Introduction – UCR Information Security Plan

Elements of UCR’s Information Security Plan

- Computing and Communications Security Organization.
- Operationalized Security Implementation Documents.
- IS3 Local Campus Overview – Departmental Planning Template.
- Security, Privacy, and Confidentiality Communications and Awareness Program.
- Security Breach Prevention and Incident Reporting Program.

Overview of Security UCR’s Information Security Plan Elements
Introduction – UCR Information Security Plan

Computing and Communications utilizes a combination of tools / techniques / staff to support desktop, network, server, database, and application security. These efforts help stop problems at the campus border router, detect intrusions, monitor traffic for denial of service patterns, and ensure the integrity and privacy of protected (personal) data.

Nevertheless, UCR is a research university that maintains a network that is more open than most networks found in the private sector. Moreover, the computing infrastructure that the network supports (web servers, applications servers, etc.) is more distributed than that deployed in many for-profit companies.

While this topology supports the research and instructional missions of the university, UCR's open and distributed network & computing infrastructure requires that the security, confidentiality, and privacy of campus electronic communications and data be a shared responsibility. Thus, security should be given the highest possible level of attention not only by C&C, but by any and all individuals, groups, departments, or organizations that provide, host, or enable electronic communications, data storage, or other computing infrastructure.

Thus, UCR’s Information Security Plan includes BOTH efforts, tools, and programs to secure core, enterprise systems, but also includes processes, policies, and outreach to assist campus organizations and departments to ensure the security of non-centrally maintained data and systems.

Elements of UCR’s Information Security Plan

UCR’s Information Security Plan consists of the following five discrete elements:

- Computing and Communications Security Organization.
- Operationalized Security Implementation Documents.
- IS3 Local Campus Overview – Departmental Planning Template.
- Security, Privacy, and Confidentiality Communications and Awareness Program.
- Security Breach Prevention and Incident Reporting Program.
Overview of Security UCR’s Information Security Plan Elements

Computing and Communications Security Organization.

Computing and Communications is UCR’s enterprise-wide technology services organization. Computing and Communications is headed by Associate Vice Chancellor and CIO Charles Rowley, who has broad responsibility for the university’s information technology and communication services strategic planning, infrastructures, and day-to-day operations.

Campus information technology security initiatives are developed, coordinated, and implemented via the following individuals:

- **Associate Vice Chancellor and CIO, Campus Information Services – Charles Rowley**
  
  The Associate Vice Chancellor (AVC) and Chief Information Officer (CIO) has primary responsibility for strategic planning and operational support related to UCR's campus-wide and system-wide information systems and voice and data networks. The AVC/CIO reports to the Executive Vice Chancellor & Provost and works closely with senior campus administrators, faculty, and staff.

  The CIO is responsible for the development and deployment of campus-wide and system-wide technology policies, procedures, and technical best practices and guidelines, including those specifically concerned with information technology security, privacy, and confidentiality.

- **Director of Computing Infrastructure and Security – Russ Harvey**
  
  The Director of Computing Infrastructure & Security (CI&S) reports to the Associate Vice Chancellor and CIO (AVC/CIO), serves as the campus Information Security Officer (ISO), and provides leadership relating to the development of long term infrastructure and security objectives as well as concomitant operational plans for acting on the long term vision.

  The CI&S Director coordinates policy development, system-wide policy implementation, campus wide-policy dissemination, and the promulgation of technology and security best practices and approaches.

- **Chief Financial and Administrative Officer (CFAO) – Shelley Gupta**
  
  The CFAO reports to the Associate Vice Chancellor and CIO (AVC/CIO) and supports the ISO and CIO relating to campus-wide technology policy implementations and information dissemination.

- **Director of Technology – Bob Grant**
  
  The Director of Technology reports to the Associate Vice Chancellor and CIO (AVC/CIO) and is responsible for providing the highest level of technical planning, consulting, and visioning support relating to the implementation and operation of systems, applications and campus computing (servers, networks, security, etc.) infrastructure. The Director of Technology provides support to the ISO in all matters relating to information technology security.
• **Director of Computing Support Services – Larry McGrath**

The Director of Computing Support Services reports to the Associate Vice Chancellor and CIO (AVC/CIO) and is responsible for campus-wide desktop computing support, instructional technology services, classroom technology support, and other faculty instructional and research technology support initiatives. The Director of Computing Support Services is a key point of contact for department and unit security efforts, especially relating to desktop security efforts.

**Operationalized Security Implementation Documents.**

UCR has operationalized its security plan via the creation and ongoing review / updating of six Security Implementation documents. An overview of these documents is as follows:

• **Risk Assessment, Disaster Recovery, and Organizational Structures.** This document provides an overview of C&C’s Risk Assessment approach, the planning assumptions behind its disaster recovery plan, and include other details concerning C&C’s security staff and organizational structure.

• **Identity Management Systems.** This document provides an overview of C&C’s Identity Management practices, processes, and technologies as well as UCR’s Identity Management stakeholders and their various roles and responsibilities.

• **Servers and Operating Systems Security.** This document defines the various measures adopted to ensure server and operating system security (e.g. firewalls, log management, patching, access controls, etc.) as well the approaches that are used to document and record compliance with these measures.

• **Database Security.** This document defines the various measures adopted to ensure database security (e.g. change control, access controls, etc.) as well the approaches that are used to document and record compliance with these measures.

• **Physical Security.** This document defines the various measures adopted to ensure appropriate physical security as well the approaches that are used to document and record compliance with these measures.

• **Network Security.** This document defines the various measures adopted to ensure network security (e.g. (e.g. ACLs, firewalls, change control, log management, patching, etc.) as well the approaches that are used to document and record compliance with these measures.

