

Effective: 6/5/2007

Supersedes: 6/1/2004

Issuing Office: [Academic Computing Services \(ACS\)/Administrative Computing & Telecommunications \(ACT\)](#)

TABLE OF CONTENTS NETWORK SECURITY

I.	REFERENCES AND RELATED POLICIES.....	1
A.	Federal & State Regulations.....	1
B.	University of California Policies.....	1
C.	Business and Finance Bulletin IS-3: Electronic Information Security.....	1
D.	University of California Electronic Communication Policy.....	1
E.	Policy and Procedure Manual (PPM).....	1
F.	Personnel Policies for Staff Members.....	1
II.	PURPOSE.....	1
III.	AUTHORITY.....	2
IV.	DEFINITIONS.....	2
V.	POLICY.....	3
VI.	PROCEDURES.....	3
A.	Sponsorship.....	3
B.	User Agreement.....	3
C.	Network Infrastructure.....	4
D.	Network Connectivity	4
E.	Service Provision.....	4
F.	Monitoring and Blocking.....	5
G.	Miscellaneous.....	5
H.	Violations.....	5
I.	Contracts.....	5
	Exhibit A, Departmental Network Based Firewall Statement.....	6
	Exhibit B, Network Service Port Blocking	7
	Exhibit C, UCSD Minimum Network Connections Standards.....	8
	Appendix A.....	18
	Appendix B.....	20
	Appendix C.....	21
	Appendix D.....	23

Effective: 6/5/2007

Supersedes: 6/1/2004

Issuing Office: [Academic Computing Services \(ACS\)/Administrative Computing & Telecommunications \(ACT\)](#)

NETWORK SECURITY

I. REFERENCES & RELATED POLICIES

A. Federal & State Regulations

California Public Records Act (1976)

Confidentiality of Medical Information Act

Electronic Communication and Privacy Act of 1986

Federal Family Educational Rights and Privacy Act of 1974

Federal Privacy Act of 1974

State of California Penal Code, Section 502, Chapter 858, relating to Computer Crime

B. [University of California Policies](#) and [UC San Diego Campus Regulations Applying to Campus Activities, Organizations, and Students](#)

C. [Business and Finance Bulletin IS-3: Electronic Information Security](#)

D. [University of California Electronic Communications Policy](#)

E. Policy and Procedure Manual (PPM)

[160-2](#) Disclosure of Information from Student Records

[460-5](#) Reporting and Investigating Improper Governmental Activities, Misuse of University Resources, Fraud, and Other Financial Irregularities

480-1A Information Within Word Processors, Personal Computers

480-1B Personal Computer Backup

[480-3](#) Responsibilities and Guidelines for Handling Records Containing Information About Individuals

[510-1](#) Use of University Properties

Other PPM sections dealing with academic, student, and staff discipline, and use of University equipment for personal financial gain.

F. Personnel Policies for Staff Members

[62](#) Corrective Action – Professional and Support Staff (Systemwide)

[62 HR-S-1](#) Corrective Action – Professional and Support Staff (UCSD)

II. PURPOSE

This document sets forth a security policy for the UCSD data communications network that will preserve network integrity and protect the information assets of network users.

Effective: 6/5/2007

Supersedes: 6/1/2004

Issuing Office: [Academic Computing Services \(ACS\)/Administrative Computing & Telecommunications \(ACT\)](#)

Other University policies also apply to the operation of the campus network. Relevant policies are mentioned under References above.

III. AUTHORITY

Jurisdiction of this policy is under the auspices of Academic Computing Services (ACS) and Administrative Computing and Telecommunications (ACT). Questions concerning this policy should be referred to computingpolicies@ucsd.edu.

IV. DEFINITIONS

A **user** is any individual who makes use of the network.

A **username** is a network user's personal identifier. Depending on the computer system this identifier may be variously known as the network user name, Kerberos principal, or account name.

A **sponsor** is an organization or individual who provides verification of a user's need for network services and their affiliation to the campus.

