

<b>ANR Administrative Handbook Section 203 INFORMATION TECHNOLOGY AND COMMUNICATIONS</b>	Date: 03/23/09 Supersedes: 06/01/06
RESPONSIBLE DEPARTMENT: <a href="#">ANR Communication Services</a>	
FOR ASSISTANCE CONTACT: <ul style="list-style-type: none"><li>➤ Claudia Myers, Information Security Officer, Communication Services and Information Technology 530-754-3909, <a href="mailto:cmyers@ucdavis.edu">cmyers@ucdavis.edu</a></li><li>➤ Robert Sams, Director, Communication Services and Information Technology 530-754-3900, <a href="mailto:rwsams@ucdavis.edu">rwsams@ucdavis.edu</a></li><li>➤ David Underwood, Principal IT Specialist, Office of the Controller and Business Services 510-987-0072 or <a href="mailto:david.underwood@ucop.edu">david.underwood@ucop.edu</a> (for Sections III and IV below)</li></ul>	

I.	INTRODUCTION
II.	ELECTRONIC COMMUNICATIONS AND INFORMATION SECURITY
III.	GUIDELINES FOR THE PURCHASE AND USE OF CELLULAR PHONES AND OTHER PORTABLE ELECTRONIC RESOURCES
IV.	AUTHORIZATION TO USE UC PROPERTY IN AN OFF-CAMPUS LOCATION

## I. INTRODUCTION

It is the policy of the University of California (UC) to encourage the use of electronic communications to share information and knowledge in support of UC's mission of education, research and public service, and to conduct UC business.

## II. ELECTRONIC COMMUNICATIONS AND INFORMATION SECURITY

### A. Introduction

1. This section of the Agriculture and Natural Resources (ANR) Administrative Handbook highlights the key requirements of University of California (UC) policies on electronic communications and information security, and provides guidance for their application in the Agriculture and Natural Resources (ANR) environment.

2. Possibly the most important of UC's electronic communications and information security policies is [Electronic Information Security, IS-3](#). Other security policies with particular relevance for ANR include [Inventory, Classification, and Release of University Electronic Information IS-2](#), [Identity and Access Management, IS-11](#), [Continuity Planning and Disaster Recovery, IS-12](#), and the [Electronic Communications Policy](#).
3. The ANR environment encompasses a range of settings, all impacting on electronic security and the policies to be followed. There are ANR managed networks in UC Cooperative Extension (UCCE) and Research and Extension Center (REC) offices, but there are also UCCE offices whose networks are managed by their county governments. In addition, ANR has offices on UC campuses, some of whose networks are managed by IT staff in campus departments or colleges, but some of which are not.
4. In general, ANR units must comply both with the above-noted UC policies, as well as the information technology (IT) policies of the organization providing network services to the office workstations and servers. This is true whether the agency providing those services is a UC campus, the local county government, or other entity.

## B. THE IMPORTANCE OF INFORMATION SECURITY

1. ANR encourages the use of its electronic communications network in support of education, research, and public service. However, this resource is limited and vulnerable to attack, and must be protected against network security threats. Attacks can come to individual computers randomly as viruses, Trojans, or worms, and may include random and/or targeted attempts to mine data. They may take the form of spyware, or be a more deliberate attempt to gain access to databases or sensitive information.
2. A security breach by a malicious virus, Trojan, or worm can require significant resources (both human and monetary) to remedy. It takes time and expertise to clean an infected computer and valuable data may be lost unavoidably in the process. A security breach of sensitive data can have legal ramifications, cause problems for our clientele and ANR, and hurt ANR's credibility.

3. State law and UC policy require compliance with various levels of computer and network security.
4. ANR requires compliance with minimum security standards to help protect not only the individual device, but other devices connected to the electronic communications network. Such security standards are also intended to prevent exploitation of ANR resources by unauthorized individuals.

C. RESPONSIBILITIES:

1. ANR Employees
  - a. Individuals who access and use ANR electronic information resources must:
    - i. Become knowledgeable about relevant security requirements and guidelines.
    - ii. Protect the resources under their control, such as access passwords, computers, and the data they download.
    - iii. Use devices that comply with the minimum standards set forth in this policy.
  - b. ANR employees using county government networks or computers are subject to county IT and other policies as well as applicable UC/ANR policies. These policies may differ.
  - c. County employees using ANR networks or computers are subject to UC/ANR electronic information security policies as well as applicable county policies. These policies may differ.
2. System Administrators
  - a. System administrators of ANR network resources (server administrators and operators of web services such as those at Communication Services, Kearney Agricultural Center, and at UCOP) must:

