University of California, Davis
Department of Nutrition

New Staff
Computer & Network Information Packet

This packet contains the following documents:

- ☐ Attestation of Notification and Comprehension of UC Davis Acceptable Use Policy Form
- ☐ UC Davis Nutrition Department Frequently Asked Questions about Computer/Network Policies & Procedures
- ☐ UC Davis Nutrition Department Computer Support Guidelines

Please contact Jennifer Ruhe, 3113 Meyer Hall, 752-4650, jruhe@ucdavis.edu with any questions you have about computer and network resources in the Nutrition Department.

This page intentionally left blank

University of California, Davis
Department of Nutrition

Attestation of Notification and Comprehension of UC Davis Acceptable Use Policy

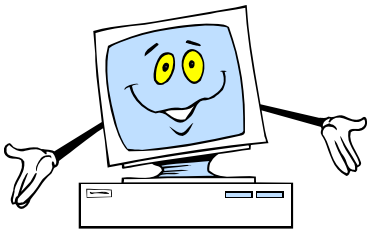
_____ _____
Employee Name **Employee ID Number**

_____ _____
Employee Email Address **Supervisor's Name**

_____ I have read and understood the **UC Davis Acceptable Use Policy (PPM Section 310-23 Exhibit A)**

_____ _____
Signature **Date**

This page intentionally left blank



FREQUENTLY ASKED QUESTIONS ABOUT UC DAVIS NUTRITION DEPARTMENT COMPUTER & NETWORK POLICIES & PROCEDURES

QUESTION: I am new to the department and need a UC Davis computing account. How do I get one? All faculty, students, and staff are eligible for a UCD Computing account, which can be used for e-mail, the MyUCDavis web portal, and access to campus computer labs. If you have access to a computer connected to the Internet, go to http://computingaccounts.ucdavis.edu/ and click on "Get your UC Davis computing account." If you do not have access to a computer connected to the Internet, then you can go in person to IT Express in Shields Library room 182 – if you are a new staff member, be sure to check with department personnel staff to make sure that your information has been entered into the campus payroll system. You may want to call IT Express before walking over to check their hours and find out what you need to bring with you (such as photo ID card, a printout of your personnel IDOC form, and/or your campus student/staff ID number). They can be reached at 530-754-HELP.

QUESTION: How do I get an account to log onto a Nutrition Department workstation in my lab or office? Step 1: Sign the attestation form in this packet and return it to your account manager in the main admin office in 3135 Meyer. Step 2: Have your supervisor submit a System Access Request Form (http://nutaccounts.ucdavis.edu/) to request that your account be set up. Once your attestation form is on file with your account manager and your supervisor has submitted a System Access Request form requesting your account, department I.T. staff will create your account and contact your supervisor when it is ready for you to pickup from the I.T. office in 3113 Meyer (be sure to bring photo I.D. with you when you come to the office). If you have any questions about the above procedure, please see Jennifer Ruhe in 3113 Meyer.

QUESTION: I have a laptop that I want to connect to the Internet while in Meyer Hall. How do I do that? The department has Moobilenet (the campus wireless network) installed in most of Meyer Hall so if you have a wireless network card in your laptop, this is easy! To find out more about Moobilenet, please visit their web site at http://wireless.ucdavis.edu/ or see Jennifer or Alex in 3113 Meyer.

QUESTION: Does the Nutrition Department have A/V equipment that can be checked out by department employees? The department has one portable data projector, two PC laptops, one digital camera, and one video camera that are available for checkout by Nutrition Department employees. Note that both the Pran Vohra Room and the Hurley Room have data projectors available in the room. Contact the front desk of the main office in 3135 Meyer, 752-4645 for information on how to reserve the equipment.

QUESTION: How can I set up a Google Calendar account so that I can access departmental calendars and share my calendar with others in the department? Please make an appointment with Alex Zingorenko (azingorenko@ucdavis.edu, 752-4650) to set up your Google Calendar account.

QUESTION: Does the department have a computer lab? Yes! We have a computer lab open to all department employees including faculty, staff, and those graduate students whose major professor is a Nutrition Department faculty member. The computer lab is located in 3249 Meyer Hall and keys can be checked out at the front desk in 3135 Meyer Hall. There are 10 computers in the lab and available software includes: MS Office Professional 2007, Adobe Acrobat Professional 9, EndNote, ImageJ, Chromas, Illustrator, Photoshop, ChemDraw, Food Processor SQL, Jmp, SAS, SPSS, Minitab, SigmaPlot, SigmaScan,and SigmaStat. The lab is also equipped with two scanners. The Microtek scanner has standard scanner features as well as a transparency tray that can be used to scan a tray of slides. The HP scanner has a document feeder that can be used to scan stacks of paper (up to 40 pages at a time). Instructions on how to use the scanners to do things like scan slides, scan documents to PDF, or scan images to .jpg are posted on the wall in front of them.

QUESTION: I have a personally owned laptop that I want to use to print to a network printer in Meyer Hall. How do I do that?
For security reasons the department does not allow personally owned laptops to access our private wired network where our network printers reside. Additionally, because of a number of security issues and campus policies, access to network printers is not allowed from systems connected to the campus wireless network (Moobilenet).