The **UCSD Backbone network** consists of routers, switches, and wiring which make up the node-to-node campus network backbone, not including building distribution equipment.

The **UCSD Production network** is all data networking at UCSD which permits data to flow over building distribution networks, the UCSD backbone, or a connection to an outside network.

A **UCSD Research network** is a network containing specialized equipment which does not connect to the production network. Should a research network connect to the production network, it is no longer considered a Research network for the purposes of this policy.

The **UCSD Data Communications Network** encompasses both the Production and Research networks.

Networking equipment is equipment which provides routing, bridging, repeating, or switching functions on a network, including routers, bridges, switches, hubs, and computers which provide any of these services for a network segment.

Data equipment is equipment capable of generating binary data on a network, including, but not limited to, desktop computers, servers, IP phones, printers, PDAs, laptops, and IP-based FAX machines.

Core network services are services such as DHCP and DNS that facilitate network use by attached data and networking equipment, and that are offered beyond the local switched segment.

Restricted network services are those from which an authorized user may make modifications to data, initiate connections to other networks, or which have data with sensitive or secure content.

Unrestricted network services are those which provide read-only access to publicly available network services.

Effective: 6/5/2007

Supersedes: 6/1/2004

Issuing Office: [Academic Computing Services \(ACS\)/Administrative Computing & Telecommunications \(ACT\)](#)

V. POLICY

Information is a principal asset of UCSD and must be protected from unauthorized modification, destruction or disclosure, whether accidental or intentional. The UCSD Data Communications Network must therefore be kept secure as it is essential to the transmission of information. The level of protection on the Network must be high enough to ensure that the most sensitive information traversing it is protected while still allowing free access to public information.

The security of the UCSD Data Communications Network, as a shared resource, is the responsibility of all network participants. Primary responsibility for the security of the production network rests with the Network Operations department of Academic Computing Services (ACS) and the Data Communications Group of Administrative Computing and Telecommunications (ACT). All other managers of a segment of the network (including managers of Research networks) are also responsible for maintaining the security of their segment.

VI. PROCEDURES

A. Sponsorship

A network user will have at least one sponsor. All campus users of the network will have an organization to act as a sponsor; in most cases this will be the individual's home department. Off-campus users of restricted services must find a sponsor within UCSD. Authorization to use services on a network device is granted by the operator of the service who may also be a sponsor.

B. User Agreement

All users of restricted network services are bound by the [University of California Electronic Communications Policy](#).

Key provisions include:

The user agrees to behave in an ethical manner and will be responsible for his or her own actions. Under California State Law any person who maliciously accesses, alters, deletes, damages or destroys any computer system, network, computer program or data is guilty of a felony.

The user understands that the network is a shared resource and will not intentionally take actions which will interfere with the operation, integrity or security of the network.

The user will not provide access to third parties without the approval of a sponsoring organization.

The user understands that network traffic and files may be subject to search under court order. In addition, system administrators may monitor network traffic or access user files as required to protect the integrity of the computer network.

The user understands that access to the network may be temporarily suspended during maintenance and that UCSD will not be liable for damages due to a failure of some network service or due to a breach of security.

The user should understand that misuse of networking resources may result in the loss of privileges. Additionally, misuse can be prosecuted under applicable statutes. The user may be held accountable for his/her conduct under any applicable University or campus policies, procedures, or collective bargaining agreements. Complaints alleging misuse of

network resources will be directed to those responsible for taking appropriate disciplinary action.

C. Network Infrastructure

Any data or networking equipment connected to the UCSD Backbone network will be approved and operated by ACS/ACT.

Core network services and networking equipment connected to the UCSD Production network will be approved by ACS/ACT. Such equipment and services will be operated by ACS/ACT except where special approval is granted. All such equipment must provide routing and access control technology to enable separation of connected segments for security and bandwidth control purposes that meet current campus standards at the time of installation.

Networking equipment will be located in physically secure areas.

