

## 2009 UC Davis Cyber-Safety Survey

### UNIT INFORMATION

*Enter the following information.*

Person completing report

Email

Phone

Unit (include sub-unit information, if appropriate)

College/School/Office

College of Agricultural and Environmental Sciences

College of Biological Sciences

College of Engineering

College of Letters and Science – Humanities, Arts and Cultural Studies

College of Letters and Science – Mathematical and Physical Sciences

College of Letters and Science – Social Sciences

Graduate School of Management

Information and Educational Technology

Office of Administration

Offices of the Chancellor and Provost

Office of Graduate Studies

Office of Research

Office of Resource Management and Planning

Office of Student Affairs

School of Education

School of Law

School of Veterinary Medicine

UC Davis Health System

University Extension

University Library

University Relations

*Enter the following general information about the computing environment in your unit.*

Number of Windows Systems

Number of Macintosh Systems

Number of Unix/Linux Variant Systems

NOTE THAT THE TERM "SENIOR ADMINISTRATOR" IS DEFINED AS A DEAN, VICE-PROVOST OR VICE CHANCELLOR OR DESIGNEE (Source Cyber-safety Policy, PPM310-022)

*YOUR RESPONSES TO EACH QUESTION SHOULD REFLECT THE OVERALL LEVEL OF CYBER-SAFETY COMPLIANCE. IN THE EVENT THAT SPECIFIC SYSTEMS OR VLANS DO NOT MEET THE OVERALL LEVEL OF COMPLIANCE, PLEASE DESCRIBE THE DISCREPANCIES IN YOUR RESPONSE TO THE FINAL "ADDITIONAL INFORMATION" QUESTION IN THE APPLICABLE SECTION.*

### SECTION 1: SOFTWARE VULNERABILITIES

*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 be able to mitigate the related security vulnerability.*

*Exceptions may be appropriate for specialized and/or research operating systems, for patches that compromise the usability of an operating system or application, or for patches for which the installation is prohibited by regulation.*

1. Are you running systems for which patches are not available? Select all that apply.
  - a. No
  - b. Yes, Windows Systems
  - c. Yes, Macintosh Systems
  - d. Yes, Unix/Linux Variant Systems
2. A. Enter the number of Windows systems for which critical security updates are released by the software publisher but not applied (check with information system totals)  
 B. Enter the number of Mac systems for which critical security updates are released by the software publisher but not applied (check with information system totals)  
 C. Enter the number of Unix/Linux systems for which critical security updates are released by the software publisher but not applied (check with information system totals)
3. Have you obtained an exception approved by a senior administrator for the unpatched systems identified in question 1.2?
  - a. Yes
  - b. No (skip to 1.4)
  - c. Not applicable – no exceptions necessary (skip to 1.4)

A. If Yes, please describe, including who approved the exception.
4. Are critical security updates applied to all systems within seven calendar days of their release?
  - a. Yes (skip to 1.8)
  - b. No
5. A. How many Windows systems are not patched within seven days? (check against unit information system totals)  
 B. How many Mac systems are not patched within seven days? (check against unit information system totals)  
 C. How many Linux/Unix systems are not patched within seven days? (check against unit information system totals)
6. Have you obtained a management exception approved by a senior administrator for the delay in patching systems?
  - a. Yes
  - b. No (skip to 1.7)
  - c. Not applicable – no exception necessary (skip to 1.7)

A. If Yes, please describe, including the identification of the approver.
7. If patching is delayed, what method(s) do you use in the interim to mitigate the related security vulnerability? Please describe:
8. A. How many of the Windows systems use an auto-update mechanism to apply critical security updates?  
 B. How many of the Mac systems use an auto-update mechanism to apply critical security updates?  
 C. How many of the Linux/Unix systems use an auto-update mechanism to apply critical security updates
9. Enter any additional information you would like to include in this report regarding your practices to reduce software vulnerabilities:

## SECTION 2: VIRUS INFECTIONS

*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 and Linux, Palm or Windows Mobile PC operating systems.*