QUESTION: I have a problem with a department owned system. How can I get help? Users should submit all non-mission critical technical support requests/questions via our online form at: http://techtracker.ucdavis.edu/ or fill out a paper form and leave it in the computer support mailbox (forms are available by the computer support mailbox by the rest of the mailboxes near the copy machine). The trouble ticket system allows department technical support staff to properly prioritize requests for support and it is the best way to ensure that your problem is resolved in a timely manner (if it's in the queue in the techtracker database, it will not fall through the cracks). If you have a mission critical problem relating to work that must be completed that day and you have no other options for completing the task, please contact Jennifer or Alex directly in 3113 Meyer Hall, 752-4650. Note that technical support will be given only for hardware/software issues relevant to the completion of work for the Nutrition Department or its affiliated units at the University of California, Davis.

QUESTION: I have a problem with my personally owned computer. Can you help me? Unfortunately, for liability reasons and limits on department resources we do not provide any support for personally owned systems.

QUESTION: I want advice on ordering a computer with my own money. Can you help me with that? Unfortunately, for liability reasons we do not give advice or recommendations on personal purchases. The campus has a web site that gives general recommendations for configurations for computers for students on campus (http://computerownership.ucdavis.edu/) and you may want to consult this site before making a purchase.

QUESTION: What software is available for my personally owned computer?
The campus has some free software available for campus members to install on personally owned computers such as Endnote and Sophos Antivirus. This software can be found on the MyUCDavis web site (https://my.ucdavis.edu) under the menu item "My Office" at the top and then "Software." If you are a UC Davis Nutrition Department employee, you may purchase one license for MS Office for your personally owned computer via the Microsoft Home Use Program as part of our departmental Microsoft license agreement for $9.95. Please email jruhe@ucdavis.edu if you would like information on how to purchase MS Office as part of the Microsoft Home Use Program. Software purchased under this program may be used for personal, non-commercial purposes and must be removed when your affiliation with the university ends. Campus members may also purchase discounted Microsoft Windows and Office software from the following web site (campus members are allowed to purchase one copy of each available application): http://tinyurl.com/onthehub . Software purchased via this site costs a bit more than the above Microsoft Home Use Program, but there are more software titles available and in most cases the software does not have to be removed when you leave the university.

QUESTION: I have a department owned computer at home (laptop or desktop). Can my family members/friends use it also?
If you want to receive technical support for your department owned system, then no one except for Nutrition Department employees who have been assigned the computer in question should ever access your off site department owned system. If your family members or friends need access to a computer, you may wish to consider obtaining a personally owned system for such use.

QUESTION: I have some software that I bought myself, that someone gave me a copy of, or that I downloaded from the Internet. Can I install it on my department owned computer? In order to comply with software licensing laws and to efficiently report for campus audits, the department must manage all software license orders and installations. Additionally, we must make sure that software applications will not cause any security issues, conflicts or problems prior to purchasing and installation. Please contact Jennifer Ruhe for any questions about ordering and installing software on department owned systems.

QUESTION: I need to order a computer with department funds that I will expect to receive support for. Can I order whatever I want and set it up myself when it gets here? In order to receive department support, department technical support staff must approve the system specifications prior to ordering. For most systems (except for some specialized systems for lab equipment), department technical support staff do the quotes and handle the ordering and setup of the system for you. Contact Jennifer Ruhe, jruhe@ucdavis.edu, 3113 Meyer to coordinate purchasing a computer.

QUESTION: A visitor, friend or family member is here with me today at work. Can they use a department owned computer here?
For security reasons and to comply with campus policies this is explicitly prohibited. No one except for Nutrition Department employees should access department owned computers connected to our internal network. It should also be noted that campus policy is that users should never share their username/password with anyone (including using them to log someone onto a computer for them to use). Note that if you have a personally owned laptop with a wireless card and a campus computing account, you can set up a wireless guest account (more info is available at http://wireless.ucdavis.edu/)

QUESTION: I purchased a license for some software through the department with department funds. Can I get the media from you and install it on more than one computer in my lab, office, or at home? Most likely you cannot. In order to comply with software licensing laws and to be able to efficiently report for campus audits, the department manages all software orders and installations. We can check the license agreement for your application to see if it allows for installation on more than one computer and take care of all installations/license purchases for you.

QUESTION: Why can't I be an administrator on my computer so that I can install software and make system configuration changes myself? Our systems are centrally managed to protect the security and stability of all systems connected to our network and to limit the amount of resources used to resolve security issues/system failures resulting from inappropriate or insecure installations and configuration changes. If you need software installed, please contact department I.T. staff and they will check that the software is properly licensed, is compatible with our systems, and does not open up any security risks for our network (and then install it on the system in question). If you need a system configuration change or a computer moved, contact department I.T. staff for assistance and they will take care of that for you.