In consultation with ACS/Network Operations, individual administrative units may implement additional access control technology such as firewalls to provide specialized protection for individual network segments. Such implementations should conform to current guidance. (See [Exhibit A, "Departmental Network-based Firewall Statement"](#) for an example)

D. Network Connectivity

Anyone wishing to attach a new piece of data equipment to the UCSD Production network will contact ACS/Network Operations prior to doing so and follow the appropriate ACS/Network Operations registration procedures. Any attempt to change connectivity by the introduction of new protocols or new physical or logical links will be subject to review by ACS/Network Operations.

Any piece of data equipment attached to the UCSD Production network is bound by this policy and its owner is subject to the policies listed in Section I, References and Related Policies. (See [Exhibit C, "UCSD Minimum Network Connection Standards"](#).)

It is recommended that departments divide their networks into separate physical networks along the lines of administration, research and instruction.

E. Service Provision

Providers of network services will do so in a manner that is consistent with good facility management; network security is a function of the network participants. For example, accounts will have passwords, sensitive data traversing the network should be encrypted at the endpoints in order to insure that it remains confidential, patches/fixes will be applied in a timely manner, etc. Providers of restricted network services will ensure that [Business and Finance Bulletin IS-3](#) guidelines for access security are followed as required.

Services offering access to non-public University resources (network bandwidth, restricted-access materials, etc) will authenticate users in accordance with the terms of use of the resource.

Organizations will designate a Technical Contact (a person or group of people) to be used in the event of questions or concerns about a device. It is the organization's responsibility to keep its contact data current with ACS/Network Operations.

F. Monitoring and Blocking

ACS/Network Operations monitors traffic on the network for the purpose of maintaining proper network function. By extension, traffic generated by users of computer systems on the network is also monitored.

Network devices which are suspected of having a security breach will be removed from the network at the discretion of ACS/Network Operations until the problem is resolved. Actions taken for the purposes of circumventing such a removal are not acceptable.

Network services having vulnerabilities which are known to pose a significant threat to campus network security may be blocked at the campus border at the discretion of ACS/Network Operations. Solutions will be available to allow access to blocked services by authorized remote users. Exceptions to service blocks for individual machines may be granted where circumstances dictate. (See [Exhibit B, "Network Service Port Blocking"](#))

G. Miscellaneous

Information regarding major security vulnerabilities and fixes for them is available from Academic Computing Services. Users should contact their Systems Administrator and/or the manager of their local network for security information and local policy.

H. Violations

University policy prohibits the use of University property for illegal purposes and for purposes not in support of the mission of the University. In addition to any possible legal sanctions, violators of this policy may be subject to disciplinary action up to and including dismissal or expulsion, as relevant, pursuant to University policies and collective bargaining agreements.

I. Contacts

Questions about network connectivity or function should be addressed to the following contacts:

General connectivity issues: userserv@ucsd.edu

General electronic mail problems: postmaster@ucsd.edu

Abusive or spamming electronic mail: abuse@ucsd.edu

Security incidents: security@ucsd.edu

Effective: 6/5/2007

Supersedes: 6/1/2004

Issuing Office: [Academic Computing Services \(ACS\)/Administrative Computing & Telecommunications \(ACT\)](#)

EXHIBIT A

DEPARTMENTAL NETWORK-BASED FIREWALL STATEMENT

In order to maintain Network Operations' ability to accurately troubleshoot network problems and ensure the correct functioning of the network, we set forth these guidelines for network-based firewall devices. Please consider these guidelines as starting points for departmental firewall needs.

While we do not encourage the installation of department-purchased firewall equipment, Network Operations supports safe computing campus-wide and acknowledges that some organizations may wish to filter traffic into and out of particular network segments on which they have machines. Department-installed network firewall devices are permitted on UCSD networks under the following rules:

Each such device must be properly registered with Network Operations, including the name of a technical contact for the device,

NetOps will be kept informed of current traffic-filtering rules in place on each such device,

firewall devices must not be used to obscure downstream hosts (i.e. no NAT),

department-installed firewalls will *not* be managed or maintained by Network Operations,

and the department is solely responsible for loss of service caused by the application of improper filtering rules to the device.