1. Select the system(s) for which you are running an anti-virus solution that provides real-time scanning.
  - a. Windows
  - b. Macintosh
  - c. Unix/Linux Variants
2. Are you running computing systems without an anti-virus product?
  - a. Yes
  - b. No (skip to 2.4)
3. A. How many Windows systems are you running without an anti-virus solution? (check against unit information system totals)  
B. How many Mac systems are you running without an anti-virus solution? (check against unit information system totals)  
C. How many Linux/Unix systems are you running without an anti-virus solution? (check against unit information system totals)
4. Has an anti-virus solution been implemented for mobile devices (personal digital assistants running Palm OS, Windows Mobile PC)?
  - a. Yes
  - b. No
  - c. Not applicable (none available)
5. Have you obtained a management exception approved by a senior administrator for the systems and/or devices not running a current and updated anti-virus solution?
  - a. Yes
  - b. No (skip to 2.6)
  - c. Not applicable – no exception necessary (skip to 2.6)

A. If Yes, please describe, including the identification of the approver.
6. Enter any additional information you would like to include in this report regarding your virus infection protection strategy. Please use this section to describe why any computing systems are not running anti-virus products.

### SECTION 3: WEAK AUTHENTICATION

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

1. *No campus electronic communications service user account shall exist without passwords or some other secure authentication system, e.g. biometrics, Smart Cards.*
  2. *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 matching the account name.*
  3. *All default account passwords for network-accessible devices must be modified upon initial use.*
  4. *Passwords used for privileged accounts must not be the same as those used for non-privileged accounts.*
  5. *All campus devices must use encrypted authentication mechanisms unless an exception has been approved by a senior administrator. 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.*
- 
1. A. How many Windows systems are you running that do not require username and password to access? (check against unit information system totals)  
B. How many Mac systems are you running that do not require username and password to access? (check against unit information system totals)  
C. How many Unix/Linux systems are you running that do not require username and password to access? (check against unit information system totals)
  2. Have you obtained a management exception approved by a senior administrator for systems not password protected?
    - a. Yes
    - b. No (skip to 3.3)
    - c. Not applicable - no exceptions necessary (skip to 3.3)  
A. If Yes, please describe the exception, including the identification of the approver.
  3. Do your password rules prohibit the use of dictionary words and account names, and meet or exceed the campus password standards?
    - a. Yes
    - b. No
  4. Have you implemented a policy and procedure requiring accounts used for privileged access to be different from those used for non-privileged or day-to-day access?
    - a. Yes
    - b. No (skip to 3.5)  
A. If no, please describe the security justification.
  5. Do you have services that transmit clear-text passwords? Examples: logins via unencrypted Web pages (http), unencrypted POP connections, telnet or ftp services.
    - a. Yes
    - b. No (skip to 3.7)

6. Please list the services and/or describe the types of any accounts your unit uses that transmit clear text passwords.
7. Have you obtained any management exception approved by a senior administrator permitting the use of weak passwords, the transmission of clear text passwords, non-privileged accounts used for privileged activities and/or use of default vendor-supplied passwords.
  - a. Yes
  - b. No (skip to 3.8)
  - c. Not applicable – no exceptions necessary (skip to 3.8)

A. If Yes, Please describe, including the identification of the approver.
8. Enter any additional information you would like to include in this report regarding your authentication practices.

#### SECTION 4: INSECURE PERSONAL INFORMATION

*Campus units must identify departmental computing systems and applications that store personal information (personal name along with Social Security number, California driver identification number, financial account information, health insurance information or medical 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 another party must do so by a formal agreement. The agreement must include a provision that replicates this data standard for the party receiving the electronic personal information.*

*Campus units that develop network-based applications that host personal information must use secure application coding practices (see Web Application Security Standard within Level 2 Security Practices).*