QUESTION: May I store personal information such as someone's name along with their social security number, California ID number, financial account information, or health insurance information on my work, home, or laptop computer? Unless an exception has been granted and user training and system configuration including encryption are in place as is required by campus policy, Nutrition department members should not store any "personal information" on any systems ("personal information" is strictly defined in this context as personal name along with **Social Security number**, **California driver identification number**, **financial account information, or health insurance information**) and "systems" include both university and personally owned desktop computers & laptops, server shares, PDA's, as well as any electronic storage media such as CD's, DVD's, Portable hard drives, disks, or USB Flash drives).

If you think you have a business need to store personal information (as defined above) on any systems, or if you need assistance in removing personal information from a system, please contact Jennifer Ruhe, jruhe@ucdavis.edu, 752-4650, 3113 Meyer.

QUESTION: I have a piece of university owned computer equipment that I want to get rid of. What is the proper procedure for this?
Contact Alex Zingorenko, azingorenko@ucdavis.edu for assistance in salvaging old computers/printers and he will coordinate this for you with Bargain Barn (in order to make sure that we comply with campus policies and procedures for equipment management users should not attempt to transfer, donate, or dispose of any university owned computers or printers on their own). Note that in order to comply with campus policies and state/federal laws about disposal of media possibly containing confidential data, we remove all hard drives from computers before they are salvaged or sent to Bargain Barn for resale and use special tools to wipe all data from the drives before they are reused or salvaged.

QUESTION: I want to print a poster. What printing resources does the department have available to me? The Nutrition Department has an HP Designjet 800 poster printer available to all department employees and those graduate students whose major professor is a Nutrition Department Faculty member. Unfortunately, we do not have the resources to provide printing to all the students in all the various graduate groups our faculty belong to, such as the Graduate Group in Nutritional Biology – just the students housed in our department. More information on the poster printer including costs, poster templates, and detailed instructions is available online: http://nutrition.ucdavis.edu/poster/

QUESTION: I want to move a university owned computer or peripheral off site (such as to my home or another building on or off campus) to use for University work. What is the proper procedure for doing this? Please contact Jennifer Ruhe or Alex Zingorenko in 3113 Meyer to make arrangements to move computer equipment (they will make sure that the proper approvals are obtained/forms are signed before the equipment is moved).

QUESTION: What are some of the basic computer/network practices I should follow when using a department computer?
Never share your campus or departmental computing account information with anyone (this includes logging onto a computer for someone else to use). Do not share your password with anyone, including your supervisor, I.T. staff, or visitors. In general, when a networked computer is left unattended the user should either log off, shut the system down, or 'lock' the computer by pressing Ctrl-Alt-Delete and selecting "Lock Computer" (unauthorized physical access to an unattended computing device can result in harmful or fraudulent modification of data, fraudulent email use, or any number of other potentially dangerous situations). So that we can ensure that all software is properly licensed, fully compatible with our systems, and does not create any security vulnerabilities, users should not attempt to install any software on their systems. If you need software installed, submit a request to department technical support and we will take care of making sure it is compatible with your system, order the proper licenses, and install it for you.

UC Davis Nutrition Department
Computing-Use Policy

Supporting a large number of computers with varying types of software and user modifications can be a costly task in terms of IT staff time and resources. To ensure the integrity of the department's data, network security, and staff productivity, it is necessary to enact a set of computer-use guidelines. The policy will apply to any computer supported by the Nutrition Department IT Support office and/or any computer connected to the departmental subnet. Below are the guidelines that must be followed in order to receive support from Nutrition Department IT.

1) The system in question must be owned by the University of California. For liability reasons and limits of time, we are unable to provide support for personally owned systems.

2) Technical support will be given for hardware/software issues relevant to the completion of work for the University of California. For liability reasons and limits of time, we are unable to provide support for issues not related to official University business.

3) Users must follow the guidelines given below:

> **a) Provide reasonable access to your machine.** If the system is on campus and it is appropriate, you may need to provide a key to the office in which the system resides for after-hours access. If the system is located off-site, you will need to bring the system to the Nutrition Department for service.
>
> **b) Consult Nutrition Department technical support personnel before purchasing any computers, peripherals, or software that you expect to receive technical support for.** Please note that you may need help in the future that you do not recognize at present.

c) Users should not attempt to install unauthorized software or hardware on departmental computers. Unauthorized software or hardware is defined as any software or hardware not explicitly approved for installation by your direct supervisor and Nutrition Department technical support personnel. Please note that this also includes, but is not limited to, software that is not properly licensed, and programs known as malware, computer viruses, Trojan Horses, and worms.

Section 310-23 **Electronic Communications--Allowable Use**	**Date:** 5/9/06 **Supersedes:** Section 310-16, 10/5/04 **Responsible Department:** Information and Educational Technology

I. Purpose

This section provides UC Davis (UCD) implementing procedures for the allowable use of University Electronic Communications (EC). The UC and UCD EC policies apply to all EC resources owned by the University; provided by the University through contracts and other agreements; users and uses of University EC resources; and all University EC records in the possession of University employees or other users of University EC resources. See also Section 310-24, Electronic Communications—Privacy and Access to Records.