Network Operations will designate a "recommended" firewall device as soon as evaluations are complete.

Technical support and sample filtering rules will be available for the recommended device; other vendors' devices are permitted, but will not be supported.

It is our intent to protect UCSD networks with centrally-funded security infrastructure at the department level (and perhaps intra-department level, as required); please contact us to discuss your needs before making a purchase - technology already in place may serve your needs.

Effective: 6/5/2007

Supersedes: 6/1/2004

Issuing Office: [Academic Computing Services \(ACS\)/Administrative Computing & Telecommunications \(ACT\)](#)

EXHIBIT B

NETWORK SERVICE PORT BLOCKING

PURPOSE:

The purpose of this addendum is to formalize and document the processes by which service ports are "blocked" (access disallowed) at the campus border.

AUTHORITY:

See the Network Security Policy

RATIONALE:

The vast number of computers installed on UCSD's network has made the task of securing individual computers extremely difficult. The increasing sophistication and automation of network scans, coupled with the increasing complexity and deployment of application software on desktop machines, make a totally host-based approach to network security impractical. A network-based firewall can at least reduce campus security exposure by blocking potentially dangerous traffic from even entering the UCSD network. Blocking commonly-attacked ports on the border router is no panacea, but can be a good first line of defense.

PROCEDURE:

Pursuant to the task of ensuring network security, ACS/Network Operations may enact blocks of network service ports at the campus border.

As blocks of this type affect all machines within the campus boundary, service port blocks will not be established unless a significant threat to the security of UCSD devices or data is perceived, either from reports of hostile action elsewhere on the Internet, or resulting from analysis of campus network traffic.

Such blocks will be discussed in advance when possible, and announced immediately upon enactment on the sysadmin-l@ucsd.edu mailing list, as well as on the UCSD ACS/Security web site.

Solutions will be available to allow access to blocked services by authorized remote users. Exceptions to service blocks for individual machines may be granted where circumstances dictate.

References:

UCSD ACS/Security homepage:
<http://www-no.ucsd.edu/security>

List of currently blocked ports:
<http://www-ono.ucsd.edu/security/UCSD-only/blocked-ports.html>

UCSD Network Security Policy:
<http://adminrecords.ucsd.edu/ppm/docs/135-3.HTML>

Effective: 6/5/2007

Supersedes: 6/1/2004

Issuing Office: [Academic Computing Services \(ACS\)/Administrative Computing & Telecommunications \(ACT\)](#)

EXHIBIT C

UCSD MINIMUM NETWORK CONNECTION STANDARDS

1. IMPLEMENTATION

Complete adoption of these standards will take time and effort. We have prioritized requirements by expected difficulty. Requirements should be satisfied as expeditiously as practical; they must be finished according to this schedule. All standards without a phase specification should be completed by the first implementation date. Standards with a phase designator must be completed by the date corresponding to the phase below:

- Phase 1: January 1, 2005
- Phase 2: January 1, 2008
- Phase 3: January 1, 2009
- Phase 4: January 1, 2010

2. MINIMUM STANDARDS

To connect a device to the campus data communications network, you must comply with the following standards and directives.

2.1 Register All Devices

Register all devices with Academic Computing Services (ACS) via the UCSD Hostmaster (see appendix D for information). Review registration information periodically and update it as needed. The registration should indicate which standard applies to the device.

2.1.1 Additional Health Sciences Host Registration (Phase 2)

In addition to registration with ACS, register all devices connected to the Health Sciences network with Medical Center Information Services. Do not install Life Sustaining Medical Equipment that is dependent upon network connectivity. If installed on the network, Life Sustaining Medical Equipment must comply with either section seven or eight. All servers must have a current Risk Assessment on file with UCSD MC Information Services. Update this information annually. All devices must be running a currently-supported operating system.