1. Have you completed a process to identify systems and applications within your unit that store personal information?
  - a. Yes
  - b. No (skip to 4.6)
2. Do you use an automated search tool to identify personal information residing in desktop and laptop computers?
  - a. Yes
  - b. No (skip to 4.6)
3. Describe the scanning frequency for personal identity information. At least:
  - a. Weekly
  - b. Once per month
  - c. Bi-monthly
  - d. Once per quarter
  - e. Once per year
  - f. Irregular frequency
4. What automated tool is used for this search function?
5. Please indicate which devices are subject to this search?
  - a. Desktops
  - b. Laptops
  - c. Servers
  - d. Portable Electronic Data Media
  - e. Not applicable
6. Do you have an automated tool to search databases for personal identity information?
  - a. Yes
  - b. No (skip to 4.8)
7. Please describe the database search tool(s)
8. Do you have a process to verify that personal information has been removed from electronic storage on systems where it is not required?
  - a. Yes
  - b. No (skip to 4.10)

9. Please describe the verification process.
10. If you store personal identity information on your computing systems and/or data storage devices, which of the following measures have been deployed?
  - a. Whole disk encryption or portable media encryption (skip to 4.11)
  - b. File encryption (skip to 4.11)
  - c. Physically secure portable data storage (skip to 4.11)
  - d. Other
  - e. Not applicable – no stored electronic identity information (skip to 4.11)

A. If Other, please describe.
11. Have you obtained a management exception with senior administrator approval exempting system(s) and/or storage devices from measures to protect personal identity data?
  - a. Yes
  - b. No (skip to 4.12)
  - c. Not applicable – no exception necessary (skip to 4.12)

A. If Yes, please describe, including the identification of the approver.
12. If your unit has developed network-accessible applications hosting personal information, have the applications been evaluated for use of common vulnerabilities, including the OWASP top ten application security vulnerabilities?
  - a. Yes
  - b. No (skip to 4.14)
  - c. Not applicable – no network-accessible applications with personal information (skip to 4.14)
13. Who performed the evaluation?
  - a. Unit developers
  - b. External unit
  - c. Other

A. If Other, please describe
14. Does your unit share personal identity data with third parties?
  - a. Yes
  - b. No (skip to 4.18)
15. Is this sharing of personal identity data with third parties conducted through a formal agreement with security requirements for the personal identity data?
  - a. Yes
  - b. No (skip to 4.17)
16. Which of the following does the agreement cover?
  - a. Contractor safeguarding data
  - b. Prohibit unauthorized use or disclosure
  - c. Deletion at the end of contract term
  - d. Contractor agrees to abide by UC Cyber-Safety Policy
  - e. Contractor will report unauthorized disclosures or misuse of data
  - f. Contractor agreement for internal audit of data handling practices
  - g. Contractor assistance in litigation or administrative proceedings in the event of security incident involving personal data
  - h. No assignable third-party rights

17. Have you obtained a management exception approved by a senior administrator reducing the need for the protection of personal identity data in third party agreements?

- a. Yes
- b. No (skip to 4.18)
- c. Not applicable – no exception necessary (skip to 4.18)

A. If Yes, please describe, including the identification of the approver.

18. Enter any additional information you would like to include in this report regarding your practices to secure personal information:

## SECTION 5: FIREWALL SERVICES

*Campus units must deploy and maintain both a network (VLAN) firewall and host-based firewall service for network-connected computers. The firewalls must be restrictively configured to deny all traffic unless expressly permitted.*

*A VLAN firewall is a system that implements security policy to control traffic between a VLAN and networks external to the VLAN. A VLAN firewall provides routing services and may also offer network address translation services.*

1. How many VLANs does your campus unit manage?
2. How many of your VLANs have a VLAN-level firewall deployed?
3. Are all of your computing systems behind a VLAN firewall with ingress filtering to authorized hosts?
  - a. Yes
  - b. No (skip to 5.5)
4. Which of the following rules are present on your VLAN firewall with ingress filtering?
  - a. Deny all inbound traffic unless specified
  - b. Normalize traffic (remove fragmented packets)
  - c. Allow Echo, Destination Unreachable, Time Exceeded from campus addresses
  - d. Allow Web traffic
  - e. Allow SSH traffic
  - f. Allow SMTP traffic
  - g. Allow secure POP/IMAP email authentication
  - h. Allow NTP time synchronization
  - i. Allow DNS traffic (if you host an internal DNS server)
  - j. Other

