UPDATED IS-3 LOCAL CAMPUS IMPLEMENTATION POLICY NUMBER 400-32

University of California, Riverside
Computing & Communications
INTRODUCTION

- UCR’s Electronic Information Security Policy → Implementation of IS-3 (UC’s primary information security policy)

- Scope
  - Defines campus responsibilities
  - Provides definitions relating to IS-3 and UCR’s local implementation of IS-3

- Objective: Requires campuses to …
  - Evaluate electronic information resources
  - Determine which resources contain Personal Protected/ essential/ restricted information
  - Develop local guidelines/policies for securing electronic assets
  - Institute mechanism for ensuring implementation and periodic review of guidelines
Campus-wide and departmental security plans must address these key issues:

- **Risk Assessment**
  - Used to inventory/determine nature of electronic information assets held by campus units

- **Essential Data / Electronic Resources**
  - Failed or compromised data/systems that could result in inability to perform mission-critical functions, loss of funds or information, or significant liability to campus

- **Restricted Data / Electronic Resources**
  - Confidential or personal information that is protected by law or policy and requires highest level of access control and security protection
GENERAL POLICY REQUIREMENTS

- Campuswide Responsibilities
  - Computing and Communications Security Organization
  - Operationalized Security Implementation Documents
  - IS3 Campus Security Departmental Planning Template
  - Security, Privacy, and Confidentiality Communications and Awareness Program
  - Security Breach Prevention and Incident Reporting Program
GENERAL POLICY REQUIREMENTS

- 6 Security Implementation Documents
  - Risk Assessment, Disaster Recovery, and Organizational Structures
  - Identity Management Systems
  - Servers and Operating Systems Security
  - Database Security
  - Physical Security
  - Network Security
  - Application Development – Change Control & Vulnerability Scanning
GENERAL POLICY REQUIREMENTS

- Departmental and Unit Responsibilities
  - Security Plan
  - Minimum Security Standards
  - Other Legal, Industry, or other Policy Security Requirements
  - Annual Risk Assessment and Inventory of Systems Containing Personal Protected Data
  - Security Communications
  - Contractual Agreements
• Remediation

  • If policy violations discovered:
  • C&C will remove impacted systems from campus network
  • Network access will be enabled after the following:
    • Remediation of issues in question
    • Consultation with appropriate Dean, Vice Chancellor, or administrative official