II. Definitions

The UC EC policy, Appendix A, defines terms used in this policy. Some terms are further defined at UCD as follows:

A. Department head—the head of a teaching, research, administrative, or other organizational unit as designated by the Chancellor. For students, "department head" shall be the Director of Student Judicial Affairs.

B. Record (EC record)—EC records residing on University-owned or –controlled EC resources are University records for the purposes of this policy and subject to disclosure as required by the California Public Records Act.

C. Restricted personal information—unencrypted data in which the individual's first and last name appears in combination with the Social Security number, driver's license number, California identification card number, or credit card or account number together with the security code, access code, or password that would permit access to the account.

D. Security Coordinator—the Electronic Information Security Guidelines Coordinator, as designated by the Chancellor pursuant to UC Business and Finance Bulletin IS-3.

E. System administrator—department designee who has the physical or logical control over EC resources.

III. Policy

The use of electronic communications resources is limited by restrictions that apply to all University property and by constraints necessary for the reliable operation of electronic communications systems and services. The University reserves the right to deny use of its electronic communications services when necessary to satisfy these restrictions and constraints.

IV. Allowable Users

A. University users may be granted access to University EC resources and services for purposes in accordance with allowable use. University users are defined as follows:

1. UCD students, staff, academic appointees, and emeriti. Department heads may grant access in support of teaching, research, public service, and patient care mission of the University, and the administrative functions that support that mission.

2. Other individuals who are affiliated with the University, including those in program, contract, or license relationships. Department heads may grant access for the term of the affiliation, when such access supports the mission of the University and is not in competition with commercial providers.

   These individuals must be sponsored by a UCD department and must complete a Temporary Affiliate form (http://email.ucdavis.edu).

   a. Students, academic appointees, and staff at other UC campuses.

   b. University Extension students enrolled in courses requiring access.

   c. Retirees.

d. Volunteers.

e. Contractors, independent consultants, and certain agents of the University other than employees may be given access for the sole purpose of conducting their business on behalf of the University, unless agreed otherwise in writing.

B. Public users. Individuals and organizations that are not University users may only access University EC resources under programs sponsored by the University, as authorized by the Vice Provost—Information & Educational Technology or other administrator designated by the Chancellor for the purpose of public access in accordance with allowable use.

C. Separation from the University

1. Access to records. If a separating individual is unable or unwilling to turn over the University records in his or her possession, the department may seek the records through the procedures for access without consent. (See Section 310-24.)

2. Mail forwarding upon separation.

a. Forwarding services for email may be provided indefinitely, subject to biennial renewal, for separated users unless they leave for disciplinary reasons.

b. Separated employees whose mail is being forwarded must agree that any mail that pertains to the University's business will be returned to the department. The department head may require that all mail forwarded to a terminated user from the UCD address also be forwarded to a departmental account.

V. Allowable Uses

A. Acceptable Use Policy

All users must comply with the Acceptable Use Policy (Exhibit A) and with applicable laws and University policies (see References, below). Users must acknowledge, in writing, that they have read and understand the Acceptable Use Policy before they are allowed access to UC Davis electronic communications resources.

B. Use for University purposes

Access to EC resources is provided at the discretion of the department in consideration of educational requirements, job demands, departmental needs, and cost and efficiency factors. EC resources may be provided to UCD employees and others for the purpose of conducting the University's business and such other purposes that conform to the Acceptable Use Policy.

C. Incidental Personal Use

1. University users may use EC resources for incidental personal purposes provided that such use does not directly or indirectly interfere with the University's operation of EC resource; does not interfere with the user's employment or other obligations to the University; does not burden the University with noticeable incremental costs; and does not violate the law or University policy. Accordingly, regular or voluminous personal messages delivered via lengthy email lists are impermissible.

a. University users are prohibited from, among other things, using EC resources in a manner that creates a hostile working environment (including sexual or other forms of harassment) in violation of the law, or violates obscenity laws.

b. When noticeable incremental costs for personal use are incurred (e.g., telephone long distance charges), users shall reimburse the University.

2. Incidental personal use on behalf of an outside organization is permitted only under the circumstances listed below. Before such use, users shall verify with their supervisors that the proposed use complies with UC and UCD policy. A UCD EC resource shall not be published as the point of contact for non-University activities.

a. Charities. UCD EC resources may be used only for charitable activities that have been approved by the Chancellor (e.g., the United Way campaign). Before such use, the user must obtain written authorization from the Chancellor or designee.

b. Professional and public service organizations. UCD EC resources may be used on behalf of outside professional or public service organizations when the individual is participating as a representative of the University in the

activities of an organization of which the University is a member, or when the individual is a member of an organization in support of the University's mission.

c. Civic committees or task forces. UCD EC resources may be used on behalf of national, state, and local committees or task forces when associated with an approved University activity.

D. Policy violations

Uses that violate this policy, other University policies, or any federal or state law or regulation may result in:

1. Service restriction;
2. Corrective action under applicable University policies and collective bargaining agreements; and/or
3. Civil lawsuit or criminal prosecution.

VI. Restrictions on Use

A. Use of University EC resources is accorded at the discretion of the University and can be restricted or revoked without prior notice and without consent of the user.