A. If Other, please describe.
5. Are you running egress filtering on all your VLAN firewalls?
  - a. Yes
  - b. No (skip to 5.7)
6. Which of the following rules are present on your VLAN firewall with egress filtering?
  - a. Deny all outbound traffic unless specified
  - b. Normalize traffic (remove fragmented packets)
  - c. Allow Echo, Destination Unreachable, Time Exceeded to campus addresses
  - d. Allow Web traffic
  - e. Allow SSH traffic
  - f. Allow SMTP traffic
  - g. Allow secure POP/IMAP email authentication
  - h. Allow NTP time synchronization
  - i. Allow DNS traffic
  - j. Other

A. If Other, please describe.
7. How frequently are VLAN firewall rules reviewed and, if necessary, updated? At least:
  - a. Weekly
  - b. Once per month
  - c. Bi-monthly
  - d. Once per quarter

- e. Once per year
  - f. Irregular frequency
8. A. How many Windows systems use a host-based firewall service? (Run check against unit information system totals)
- B. How many Mac systems use a host-based firewall service? (Run check against unit information system totals)
- C. How many Unix/Linux systems use a host-based firewall service? (Run check against unit information system totals)
9. Generally describe the predominant configuration of host-based firewalls within your unit:
- a. Ingress rules only
  - b. Egress rules only
  - c. Ingress and egress rules are present
  - d. Not applicable – no rules present (skip to 5.12)
10. For systems using a host-based firewall service, are you running rules appropriate for the role of the system?
- a. Yes, rules are system-specific
  - b. Yes, custom rules
  - c. No, the same rules are applied to all systems
  - d. Not applicable – no rules present
11. How frequently are host-based firewall rules reviewed and, if necessary, updated? At least:
- a. Weekly
  - b. Once per month
  - c. Bi-monthly
  - d. Once per quarter
  - e. Once per year
  - f. Irregular frequency
12. Have you obtained a VLAN firewall or host-based firewall-related exception approved by a senior administrator?
- a. Yes
  - b. No (skip to 5.13)
  - c. Not applicable – no exceptions necessary (skip to 5.13)
- A. If Yes, please describe, including the identification of the approver.
13. Enter any additional information you would like to include in this report regarding your firewall practices:

## SECTION 6: UNNECESSARY COMPUTER PROGRAMS/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 system.*

1. Are you aware of the services/processes running on your hosts?
  - a. Yes
  - b. No (skip to 6.6)
  
2. Describe how you perform this identification of services/processes
  - a. Use the campus self-directed Nessus scanning service
  - b. Other

A. If Other, please describe.
  
3. Describe the frequency for identifying the services/process on your hosts. At least:
  - a. Weekly
  - b. Once per month
  - c. Bi-monthly
  - d. Once per quarter
  - e. Once per year
  - f. Irregular frequency
  
4. Do you evaluate the security risk of running the identified services?
  - a. Yes
  - b. No (skip to 6.5)

A. If Yes, please describe the evaluation process, including advisement of management.
  
5. Identify which of the following services have been determined necessary to run?
  - a. Mail
  - b. Web
  - c. FTP
  - d. Telnet
  - e. VNC, rsh or other remote administration services
  
6. If you have not disabled unnecessary computer services/processes, have you obtained a management exception that has been approved by a senior administrator?
  - a. Yes
  - b. No (skip to 6.7)
  - c. Not applicable – no exceptions necessary (skip to 6.7)

A. If Yes, please describe, including the identification of the approver.
  
7. Enter any additional information you would like to include in this report regarding your practices to disable unnecessary computer programs/services:

