



Information Technology Services

UCSC Information Security Program Framework

SECURITY STRATEGIC DIRECTIONS: PRIORITIES #1-3

#1: Supporting a Secure and Mobile Community

#2: Locating and Protecting our Most Sensitive Data

#3: Practices that Manage Risk from a Changing Security Landscape

OUTCOMES

Implementing Minimum Network Connectivity Requirements

Minimum Requirements / Remote Access checklist for personally-owned computers

Clearly identify tools that can strengthen security for personally-owned computers

Evaluate posture assessment for each connection method (VPN, wired network, wireless)

Identify targets in Minimum Requirements for technical enforcement

Minimum patching recommendations

Security standards and validation procedures for devices in DC

** Compliance audit for campus servers & workstations consistent with IS-3

** Enforce secure desktop configuration settings with remote management tools

Enable Secure Communications

Identify gaps in ITS use of secure protocols (SSH or SSL)

Evaluate requirements for campus VPN service

** Tools for secure communication readily available to the campus:
- Secure wireless
- Campus VPN

Identify Sensitive Data

Identify systems that should not contain PII and are at risk of having it for periodic scans

Faculty-directed communication re. where PII is likely to be and how to check for it

** Reinforce procedures to check/scan for PII in response to established triggers

Manage Sensitive Data

ITS Backup Retention Standards

Scope and implement IDS: hardware, and FTE/processes

Evaluate REN ISAC Security Event System as correlation/aggregation system for security event information

Scope and implement centralized log collection and management

** ITS Log Policy & Standards

Manage Privileged Access

Develop role-based matrix of privileged access

Review/refine privileged accounts for least restrictive access to systems/applications in DC

Technical measures to further restrict access to privileged systems and accounts

Assess and Define Data Center (DC) Perimeter

Risk assessment of DC perimeter

Privileged access to DC via DC VPN only: policy & implement

Education and Security Awareness Training

Tools for end user security evaluation of external ("Cloud") services/applications

Cloud services security and privacy education

Faculty-directed computer security communication

** Continuing campus and ITS computer security outreach

Implement Defined Password Strategy

Identify ITS-managed systems/applications that can technically use CruzID Gold; review implications regarding InCommon audit or certification

Policy on required use of two-factor authentication

Carry-Over from Electronic Information Policy Framework

Roles and Responsibilities for UCSC Electronic Information Resources