2.2 Patch and Update Software (Phase 1)

Campus networked devices must run software for which security patches are made available in a timely fashion. Review available patches no later than three days from availability; apply as appropriate. If a patch is not applied, or cannot be applied for a specific reason, you must apply for an exception with ACS/Network Security and comply with all required mitigation.

2.3 Protect Against Malicious Software (Phase 1)

Malicious software detection and prevention tools appropriate for the platform, such as anti-virus software, rootkit detectors, and system integrity monitoring software, must be running and kept up to date.

Effective: 6/5/2007

Supersedes: 6/1/2004

Issuing Office: [Academic Computing Services \(ACS\)/Administrative Computing & Telecommunications \(ACT\)](#)

2.4 Limit Services (Phase 1)

Do not run any service that is not necessary for the intended purpose or operation of the device.

2.5 Configure Host-based Firewall Software (Phase 1)

Run and configure host-based firewall software to allow communication only from necessary clients and only to required services. The presence of an external access control mechanism does not obviate the need for host-based firewalls. Depending on how the device or data on it is used, UCSD Network or Data Security groups may require you to install additional protection.

2.6 Use Complex Passwords (Phase 1)

Campus electronic communications service providers must have a suitable process for authorizing any use of shared restricted electronic communications services under their control. The mechanism for providing access to service users will be referred to here as an "account".

All campus electronic communications service user accounts must have either passwords or another secure authentication system (e.g. biometrics, Smart Cards).

Where possible, devices must be configured to enforce at least the minimum password complexity requirements specified at the resource found in appendix D.

Modify all default passwords for network-accessible device accounts, and ensure they are complex.

Do not use the same passwords for privileged and non-privileged access. Organizations are strongly encouraged to use multi-factor authentication with appropriate credential controls for administrative access to systems.

2.6.1 Additional Health Sciences Password Standards (Phase 2)

Passwords for administratively privileged accounts must be at least 14 characters long, unless long passwords are not supported.

2.7 Do Not Allow Unencrypted Authentication (Phase 2)

All campus devices must use only encrypted authentication mechanisms. In particular, historically insecure services such as Telnet, FTP, SNMP, POP, and IMAP should be replaced by their encrypted equivalents. In cases where protocols are used without authentication (e.g. anonymous FTP), use of legacy protocols is permitted.

2.8 Do Not Run Unauthenticated Email Relays (Phase 1)

Campus devices must not provide an active SMTP service that allows unauthorized third parties to relay email messages, i.e., to process an e-mail message where neither the sender nor the recipient is a local user. IP-based authentication is not adequate to meet this requirement. Open email relays will be removed from the network as soon as they are detected and without warning.

Effective: 6/5/2007

Supersedes: 6/1/2004

Issuing Office: [Academic Computing Services \(ACS\)/Administrative Computing & Telecommunications \(ACT\)](#)

2.9 Do Not Allow Uncontrolled Access to Proxy Services (Phase 1)

Proxy services are not allowed on the campus network unless they have been approved by ACS/Network Operations and unless their configuration and use have been reviewed and deemed appropriate by that group.

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

Open proxy services will be removed from the network as soon as they are detected and without warning.

2.10 Enable Logging (Phase 2)

Log all authentication successes and failures on all devices. Retain logs for at least the default retention period for the operating system in use.

2.11 Employ Physical Security (Phase 2)

Where possible and appropriate, configure devices to "lock" and require a user to re-authenticate if left unattended for more than 20 minutes.

Efforts must be taken to protect computer hardware and removable media from theft.

2.12 Protect Embedded Data (PHASE 2)

When device is decommissioned or serviced, clean/destroy any internal hard drives according to the applicable standard. If disk drives are used in these devices for temporary storage, encrypt data where possible. Delete data after it is no longer needed.

