UC Davis 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 computers connected to the campus network. This standard applies to computers connected to the campus network using Windows, Mac OS X, and Linux operating systems. Mobile handheld devices connecting to email servers configured to use message hygiene programs are consistent with this standard.

3. Non-secure 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 passphrases or other secure authentication system (e.g. biometrics, smart cards). This includes accounts used on mobile devices, such as smartphones and tablet computers, that provide access to restricted university information.

   b. Where passphrases are used to authenticate users, the passphrase selection method must be configured to require the use of passphrases that are resistant to discovery attacks. Mobile handheld devices will be configured with at least a four character passphrase or password.

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

   d. Passphrases 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 (see definition of Personal Identity Information, below). Personal information must be removed from all computers for which it is not required. 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. 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. The plan must be reviewed annually.

Campus units providing electronic personal information, as defined below, 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.

Departments that develop network-based applications that host personal identity information as defined below, or run applications that pull such information from data sources, must develop and maintain a risk management plan for those applications. Measures documented in the plan should include a description of secure coding practices in place in the unit, annual code vulnerability scans, remediation strategies to address web application vulnerabilities should any be identified, and other measures identified by the departments to secure the integrity and privacy of personal identity information. The plan must be submitted by the senior administrator of the department and reviewed and approved by the Office of the Chancellor and Provost, or designee. The plan must be reviewed annually.

In addition, developers of campus network-based applications that hos PII must acquire appropriate secure-coding expertise. Formal training programs, whether provided by the campus or otherwise, may be useful.

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 computer 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 used from non-university locations must ensure that:

   a. All users are authenticated; AND
   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 required 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. A remotely administered data wipe capability is required for mobile handheld devices.

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.

Computers—Computers include tablet devices, and personal digital assistants and smartphones, which are also referred to as mobile handheld devices.

Critical and Sensitive University Electronic Communication Records—*See UC Business and Finance Bulletin IS-3 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 describes the 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.

Personal Identity Information (PII)—a personal name with one or more of the following: social security number, California driver identification number, medical information, health insurance information, or financial account information. The definition of PII also takes into consideration PPM 310-21, Privacy and Disclosure of Information from Student Records, which references the requirement to protect a student's name, the name of a student's parent or other family members, the address of a student or student's family, any personal identifier, and any personal characteristics or other information that would make a student's identity easily traceable.

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.*

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.