## SECTION 7: BACKUP, RECOVERY AND DISASTER PLANNING

*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 to ensure recoverability from the backup media.*

**Restricted information** is defined as data that is considered sensitive to some degree and may include personal information or information whose unauthorized access, modification or loss could seriously or adversely affect the university (Source: Business and Finance Bulletin, IS3)

1. Does your campus unit store electronic **restricted information** on local computers or unit servers?
  - a. Yes
  - b. No (skip to 7.11)
  - c. Unknown or uncertain (skip to 7.10)
2. Are backup frequency and storage requirements for computing/storage systems containing **restricted information** defined in a campus unit backup plan or practice?
  - a. Yes
  - b. No
3. Is **restricted information** backed up on a regular schedule?
  - a. Yes
  - b. No (skip to 7.5)
4. Describe the backup frequency. At least:
  - a. Daily full backup and daily incremental backup
  - b. Weekly full backup
  - c. Once per month full backup
  - d. Bi-monthly full backup
  - e. Other

A. If Other, please describe.
5. Is **restricted information** backup media stored in a different location from the original media?
  - a. Yes
  - b. No
6. Is **restricted information** backup media protected from unauthorized physical access?
  - a. Yes
  - b. No
7. Is **restricted information** backup media containing personal identity data encrypted?
  - a. Yes
  - b. No
8. Is **restricted information** backup media regularly tested to ensure recoverability?
  - a. Yes
  - b. No (skip to 7.10)
9. Describe the frequency for testing the recoverability from backup media. At least:
  - a. Monthly
  - b. Quarterly
  - c. Semi-annually

- d. Annually
10. Have you obtained a management exception for the absence of a backup plan that provides restricted information with periodic backup, physical protection of backup media, off-site storage of backup media and testing of backup for recoverability?
- a. Yes
  - b. No (skip to 7.11)
  - c. Not applicable – no exceptions required (skip to 7.11)
- A. If Yes, please describe, including the identification of the approver.
11. Enter any additional information you would like to include in this report regarding your practices to disable unnecessary computer programs/services.

## SECTION 8: 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.*

1. Are automatic keyboard lock controls available for desktop and laptop computers that are subject to unauthorized physical access?
  - a. Yes
  - b. No (skip to 8.4)
  
2. Have you implemented automatic keyboard lock controls to discourage unauthorized use of all unattended computers?
  - a. Yes
  - b. No

A. If No, please describe why not. (skip to 8.4)
  
3. Regarding systems with the lock mechanism referenced in question 8.2, is the “lock” mechanism automatically deployed after no more than 20 minutes of unattended use?
  - a. Yes (skip to 8.7)
  - b. No

A. If no, please describe why “lock: mechanism exceeds 20 minutes
  
4. Have you obtained an exception approved by a senior administrator for not using unattended computer controls or using a lock time that exceeds 20 minutes?
  - a. Yes
  - b. No (skip to 8.5)
  - c. Not applicable – no exception necessary (skip to 8.5)

A. If Yes, please describe, including the identification of the approver.
  
5. Are all computer systems hosting restricted university electronic communication records using physical locking devices/measures and/or data encryption to prevent data theft?
  - a. Yes (skip to 8.7)
  - b. No
  - c. Not applicable (skip to 8.7)
  
6. Have you obtained a management exception approved by a senior administrator for the avoiding the use of anti-theft physical security deterrents?
  - a. Yes
  - b. No (skip to 8.7)
  - c. Not applicable – no exception necessary (skip to 8.7)

A. If Yes, please describe the exception(s) and identify the approver(s).
  
7. Please mark any of the following location characteristics for the area in which your servers reside:

- a. Located in a locked room isolated from other storage areas with room entry restricted to those with system responsibilities
  - b. Unit administration deploys strict key control to server location – only those with assigned responsibility have key access to server location
  - c. Location has an automatic alerting mechanism for forced entry
  - d. Location uses industry-accepted measures to ensure proper heating, ventilation and air conditioning for resident servers
  - e. Location has fire detection and warning system specifically for the server area
  - f. Location has uninterrupted backup power systems to ensure a facility power failure does not interrupt critical server functions
  - g. Compliance with “Server Room Best Practices” (see <http://vpiet.ucdavis.edu/bestpractices.cfm>)
  - h. Not applicable – campus unit does not locally maintain any servers
8. If your unit locally hosts applications with restricted information, the associated servers must reside in a physically secure location. Have you completed an annual physical security/risk assessment using the template provided by the Cyber-safety policy (<http://security.ucdavis.edu/documents/assessmenttool.pdf>)?