1. A system administrator may temporarily restrict access to perform required maintenance. The system administrator shall give reasonable notice if possible.

2. A system administrator may temporarily restrict access to control an emergency or prevent damage or loss. The system administrator shall notify the department head and users as soon as possible.

3. A system administrator may restrict or rescind a user's access as described in UC Policy, III.E, Access Restriction. The system administrator shall:

a. Obtain approval from the department head prior to restricting the individual user's access.
b. Notify the user of the reason for the restriction and the name of the person who authorized the restriction.
c. Restore access when authorized to do so by the department head who authorized the restriction.

B. Recourse

The decision to restrict access may be appealed to the Vice Provost—Information and Educational Technology within 30 days of notification.

C. Copyright infringement

As permitted by the Digital Millennium Copyright Act (DMCA), the University may suspend access to EC systems by any user allegedly violating copyright law upon receipt of a DMCA notification. (See Section 250-05.)

VII. References and Related Policies

A. Office of the President: University of California Electronic Communications Policy.

B. UCD Policy and Procedure Manual:

1. Section 250-02, Use of Copyrighted Materials.
2. Section 250-05, Digital Millennium Copyright Act.
3. Section 270-20, Use of University Properties.
4. Section 270-25, Commercial Activities.
5. Section 310-10, Telecommunications Services.
6. Section 310-24, Electronic Communications—Privacy and Access to Records.
7. Section 310-65, Use of the University's Name and Seal.
8. Section 310-70, World Wide Web (pending approval).

C. State of California, Education Code Section 92000.
D. Digital Millennium Copyright Act of 1998 (U.S. Code Title 17, Section 512).
E. UC Davis Principles of Community.
F. Business and Finance Bulletin IS-3, Electronic Information Security.

UC Davis Policy and Procedure Manual
Acceptable Use Policy
Section 310-23 Exhibit A
5/9/06

I. Introduction

The University encourages the use of electronic communications to share information and knowledge in support of the University's mission of education, research, community service, and patient care, and to conduct the University's business. To these ends, the University supports and provides electronic communications resources such as computers, networks, video and audio equipment, telecommunications devices, email, and the World Wide Web.

Incorporating the values affirmed by the UC Davis Principles of Community, this policy governs the use of electronic communications resources at UC Davis. All UC Davis users are responsible for reading and understanding this policy. Users must acknowledge, in writing, that they have read and understand this policy before they are allowed access to UC Davis electronic communications resources.

II. Rights and Responsibilities

Electronic communications provide access to resources on and off campus, as well as the ability to communicate with other users worldwide. Such open access is a privilege and requires that individual users act responsibly. Users must respect the rights of other users, respect the integrity of the systems and related physical resources, and observe all relevant laws, regulations, and contractual obligations. Since electronic information is volatile and easily reproduced, users must exercise care in acknowledging and respecting the work of others through strict adherence to software licensing agreements and copyright laws.

The University is the legal owner and operator of all electronic communications resources purchased or leased with University funds. Overall responsibility for administering the University's electronic communications resources is primarily that of the Vice Provost--Information & Educational Technology. The Vice Provost--Information & Educational Technology may delegate overall responsibility for certain resources.

Other organizations such as universities, companies, and governments that operate resources that are accessible via the UC Davis network may have their own policies governing the use of those resources. When accessing remote resources from UC Davis facilities, users are responsible for following the policy of UC Davis and/or the remote facility, whichever is more restrictive.

III. Privacy

The University recognizes that principles of academic freedom and shared governance, freedom of speech, and privacy hold important implications for the use of electronic communications resources. This policy reflects these principles within the context of the University's legal and other obligations. The University respects the privacy of electronic communications in the same way that it respects the privacy of paper correspondence and conversations, while seeking to ensure that University administrative records are accessible for the conduct of University business.

The University does not routinely inspect, monitor, or disclose electronic communications without the holder's consent. Nonetheless, the University may deny access to its electronic communications resources and may inspect, monitor, or disclose electronic communications under certain limited circumstances, subject to the requirements for authorization, notification, and recourse in the UC and UC Davis Electronic Communications Policies.

IV. Enforcement of Laws and University Policies

Federal and state laws and University policies apply to electronic communications resources, including not only those that are specific to computers, but also those that apply generally to personal conduct.

Minor or accidental violations of this policy may be handled informally by the unit administering the accounts or network. This may be done through electronic mail or in-person discussion and education.

More serious violations (including repeated minor violations) may result in the temporary or permanent loss of access privileges or the modification of those privileges. Violators may be subject to disciplinary action up to and including dismissal or expulsion under applicable University policies and collective bargaining agreements. Violators may be referred to their sponsoring advisor, supervisor, manager, dean, vice chancellor, Student Judicial Affairs, or the Misuse of University Resources Coordinating Committee or other appropriate authority for further action.