- i. Ensure compliance of servers and systems with minimum standards for security as set forth in the Minimum Standards section below.
    - ii. Ensure compliance with additional areas including identity and access management, and application systems management.
3. ANR Chief Information Officer and Director, ANR Communication Services
  - a. The ANR Chief Information Officer and Director, ANR Communication Services must:
    - i. Provide direction, planning, and guidance on information security.
    - ii. Develop and review ANR information security policy and procedures.
    - iii. Work with the ANR community to protect ANR computers and network infrastructure from electronic attack.
    - iv. Serve as Electronic Communications Policy Coordinator (ECP).
4. ANR Information Security Officer
  - a. The ANR Information Security Officer must:
    - i. Conduct a periodic inventory to assess where critical systems and data exist in ANR.
    - ii. Ensure that training on UC policies (especially critical systems and data) is available for ANR system administrators and programmers.
    - iii. Make electronic information security training available annually for regular desktop users.
    - iv. Review and revise minimum security standards for networked devices as outlined in this ANR *Administrative Handbook* section.

## D. MINIMUM STANDARDS

1. The following minimum standards are required for all ANR devices (desktop and laptop computers for the most part) connected to a network, or all devices connected to an ANR or UC network. Servers must also meet these minimum standards but additional requirements also apply as outlined below. County governments will have similar or even stricter minimum standards. All UC campuses have very similar minimum standards. If desired, individual ANR units may develop and implement security standards that are more rigorous than these.
2. Computing applications hosting critical and/or sensitive UC information are subject to more stringent security standards which are addressed below.
3. ANR reserves the right to deny access to its electronic communications network by devices that do not meet its standards for security.
4. Software Patch Updates
  - a. ANR networked devices must run operating systems for which security patches are made available.
  - b. Such security patches must be current and installed in a timely fashion. However, exceptions may be made for operating system patches that compromise the usability of critical applications.
  - c. As much as possible, ANR networked devices must use only applications for which security patches are made available.
5. Anti-virus Software and Anti-Spyware Software

Anti-virus software must be running and up-to-date on every level of device. Anti-spyware software must also be installed when readily available.
6. Host-based Firewall Software

Host-based firewall software must be running and configured.

7. Accounts and Passwords

- a. Computers and other similar devices must have user accounts and passwords assigned to them. Passwords must meet [Minimum Password Complexity Standards](#).
- b. All default passwords for access to network-accessible devices must be modified.
- c. Where possible and appropriate:
  - i. Devices should be configured with separate accounts for privileged and unprivileged access (administrator versus limited accounts).
  - ii. Users should authenticate with an unprivileged account (limited) rather than a privileged account (administrator).
  - iii. Privileged (administrator) access should only be used for as long as necessary to complete the task which requires additional privileges.
  - iv. Passwords for privileged and limited accounts must not be the same.

8. Physical Security

Unauthorized physical access to an unattended device can result in harmful or fraudulent modification of data, fraudulent email use, or any number of other potentially dangerous situations. Accordingly, where possible and appropriate, devices must be configured to "lock" and require a user to re-authenticate if left unattended for more than twenty (20) minutes. For most computers this means setting a user name and password, setting the screen saver to wait for no more than twenty (20) minutes, and setting it to display the welcome screen when it resumes. In other words, computers must be configured to require a login upon booting or restart and before exiting "sleep" or screen-saver modes.

9. Additional Minimum Standards for Servers

- a. Unencrypted authentication is prohibited.
  - i. Unencrypted device authentication mechanisms are only as secure as the network upon which they are used. Traffic across the network may be surreptitiously monitored, rendering these authentication mechanisms vulnerable to compromise. Therefore, all ANR servers must use only encrypted authentication mechanisms.
  - ii. In particular, historically insecure services such as Telnet, FTP, SNMP, POP, and IMAP must be replaced by their encrypted equivalents.
  - iii. Traffic for one-time password authentication systems is exempted from this encryption requirement, because its exposure does not compromise the integrity of the underlying authentication system. Users must change any pre-assigned passwords after initial access to the account.

- b. Unauthenticated email relays are prohibited.

ANR devices must not provide an active SMTP service that allows unauthorized third parties to relay email messages, i.e., to process an e-mail message for which neither the sender nor the recipient is a local user. Before transmitting email to a non-local address, the sender must authenticate with the SMTP service.

- c. Unauthenticated proxy services are prohibited.
  - i. Although properly configured unauthenticated proxy servers may be used for valid purposes, such services commonly exist only as a result of inappropriate device configuration. Unauthenticated proxy servers may enable an attacker to execute malicious programs on the server in the context of an anonymous user account.

- ii. In particular, software program default settings in which proxy servers are automatically enabled must be identified by the system administrator and re-configured to prevent unauthenticated proxy services.

d. Unnecessary Services

If a service is not necessary for the intended purpose or operation of the server, that service shall not be running.