**Restricted information** is defined as data that is considered sensitive to some degree and may include personal information or information whose unauthorized access, modification or loss could seriously or adversely affect the university (Source: Business and Finance Bulletin, IS3, <http://www.ucop.edu/ucophome/policies/bfb/is3.pdf> ). Examples include name with SSN, California driver’s license number, health insurance information or financial account information, or campus/unit/employee/student information which is essential for university or school operations.

- a. Yes
  - b. No – my unit hosts local applications/servers with restricted information but has not performed this assessment (skip to 12)
  - c. Not applicable – my unit does not host local applications/servers with restricted information (skip to 12)
9. Describe any physical security/risk assessment practices which were not marked “Yes” and received a self-assigned risk level of 4.
10. If you identified non-performance of practices with a high-risk level of 4, was this risk information shared with unit management?
- a. Yes
  - b. No (skip to 12)
  - c. Not applicable – no high security/risk assessment practice areas (skip to 12)
11. Do you have a management approved mitigation plan to address high security/risk assessment practice areas identified through the annual physical security/risk assessment?
- a. Yes
  - b. No
12. Enter any additional information you would like to include in this report regarding your practices to reduce physical security vulnerabilities:

## SECTION 9: OPEN RELAY EMAIL PROXIES

*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 e-mail message where neither the sender nor the recipient is a local user.*

1. Do you prevent outbound SMTP network traffic via firewall controls except from known email servers?
  - a. Yes
  - b. No (skip to 9.3)
2. Please describe how you identify and remediate open relay email systems
3. Have you obtained a management exception approved by a senior administrator for the systems and/or devices configured to provide open email relay services that have not been removed your VLAN?
  - a. Yes
  - b. No (skip to 9.4)
  - c. Not applicable – no exception necessary (skip to 9.4)

A. If Yes, please describe the exception(s) and identify the approver(s).

4. Enter any additional information you would like to include in this report regarding your practices to secure eliminate open email relays:

## SECTION 10: UNRESTRICTED PROXY SERVERS

*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:*

- 1. All users are authenticated*
- 2. 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.*

1. Please describe how you identify and remediate access to unrestricted Web proxy servers:
2. Have you obtained a management exception approved by a senior administrator for the systems and/or devices configured to provide unrestricted Web proxy servers that have been identified and not been removed your VLAN?
  - a. Yes
  - b. No (skip to 10.3)
  - c. Not applicable – no exception necessary (skip to 10.3)

A. If Yes, please describe the exception(s) and identify the approver(s).
3. Enter any additional information you would like to include in this report regarding your practices to secure eliminate unrestricted proxy servers.

## SECTION 11: 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.*

1. Do you have a formal campus unit policy or practice requiring the identification of systems for which audit logs will be activated AND specifying the events to be included in these audit logs?
  - a. Yes
  - b. No (skip to 11.7)
2. Do you have a formal campus unit policy or practice defining the frequency at which required audit logs are to be inspected?
  - a. Yes
  - b. No
3. Are your system audit logs inspected according to the frequency defined by policy or practice?
  - a. Always
  - b. At least 80 percent of the time
  - c. Inconsistent compliance
4. Do you have a formal campus unit policy or practice defining the retention requirement for all required audit logs?
  - a. Yes
  - b. No (skip to 11.6)
5. Are the audit logs retained according to the retention policy or practice?
  - a. Yes
  - b. No
6. Describe how you secure your audit logs from unauthorized modification:
7. Have you obtained a management exception approved by a senior administrator that permits campus unit systems and/or devices to be without a formal policy or practice defining log use, inspection and retention?
  - a. Yes
  - b. No (skip to 11.8)
  - c. Not applicable – no exception necessary (skip to 11.8)

A. If Yes, please describe, including the identification of the approver.
8. Enter any additional information you would like to include in this report regarding your campus unit audit log policy or practices.