V. Unacceptable Conduct

Unacceptable conduct includes, but is not limited to, the following attempted or completed actions:

A. Copyrights and licenses. Users shall respect copyrights and licensing agreements.
   1. Copying. Software shall not be copied except as permitted by copyright law or a license agreement.
   2. Number of simultaneous users. The number and distribution of copies shall be handled in such a way that the number of simultaneous users in a department does not exceed the number of copies purchased by that department, unless otherwise stipulated in the purchase contract.
   3. Plagiarism. Copied material shall be properly attributed. Plagiarism of electronic communications information is subject to the same sanctions as in any other medium.

B. Integrity of electronic communications resources. Users shall not interfere with the normal operation of electronic communications resources.
   1. Modification, damage, or removal. Users shall not modify, damage, or remove electronic communications resources that are owned by the University or other users without proper authorization.
   2. Encroaching on others' access and use. Users shall not encroach on others' access and use of the University's electronic communications resources. This includes but is not limited to: the sending of chain-letters or excessive messages; printing excessive copies; running grossly inefficient programs when efficient alternatives are available; unauthorized modification of electronic communications resources; attempting to crash or tie up electronic communications resources.
   3. Unauthorized or destructive programs. Users shall not intentionally develop or use programs such as, but not limited to, viruses, backdoors, and worms that disrupt other

users, access private or restricted portions of the system, identify security vulnerabilities, decrypt secure data, or damage the software or hardware components of an electronic communications resource. Legitimate academic pursuits for research and instruction that are conducted under the supervision of academic personnel are authorized by the Vice Provost—Information and Educational Technology to the extent that the pursuits do not compromise the University's electronic communications resources.

4. Unauthorized equipment. Users shall not install or attach any equipment to a UCD electronic communications resource without the explicit approval of the system administrator for that electronic communications resource.

C. Unauthorized access. Users shall not seek or enable unauthorized access.

1. Authorization. Users shall not access electronic communications resources without proper authorization, or intentionally enable others to do so.
2. Password protection. A user who has been authorized to use a password-protected account shall not disclose the password or otherwise make the account available to others without authorization.
3. Misuse of EC records. Users may seek out, use, or disclose information contained in EC records only for University business.

D. Usage. Users shall comply with applicable law and University policy.

1. Hostile working environment. Users shall not use electronic communications resources in a manner that creates a hostile working environment (including sexual or other forms of harassment), or that violates obscenity laws.
2. Unlawful activities. Users shall not use electronic communications resources for unlawful activities or activities that violate University policy, including fraudulent, libelous, slanderous, harassing, threatening, or other communications.
3. Mass messaging. Users shall avoid spamming, and other inappropriate mass messaging to newsgroups, bulletin boards, mailing lists, or individuals. Subscribers to an electronic mailing list will be viewed as having solicited any material delivered by the list so long as the material is consistent with the list's purpose.
4. Information belonging to others. Users shall not intentionally seek or provide information on, obtain copies of, or modify data files, programs, or passwords belonging to other users without the permission of those other users.
5. False identity. Users shall not use the identity of another user without the explicit approval of that user, or mask the identity of an account or machine.
6. Implying University endorsement. Users shall not imply University endorsement of products or services of a non-University entity from a University electronic communications resource without approval. Users shall not give the impression that the user is representing, giving opinions, or otherwise making statements on behalf of the University unless authorized to do so. To avoid this, the user may use a disclaimer such as "The opinions or statements expressed herein should not be taken as a position of or endorsement by the University of California."
7. Protection of restricted personal information. Employees are responsible for maintaining the security of individual's restricted personal information. Restricted personal information that is not necessary for an employees position responsibilities shall be removed from electronic communication devices. If the security of restricted personal information is compromised (e.g., loss of computer, theft, hacking), the employee must immediately inform their supervisor and the Security Coordinator at security@ucdavis.edu.

E. Political, religious, personal, and commercial use. The University is a not-for-profit, tax-exempt organization and, as such, is subject to federal, state, and local laws on the use of University property.

1. Political or religious use. In communications relating to religious or political activities or issues, the user's University title may be used only for identification. If such identification might reasonably be construed as implying the support, endorsement, or opposition of the University with regard to any religious or political activity or issue, a disclaimer (see D.6 above) shall be used.
2. Personal use. University users may use electronic communications resources for incidental personal purposes provided that such use does not: (a) directly or indirectly interfere with the University's operation of electronic communications resources, (b) interfere with the user's employment or other obligations to the University, (c) burden the University with noticeable incremental costs, or (d) violate the law or University policy.
3. Commercial use. University electronic communications resources shall not be used for non-University commercial purposes, except as permitted under University policy or with the appropriate approval.
4. Advertisements. The University's electronic communications resources shall not be used to transmit commercial or personal advertisements, solicitations, or promotions, except as permitted under University policy or with the appropriate approval.

VI. Further Information

UC Davis Policy & Procedure Manual Sections 310-23 and 310-24 (available on the Web at http://manuals.ucdavis.edu), and the University of California Electronic Communications Policy (available on the Web at http://www.ucop.edu/ucophome/policies/ec/), give further information and a list of relevant federal and state laws and University policies.

The Information & Educational Technology Services Website at http://iet.ucdavis.edu/ provides information on the use of the University's electronic communications resources.

