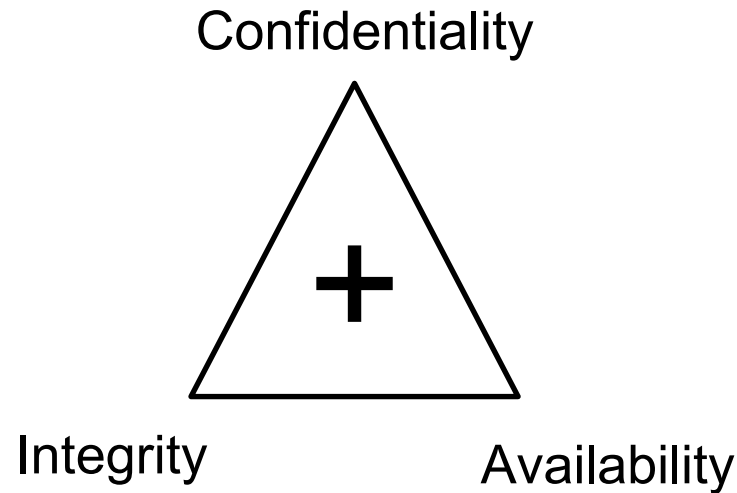
The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.

...

...schools must ... allow parents and eligible students a reasonable amount of time to request that the school not disclose directory information about them. Schools must notify parents and eligible students annually of their rights under FERPA.

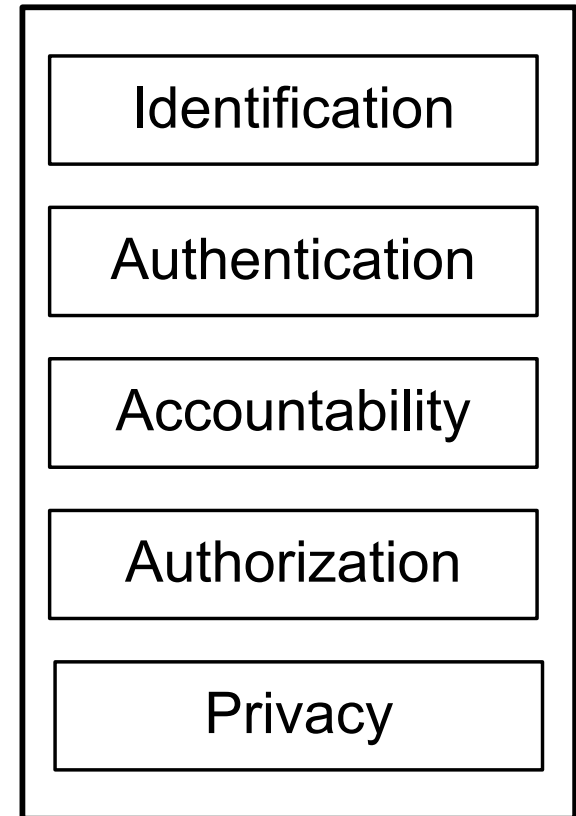
<http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html>

Review: How do we think about security?



Access Controls

- Mechanisms that allow managers to direct or restrain use of a system: what the user can do, what they can access.
- Common target for attacks.



Access Controls: Campus Password Practices

- Passwords are a *means to provide all three*: confidentiality, integrity, availability
- In order to ensure that they are an effective means, we must address the threats that make them less effective.
- Following good password practices is a way for you to help improve security – which benefits you and the University.

How do campus password practices fit in?

- Threats: guessing, disclosure, sharing, reuse
 - Guessing: passwords must be difficult to guess (including by automated means) → they must include many different characters and not be based on words
 - How ITS is helping: the Password Manager available at my.calpoly.edu displays and follows rules for creating passwords which are difficult to guess.

How do campus password practices fit in?

- Threats: guessing, disclosure, sharing, reuse
 - Disclosure: each user should protect the secrecy of their own password; do not put it on a sticky-note on your monitor!
 - How ITS is helping: we're standardizing on a single username and password (used for my.calpoly.edu, e-mail, calendar, PeopleSoft, etc. etc.)
 - If you only have one to remember, and you use it often, there's less need to write it down.
 - If you have trouble, call the Service Desk at X67000 or your local support staff – they can help!
 - If you're developing a new information system, don't create new passwords – talk to us!

How do campus password practices fit in?

- Threats: guessing, disclosure, sharing, reuse
 - Sharing: (intentional disclosure) each user should have and use their own password, and not share it with others.
 - If someone else has a legitimate need to access a system, help them to obtain their own account!

How do campus password practices fit in?

- Threats: guessing, disclosure, sharing, reuse
 - Reuse: Don't reuse your Cal Poly password in other contexts, such as non-University web sites.
 - We have measures in place to keep your password secure when it is used within Cal Poly systems -- but we can't protect it if you share it with xyz.com!

Further reading...

- ISC2 Certified Information Systems Security Professional (CISSP) – esp. Associate Program
 - <http://www.isc2.org/>
- Cal Poly IT Responsible Use Policy
 - <http://www.calpoly.edu/computing/policy.html>
- Password practices
 - http://helpdesk.calpoly.edu/faq/password_faq.html
- Campus Information Security Program
 - <http://its.calpoly.edu/Policies/isp.pdf>
- Beyond Fear
 - “Thinking Sensibly About Security in an Uncertain World”
 - Bruce Schneier, HV6432 .S36 2003
 - Non-technical. It will help you think about security as it applies to your day-to-day life, from your ATM card to the threat of terrorism.

Contacts

- Immediate threats to safety: call 911
- Violations of campus information or responsible use policies:
abuse@calpoly.edu
- Discussion or questions on information security issues: rmatteso@calpoly.edu