3. STANDARDS FOR SHARED PUBLICLY ACCESSIBLE COMPUTERS

These guidelines cover any publicly accessible machine that is shared by many different people who may not know or trust each other. Workstations shared by a group working together are not considered "publicly accessible" for the purposes of this policy. All devices in this category must meet the Minimum Standards outlined above as well as the standards which follow.

3.1 Prevent Accidental Disclosure of Sensitive Information (Phase 2)

In order to prevent the accidental disclosure of sensitive data or the misuse of credentials, devices must prevent persistent storage of files. Any private information must be cleared from the computer between uses. Web browser histories and caches must be cleared.

3.2 Preserve System Integrity (Phase 2)

Verify and repair the integrity of the system on a regular basis. Do not permit changes to the hard disk that could result in unauthorized installation or modification of software on the computer. Limit access to system features to only those necessary to support the primary function of the computer.

3.3 Employ Physical Security (Phase 4)

Physically secure system data cables (e.g. keyboard, network) and their connections to prevent the insertion of key-logging or other monitoring hardware by unauthorized persons.

Effective: 6/5/2007

Supersedes: 6/1/2004

Issuing Office: [Academic Computing Services \(ACS\)/Administrative Computing & Telecommunications \(ACT\)](#)

4. STANDARDS FOR PRINTERS, NETWORK SCANNERS, NETWORK FAXES, WEBCAMS AND OTHER NETWORK APPLIANCES

4.1 Restrict Network Access (Phase 3)

Deploy all such devices in private IP space. Limit network access to authorized entities (using device-local or network firewall means).

4.2 Update Firmware (Phase 2)

Apply firmware updates promptly when available.

4.3 Protect Embedded Data (Phase 2)

When device is decommissioned or serviced, clean/destroy any internal hard drives according to the applicable standard. If disk drives are used in these devices for temporary storage, encrypt data where possible. Delete data after it is no longer needed.

5. STANDARDS FOR CLIENTS THAT PARTICIPATE IN SENSITIVE ACTIVITIES

These standards cover any desktop machine where one or more of the users participate in business or research activities that expose them to sensitive data. Health Sciences clinical workstations are considered "sensitive clients" for the purposes of this document. See Appendix A for definitions of data and activities that are considered sensitive.

5.1 General Requirements (PHASE 2)

- All such devices must meet the Minimum Standards outlined above
- If unauthorized access is reasonably believed to have occurred, the security incident process of the UCSD Computer Incident Response Team (CIRT) will be invoked.

5.2 System Configuration

5.2.1 Configure Host-based Firewall Software to Enforce Client Status (Phase 2)

Configure the host-based firewall to prevent incoming connections to all ports.

The host-based firewall must be a departmentally or centrally managed firewall product that logs to a departmental/central server. We recommend that intrusion prevention capabilities be part of the host-based firewall product.

Incoming connections through the host-based firewall are permitted when they support IT management and help desk activities, when they apply to specific administrative machines and specific services, and/or when they allow remote access through VPN or local network segment to primary users of the machine.

5.2.2 Patch and Update Software (Phase 2)

Apply security patches within two weeks of availability.

Effective: 6/5/2007

Supersedes: 6/1/2004

Issuing Office: [Academic Computing Services \(ACS\)/Administrative Computing & Telecommunications \(ACT\)](#)

5.2.3 Protect Against Malicious Software (Phase 2)

Anti-spyware software, if it is available for the platform, must be run and logs must be reviewed on at least a weekly basis. To prevent exposure to malicious software, scan e-mail file attachments for viruses and block risky file types (See Appendix C.)

Web filtering must be used to prevent exposure to sites that host malicious software.

5.2.4 Enable Logging (Phase 2)

Enable verbose logging at the operating system level. Logs must be able to show user, type of event, date and time with time zone, success or failure, and origin of event, and must identify system component, affected data, or resource.

In order to allow for event correlation between different log sources, synchronize clocks using Network Time Protocol (NTP). Set the time source to ntp.ucsd.edu, an Active Directory domain controller, or another accurate time source.

To prevent tampering, push logs off machine at least weekly to a central log server and store them for at least two months.