Cyber-Safety Program Security Standards

I. PRACTICES

1. Software Patch Updates
Computers connected to the campus network must use an operating system and application software for which the publisher maintains a program to release critical security updates. Campus units must apply all currently available critical security updates within seven calendar days of update release or implement a measure to mitigate the related security vulnerability. Exceptions may be appropriate for specialized and/or research operating systems, patches that compromise the usability of an operating system or application or for patches for which the installation is prohibited by regulation.

2. Anti-virus Software
Anti-virus software must be running and updates must be applied within no more than 24 hours of update release for computing hosts connected to the campus network. This standard applies to computers and PDAs connected to the campus network using Windows, Mac OS X, Linux, Palm, or Windows Mobile PC operating systems.

3. Nonsecure Network Services
Computers connected to the network must use only network services/processes that are needed for their intended purpose or operation. All unnecessary services must be disabled. Where such services are operationally required, the available encrypted equivalent service must be used (e.g., SSH rather than Telnet) if data of a restricted nature, such as passwords or other confidential information, will be transmitted by the service. This standard applies to computers using the Windows, Mac OS X, or Linux operating systems.

4. Authentication
Campus electronic communications service providers must have a suitable process for authenticating users of shared electronic communications resources under their control.

a. No campus electronic communications service user account shall exist without passwords or other secure authentication system, e.g. biometrics, Smart Cards.

b. Where passwords are used to authenticate users, the password selection method must be configured to prohibit the use of passwords found in common dictionaries or that match the account name.

c. All default account passwords for network-accessible devices must be modified upon initial use.

d. Passwords used for privileged accounts must not be the same as those used for non-privileged accounts.

e. All campus devices must use encrypted authentication mechanisms unless an exception has been approved by a senior administrative official. Unencrypted authentication mechanisms are only as secure as the network upon which they are used. Any network traffic may be surreptitiously monitored, rendering unencrypted authentication mechanisms vulnerable to compromise.

5. Personal Information
Campus units must identify departmental computing systems and applications that house personal information (personal name along with Social Security number, California driver identification number, financial account information, health insurance information or financial account information). Personal information must be removed from all computers for which it is not required. If the personal information cannot be removed from the computing system, the campus unit must develop a plan specifically outlining how the information and systems will be kept secure. Measures to protect the information could include removing several digits from the personal identifiers, moving the files to removable media and storing this media in a secure location apart from the computer, or encrypting the personal information.

Campus units providing electronic personal information as defined above, to any private party must do so by formal agreement. The agreement must include a provision that the party receiving the electronic personal information will abide by these data standards. A formal agreement is not necessary with governmental agencies that receive electronic personal information. However, campus units are encouraged to discuss the privacy and security requirements pertaining to the shared data with these agencies to ensure similar standards of compliance.

Campus units that develop network-based applications that host personal information must use secure application coding practices (see 16, below).

6. Firewall Services

Campus units must deploy and maintain both a network (VLAN) firewall and host-based firewall service for network connected computers. The firewall must contain ingress rules that are restrictively configured to deny all traffic unless expressly permitted. Egress firewall rules must be configured to deny identified malicious network traffic if not configured to deny all traffic unless expressly permitted.

7. Physical Security

Unauthorized physical access to an unattended computing device can result in harmful or fraudulent modification of data, fraudulent email use, or any number of other potentially dangerous situations. In light of these risks, where possible, devices must be configured to "lock" and require a user to re-authenticate if left unattended for more than 20 minutes. Portable storage devices must also not be left unattended and be protected from data theft or unauthorized data modification or deletion. Physical security measures protecting computers hosting critical or sensitive university electronic communication records from theft must also be implemented. The use of data encryption may mitigate the security risks related to a physical security breach.

Servers hosting applications with essential or restricted functions or information must reside in a physically secure location. An annual physical security/risk assessment (http://security.ucdavis.edu/documents/assessmenttool.pdf) must be completed and reviewed by unit management for each area/room in which such servers are placed. Significant physical security risks identified through the assessment will be communicated by campus units to their respective Dean, Vice Chancellor or Vice Provost via the annual Cyber-safety reporting process.

8. No Open Email Relays

Devices connected to the campus network must not provide an active SMTP service that allows unauthorized third parties to relay email messages, i.e., to process an email message where neither the sender nor the recipient is a local user.

9. Proxy Services

An unrestricted proxy server for use from non-university locations is not allowed on the campus network. Use of an unauthenticated proxy server is not permitted on the campus network unless approved as an exception to the campus security standards by a senior administrative official. Although properly configured unauthenticated proxy servers may be used for valid purposes (e.g. a caching proxy for local LAN users), such services commonly exist as the result of inappropriate device configuration.

Any proxy server for use from non-university locations must ensure that

a. all users are authenticated.

b. all users meet the criteria used to qualify for access to campus licensed intellectual property such as online journals restricted to UC Davis IP addresses.

10. Audit Logs

Campus units must develop and implement a policy defining the use, inspection and retention of audit logs. Audit log inspection may permit the identification of unauthorized access to sensitive electronic communication records. The use of audit logs should be extended to document activities such as account use and the network source of the login, incoming and outgoing network connections, file transfers and transactions.