## SECTION 12: SECURITY TRAINING

*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."*

1. Has your unit deployed a security awareness program for all employees, volunteers, and sponsored affiliates using computing technology for university related purposes?
  - a. Yes, unit uses either UC Davis or System-wide security training module from campus security Web site (skip to 12.3)
  - b. Yes, unit uses security awareness training either developed internally or acquired
  - c. No (skip to 12.5)
2. Describe what Cyber-safety topics are covered by the internally developed or acquired training for all employees using computing technology.
3. Describe the target audience for current security awareness training in your unit:
  - a. Staff
  - b. Staff, faculty and researchers
  - c. Staff, faculty, researchers and affiliates
4. Describe the training frequency for security awareness training for employees using technology. At least:
  - a. Once per quarter
  - b. Once per year
  - c. Irregular frequency
5. Have you obtained a management exception approved by a senior administrator that exempts your unit from ensuring staff, faculty and affiliates using computing technology participate in general security training?
  - a. Yes
  - b. No (skip to 12.6)
  - c. Not applicable – no exception necessary (skip to 12.6)

A. If Yes, please describe, including the identification of the approver.
6. Has your unit identified the skills and knowledge that are required for system administrators to deploy and administer secure computing systems?
  - a. Yes
  - b. No (skip to 12.8)
  - c. Not applicable – technology support is performed by another unit (skip to 12.8)
7. Has your unit developed a training program to respond to any gaps between required security skills and knowledge (from 12.6) and incumbent security skills and knowledge?
  - a. Yes
  - b. No
  - c. Not applicable
8. During the last 12 months, have system administrators attended training to strengthen their security skills and knowledge?
  - a. Yes
  - b. No (skip to 12.9)
  - c. Not applicable (skip to 12.9)

A. If Yes, please describe the training received.

9. Have you obtained a management exception approved by a senior administrator for the absence of system administrator security training?
  - a. Yes
  - b. No (skip to 12.10)
  - c. Not applicable – no exception necessary (skip to 12.10)

A. If Yes, please describe, including the identification of the approver.

10. Enter any additional information you would like to include in this report regarding your security training program:

## SECTION 13: ANTI-SPYWARE

*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."*

1. Are all Windows computing systems (non-mobile devices) using an anti-spyware product?
  - a. Yes
  - b. No (skip to 13.4)
  - c. Not applicable – no Windows systems (skip to 13.6)
  
2. Does the anti-spyware product provide both real-time scanning for spyware and automatic spyware removal functions?
  - a. Yes
  - b. No
  
3. Is the anti-spyware product configured for automatic solution updates?
  - a. Yes
  - b. No
  
4. How many Windows systems are you running without an anti-spyware solution?
  
5. Have you obtained a management exception approved by a senior administrator for the Windows systems not running a current and updated anti-spyware solution?
  - a. Yes
  - b. No (Skip to 13.6)
  - c. Not Applicable – no exception necessary (skip to 13.6)

A. If Yes, please describe, including the identification of the approver.
  
6. Enter any additional information you would like to include in this report regarding your spyware protection strategy:

## SECTION 14: RELEASE OF 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.*

1. Do you always remove data from electronic storage on desktop and laptop computers before releasing or transferring the system to another party?
  - a. Yes (skip to 14.3)
  - b. No
  
2. Describe the conditions under which data from electronic storage on desktop or laptop computers is not removed prior to releasing or transferring the system to another party:
  