E. IDENTITY AND ACCESS MANAGEMENT

Administrators of ANR central IT resources or of critical or sensitive systems must implement a process to identify those who are authorized to access the information, and to authenticate them when they do so. Detailed information can be found in [Identity and Access Management, IS-11](#). This topic is to be included in the trainings conducted by ANR for system administrators.

F. APPLICATIONS SYSTEMS MANAGEMENT

1. Applications that are developed by ANR programmers or by a vendor for ANR, and that are part of essential ANR functions or relate to critical or sensitive systems or data, must conform to relevant sections of [Systems Development and Maintenance Standards, IS-10](#). While much of IS-10 may not apply, programmers and system administrators need to be aware of it and take into account relevant sections regarding the manner in which sensitive data is collected, stored, shared and managed, as well as who may access it.
2. This topic is to be included in the trainings conducted by ANR for system administrators.

G. RISK ASSESSMENT AND SECURITY PLAN

1. Every one (1) to two (2) years the ISO will conduct an assessment of computing resources in ANR to identify and locate critical or sensitive systems and data.
2. Appropriate risk mitigation measures must be identified for critical or sensitive systems and data. Basic measures include encryption; redundant systems; off-site backups; and locked,

controlled server rooms. These are important for central ANR IT resources. Every one (1) to two (2) years ANR will conduct training for system administrators with critical or sensitive systems or stored data.

#### H. INCIDENT RESPONSE AND NOTIFICATION

1. Incident response refers to establishing and implementing procedures to deal with known or suspected security breaches. By law a security breach of personal information requires notification of those affected.
2. All campuses and UCOP have incident response and notification processes. Most ANR central IT systems can make use of the processes in place on their respective campuses. However, some ANR units with critical resources are not covered by a campus.
3. If a suspected security breach of critical or sensitive systems or data occurs, the system administrator must take the system offline. They must then report the suspected security breach to the ANR Chief Information Officer (CIO) and document the incident. The ANR CIO will designate a team to investigate the suspected breach, or will activate the appropriate campus incident and response process if not already notified, to determine if a breach did in fact occur and to implement remediation strategies. The CIO will determine the need for notification based on the systemwide notification procedures as outlined in UC's [Electronic Information Security, IS-3](#) bulletin.

#### III. GUIDELINES FOR THE PURCHASE AND USE OF CELLULAR PHONES AND OTHER PORTABLE ELECTRONIC RESOURCES

- A. UC Business and Finance Bulletin [G-46](#), *Guidelines for the Purchase and Use of Cellular Phones and Other Portable Electronic Resources* provides guidance as to the appropriate circumstances for UC purchase of and service support for cellular phones, personal digital assistants (PDAs), pagers, and other electronic communication devices for use by employees outside of the workplace. It also provides guidance on the use of electronic communications resources and related equipment and software purchased for an employee's home use, including personal computers, laptop computers, phone lines, facsimile (fax) machines, and connection and access to Internet services and e-mail. In addition, the [G-46](#) establishes procedures for documenting the use of UC-

provided cellular phones and reimbursement to UC of any non-incidentual personal use of such devices.

- B. Prior to receipt of equipment an employee must sign a usage agreement acknowledging that use of the equipment will be limited to UC business and only incidental personal use. This form, *Employee Agreement Concerning the Use of Electronic Communications Resources* is provided as Appendix A to [G-46](#) (page 8).

#### IV. AUTHORIZATION TO USE UC PROPERTY IN AN OFF-CAMPUS LOCATION

Use of UC's [Authorization To Use University Property in an Off-Campus Location form](#) is required to record property loans between UC departments and private individuals, agencies, or other campuses; whereby said property is loaned by UC for purposes of instruction, demonstration, experimentation, administrative support, or research; and is used on premises other than those of UC.

**ADDITIONAL RESOURCES:**

- [Implementing Guidelines for the Minimum Standards for Security of Berkeley Campus Networked Devices](#)
- [Minimum Standards for Connecting Microsoft Windows-based Desktop Computers and Servers to the UCOP Network](#)
- [Minimum Standards for Connecting Apple Macintosh Desktop and Laptop Computers to the UCOP Network](#)
- University of California [Electronic Communications Policy](#)
- University of California Information Systems Bulletin IS-2, [Inventory, Classification, and Release of University Electronic Information](#)
- University of California Information Systems Bulletin IS-3, [Electronic Information Security](#)
- Business and Finance Bulletin IS-10, [Systems Development and Maintenance Standards](#)
- Business and Finance Bulletin IS-11, [Identity and Access Management](#)
- Business and Finance Bulletin IS-12, [Continuity Planning and Disaster Recovery](#)
- [Glossary of Terms in Selected Business and Finance Bulletins in the Information Systems \(IS\) Series](#)
- [Employee Agreement Concerning the Use of Electronic Communications Resources](#)  
(Appendix A, page 8 of 8)