11. Backup and Recovery

Campus units must develop, implement, and maintain a backup plan for restricted information residing on electronic storage. The backup media must be protected from unauthorized access and stored in a location that is separate from the originating source. The backups must be tested on a regular basis to ensure recoverability from the backup media.

12. Training for Users, Administrators and Managers

A technical training program must be documented and established for all systems staff responsible for security administration. In addition, campus unit administrators and users handling restricted University electronic communication records must receive annual information security awareness program training regarding University policy and proper information handling and controls.

13. Anti-Spyware Software

The use of programs to identify and remove spyware programs is strongly advised to help to maintain the privacy of personal information and Internet use. The use of an anti-spyware program must be accompanied by installing program updates on regular basis to ensure the ability to detect and remove new spyware or adware programs. This standard applies to computers connected to the campus network using Windows operating systems.

14. Release of Equipment with Electronic Storage

All data must be removed from electronic storage prior to being released or transferred to another party. Data removal must be consistent with physical destruction of the electronic storage device, degaussing of the electronic storage or overwriting of the data at least three times. A “quick” format or file erasure is insufficient.

15. Incident Response Plan

Campus units must develop, publish, and maintain an incident response plan. An incident response plan will identify immediate action to be taken upon incident discovery, investigation, restoration, and reporting.

16. Web Application Security

Web applications developed or acquired by campus units must support secure coding practices. Web applications must mitigate the vulnerabilities described within the OWASP Top Ten Critical Web Application Security Vulnerabilities.

II. DEFINITIONS

Anti-virus software--A program that searches a computing device for evidence of a resident virus and removes the virus program from the device. An antivirus program is expected to include an auto-update feature that enables the program to download profiles of new viruses so that it can check for the new viruses either on the computer device or targeted towards the computing device as soon after a virus is discovered.

Campus electronic communications service providers--A unit, organization, or staff person with responsibility for allowing access to any part of UC Davis' electronic communications resources.

Computer service or process--A general term for a program that is being executed in the background of the computing device. Windows services and Unix processes load and start running as a fundamental part of operating system initiation whether or not anyone logs into the computer.

Computing hosts--Computers and personal digital assistants, including smartphones.

Critical and sensitive university electronic communication records--See UC Business and Finance Bulletin IS-3 (http://www.ucop.edu/ucophome/policies/bfb/is3.pdf) and Sections 310-23 and 310-24.

Critical security updates--An operating system or application update that corrects a vulnerability whose exploitation could allow remote control of the computing device, the propagation of an Internet worm without user authorization, a denial of the service condition, or an escalation or reduction of account privilege. Typically, the availability of a critical security update indicates the broad availability of exploit code that can take advantage of a computing device with the uncorrected vulnerability,

Incident Response Plan—A plan that describe action to be taken in response to an incident that originates from, is directed towards, or transits University controlled computer or network resources. Incident types include, but are not limited to, unauthorized access and use in violation of the acceptable use policy.

Information security awareness program training--A formal program to assist employees in understanding University policy for protecting information availability, integrity and, if appropriate, confidentiality and the role of employees in the implementation of such policies.

Native host-based firewall software--Software provided with the operating system that controls network traffic between a computer operating system and the campus network traffic. The firewall capability of the operating system may not be enabled by default.

Network Address Translation (NAT)--Internet standard that enables a local area network (LAN) to use one set of IP addresses for internal traffic and a second set for external traffic. The internal IP addresses are hidden from the external IP addresses. NAT services may be provided by a network firewall or a router.

Proxy--Acts on behalf of another whose identity may be undisclosed, creating an exploitable vulnerability for those who extend trust to the proxy.

Restricted Data—See definition in Business and Finance Bulletin IS-3 (http://www.ucop.edu/ucophome/policies/bfb/is3.pdf)

Senior Administrator—A dean, vice provost, or vice chancellor, or his/her designee.

Simple Mail Transfer Protocol (SMTP)--An Internet protocol for sending email between servers or to send email from an email client program to a mail server.

Spyware--Also referred to as adware, these computer programs typically track your Internet use and report this information to a remote location. The more malicious spyware programs may capture and report actual key strokes or personal information. The spyware programs may be installed without the computer owner's knowledge or identified in a lengthy end-user license agreement.

Technical training program--A program outlining the technical skills and knowledge required for job responsibilities. Where the position incumbent does not possess the requisite skills and knowledge, the program must outline the needed courses and course schedule. Where the system administrator possesses the requisite skills and knowledge, the technical training plan must document a plan for periodic skill and knowledge refresher courses.

Unattended computing device--A computer with an active login account that permits an unauthorized person to interact with the computing host.

Unauthenticated proxy servers--Also referred to as an open proxy, a computer that permits an unauthorized Internet user to connect through it to other network hosts.

Unencrypted authentication--The transmission of user account and password information in clear-text over the campus network.

Virtual local area network (VLAN)--A logical network of computers that appear as if they are connected to the same subnet even though they may actually be physically located on different segments of a network.

VLAN Firewall--A tool that implements security policy to control traffic between a VLAN and networks external to the VLAN.