3. Enter the method by which you remove data before releasing the storage to another party (select all that apply):
  - a. Use a degausser to destroy data on the electronic storage (skip to 14.4)
  - b. Overwrite the entire disk drive/media at least three times using a utility that performs this function and exceeds a simple format or file erasure (skip to 14.4)
  - c. Storage is physically destroyed (skip to 14.4)
  - d. Other method

A. If Other, please describe.
  
4. Do you always remove data from electronic storage on file servers before releasing the server to another party?
  - a. Yes
  - b. No (skip to 14.6)
  - c. Not applicable - no file servers in use (skip to 14.7)
  
5. Enter the method by which you remove this data (select all that apply):
  - a. Use a degausser to destroy data on the electronic storage (skip to 14.7)
  - b. Overwrite the entire disk drive/media at least three times using a utility that performs this function and exceeds a simple format or file erasure (skip to 14.7)
  - c. Storage is physically destroyed (skip to 14.7)
  - d. Other method

A. If Other, please describe.
  
6. Have you obtained a management exception approved by a senior administrator for insecure handling of released electronic storage?
  - a. Yes
  - b. No (skip to 4.7)
  - c. Not applicable – no exception necessary (skip to 4.7)

A. If Yes, please describe, including the identification of the approver.
  
7. Enter any additional information you would like to include in this report regarding your secure handling of released electronic storage.

## SECTION 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."*

1. Do you have an established campus unit plan for computer/network incident response?
  - a. Yes
  - b. No (skip to 15.3)
  
2. Enter which of the following components are included in your campus unit incident response plan or established practice:
  - a. Definition of an incident that is subject to the incident response plan
  - b. Determination of incident severity
  - c. Internal management notification of incident with a moderate to high severity rating
  - d. Incident responsibilities for management and system administrators
  - e. Investigation procedures
  - f. Approval process for recovery or bypass of the problem source
  - g. Notification of IT Security Coordinator for incidents involving personal identity information
  - h. Notification of [abuse@ucdavis.edu](mailto:abuse@ucdavis.edu) for incidents possibly representing campus-wide threats
  - i. Identification of lessons learned from incident for management and system administration review
  
3. Have you obtained a management exception approved by a senior administrator for not developing and implementing a campus unit incident response plan?
  - a. Yes
  - b. No (skip to 15.4)
  - c. Not applicable – no exception necessary(skip to 15.4)

A. If Yes, please describe, including the identification of the approver.
  
4. Enter any additional information you would like to include in this report regarding your campus unit incident response plan.

## SECTION 16: WEB APPLICATION SECURITY VULNERABILITIES

*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."*

1. Do you host or have contracts with a non-University provider to host any Web applications?
  - a. Yes
  - b. No (skip to 16.8)
  
2. Indicate which of the following Web application vulnerabilities for which your Web application is tested:
  - a. Cross-site scripting
  - b. Injection flaws
  - c. Malicious remote file execution
  - d. Insecure direct object reference
  - e. Cross-site request forgery
  - f. Broken authentication
  - g. Insecure cryptographic storage
  - h. Insecure communications
  - i. URL access restrictions
  - j. Please describe any other vulnerabilities for which you test:
  
3. Describe how you or your vendor tests your applications for any of the vulnerabilities you identified in 16.2:
  
4. Does your campus unit possess development, test and production servers for your Web application?
  - a. Yes
  - b. No (skip to 16.6)
  
5. Enter which of the following instances of your Web application are tested for the vulnerabilities you identified in 16.2:
  - a. Development
  - b. Test
  - c. Production
  
6. Describe how you ensure development staff are knowledgeable of secure coding practices for Web applications:
  
7. Have you obtained a management exception approved by a senior administrator that exempts your campus unit from developing/using Web applications that employ secure coding practices?
  - a. Yes
  - b. No (skip to 16.8)
  - c. Not applicable – no exception necessary (skip to 16.8)

A. If Yes, please describe, including the identification of the approver.
  
8. Enter any additional information you would like to include in this report regarding your approach to identify and eliminate Web application security vulnerabilities?