• **Application Development – Change Control & Vulnerability Scanning.** This document defines C&C’s approach to application develop (including request intake, testing, user approvals, migration management, change control, source code management, and vulnerability scanning) as well the approaches that are used to document and record compliance with these measures.
Campus organization and departments must utilize appropriate safeguards to protect sensitive and/or protected information resources based upon the sensitivity of data in question, legal requirements, and risks to the university. These safeguards are expressed within a technical plan that addresses (at a minimum) the following:

- **Administrative Workforce Controls**
  - Workforce and authorization management
  - Critical positions
  - Violations

- **Operational and Technical Controls**
  - Identity and access management
  - Access controls
    - Passwords and other authentication credentials
    - Session protection
    - Privileged access

- **Systems and Application Security**
  - Systems personnel
  - Backup and retention
  - System protection
  - Patch management
  - Systems and application software development

- **Network Security**
  - Change management
  - Audit logs
  - Encryption

- **Physical and Environmental Controls**
  - Risk mitigation measure
  - Physical access controls
  - Tracking reassignment or movement of devices and stock inventories
  - Disposition of equipment
  - Portable devices and media

C&C has prepared an overview of IS3 requirements in this regard and it is available for UCR departments and organizations at the following web address: ucrsecurity.ucr.edu

*Security, Privacy, and Confidentiality Communications and Awareness Program.*

**Proactive Communications**

- **October Cyber Security Awareness.** As part of the national Cyber Security Awareness effort, C&C engages in a variety of communications in October of each year highlighting security
issues and best practices (e.g. portal alerts, communications with management, e-mails to campus, etc.).

- **January / February Communications.** As part of its twice-annual communications strategy, C&C updates the campus on various security issues and best practices after the first of the year (e.g. portal alerts, communications with management, e-mails to campus, etc.).

- **Updates to Technical Advisory Group.** UCR’s distributed information technology leadership group (TAG) meetings four times a year. During these meetings, security issues and best practices are frequent topics, including IS3 and other policy / operational issues.

- **Annual Protected Personal Information (PPI) / Sensitive Data Review – All Information Technology Organizations.** UCR engages in an annual, detailed review of campus systems that contain protected and/or sensitive information. Details concerning this process are presented below.

- **Security Presentations to Campus Management.** UCR engages in annual updates to campus management (e.g. Dean’s Council, Operations Council, etc.) concerning security efforts and the overall status UCR’s information security environment.

**Online Electronic Resources**

- **Security Web Site.** UCR provides the campus with a comprehensive security web site at the following web address: cnc.ucr.edu/security

- **Security Tutorials.** UCR provides the campus three security tutorials and promotes the use of these tutorials via the portal and other electronic communications. The tutorials are as follows:
  - Phishing Tutorial – http://cnc.ucr.edu/phishing_flv.html

**Certifications**

- **Annual Online Certifications.** UCR is utilizing online certifications as a method of enhancing campus information technology security efforts. Two of the most important certifications are as follows:

  - **Annual Security Certifications via Portal.** UCR requires annual user certifications PRIOR to permitting users to log into the portal and access campus information systems. These certifications are as follows (links to cnc.ucr.edu/security are included in the certifications):

    “R’Space users must be aware of the following security precautions. Please thoroughly read each precaution carefully. You may then click on the checkbox to certify that you have read, understand, and agree to comply with the following 5 security precautions:

    1. Choose a strong password.
2. Do not share your password.
3. Do not store your password in your Web browser.
4. Protect your password against theft.
5. Sign out of R’Space and quit your Web Browser when your session is finished.”

**Quarterly and Annual Systems Access Administrator (SAA) Certifications.** Authorization to utilize campus systems is granted directly by departmental administrators (knows as SAAs) using the Enterprise Access Control System. SAAs are required to make annual and quarterly certifications as follows:

**Quarterly Certification:**

“I certify for this Accountability Structure that user access privileges are appropriate and a quarterly review has been conducted to ensure:

1. Access is appropriate for each employee(s) current job responsibilities
2. Access is appropriate for current department operations
3. Access provides for adequate separation of duties within the department
4. Users received the required training and appropriate guidance
5. Access and/or accountability structure updates have been initiated as appropriate via EACS
6. User access is coordinated with the departmental financial manager or department head (if different from the SAA)”

**Annual Certification:**

“I certify that I understand my responsibilities as a Systems Access Administrator (SAA) to ensure the integrity and effectiveness of departmental operations by:

1. Coordinating user access privileges with my departmental financial manager or department head (if different from SAA)
2. At least annually reviewing user access and application routing for my Accountability Structure(s) with the unit departmental financial manager (if different from SAA) for appropriateness and consistency with campus guidance
3. Access is appropriate for each employee(s) current job responsibilities
4. Access is appropriate for current department operations
5. Access provides for adequate separation of duties within the department
6. Users received the required training and appropriate guidance
7. Access, routing and/or accountability structure updates have been initiated as appropriate via EACS.”

**Security Breach Prevention and Incident Reporting Program.**
C&C conducts (and has conducted since 2004) annual reviews of campus systems containing personal protected and/or sensitive data. The campus also has a formal process in place to address campus security breaches; more information about incident reporting and campus efforts in this regard can be found at sb1386.ucr.edu.

An overview of UCR’s Security Breach Prevention and Incident Reporting Program is as follows:

- C&C CFAO issues the Annual Call for Reporting of Systems Containing PPI / Sensitive Data.
- UCR’s Organizational Units provide C&C with Reports / Inventories.
- C&C Reviews these Reports.
- C&C, as required, Provide Remediation Suggestions.
- C&C Reviews Responses to these Remediation Suggestions.
- C&C Presents Findings to UC Riverside Executive Management (annually).

Results of the annual process are available from C&C’s CFAO.