5.2.5 Scan For Sensitive Data (Phase 2)

Scan system for unencrypted sensitive data at least monthly. Where possible, remove sensitive data from the system. If it cannot be removed, sensitive data must be encrypted.

5.3 User Management

5.3.1 Use Secured Authentication (Phase 3)

Authenticate to an infrastructure that supports account fraud detection, authentication logging, disaster recovery and fault tolerance for system level authentication.

5.3.2 Restrict Administrative account USE (Phase 2)

User accounts must not be administrative users, and administrative access must only be used when required.

5.4 Vulnerability Management

5.4.1 Vulnerability Scanning (Phase 2)

ACS/Network Operations will scan devices on a regularly scheduled basis. Firewall rules must allow for comprehensive scanning from ACS/Network Operations scanning machines. Systems must have no real critical vulnerabilities.

5.4.2 Blocking (Phase 2)

In order to protect the sensitive data on these systems, a designated party will block devices from using the Internet or intranet on detection of critical vulnerabilities, unless prior arrangements have been made to mitigate any risk.

Effective: 6/5/2007

Supersedes: 6/1/2004

Issuing Office: [Academic Computing Services \(ACS\)/Administrative Computing & Telecommunications \(ACT\)](#)

5.5 Additional Health Sciences Standards (Phase 2)

Only secured email servers should be used to exchange sensitive data. As of March 2007, popmail.ucsd.edu does not meet this standard and shall not be used for this purpose. Non-UCSD e-mail providers do not meet this standard unless approved by Medical Center Information Services.

6. STANDARDS FOR SERVERS THAT PARTICIPATE IN SENSITIVE ACTIVITIES

These standards cover any servers that host applications or support clients that participate in sensitive activities. See Appendix A for definitions of data and activities that are considered sensitive.

6.1 General Requirements (Phase 2)

- All such devices must meet the Minimum Standards outlined above
- If unauthorized access is reasonably believed to have occurred the security incident process of the UCSD Computer Incident Response Team (CIRT) will be invoked.

6.2 System Configuration

6.2.1 Configure Host-based Firewall (Phase 2)

Configure host-based firewall software to allow communication only from necessary clients and only to required services. To support management, review, and logging, use a centrally managed and centrally logging firewall product. Firewall rules should be supplemented by network ACLs or network-level firewall rules.

6.2.2 Protect Against Malicious Software (Phase 2)

Use host-based intrusion-prevention system (IPS) software that can log and prevent malicious activity. For machines that deal with large amounts of sensitive data or installations that consist of many systems dealing with sensitive data, network intrusion detection must also be used.

Protect the system with anti-spyware software if it is available for the platform.

6.2.3 Patch and Update Software (Phase 2)

Apply security patches within a week of availability.

6.2.4 Enable Logging (Phase 3)

Enable logging for the operating system, web server, and applications which may be running on the server. Logs must be able to show user, type of event, date and time with time zone, success or failure, and origin of event, and must identify system component, affected data, or resource. Review logs regularly, at least three times a week.

To prevent tampering, archive logs to a central log server or read-only media and restrict access to only those with a true business need. Monitor online archived logs with change detection software. Retain logs for at least three months.

In order to allow for event correlation between different log sources, synchronize clocks using Network Time Protocol (NTP). Set the time source to ntp.ucsd.edu, an Active Directory domain controller, or another accurate time source.

Effective: 6/5/2007

Supersedes: 6/1/2004

Issuing Office: [Academic Computing Services \(ACS\)/Administrative Computing & Telecommunications \(ACT\)](#)

6.2.5 Limit Services (Phase 3)

Use a single server to support only services related to a single purpose, rather than offering many generalized services, in order to limit the potential for compromise. For example, departmental e-mail can not be hosted on the same server as departmental personnel's Web pages. Services must run with the least privilege necessary.

6.2.6 Scan for Sensitive Data (Phase 3)

Scan system for unencrypted sensitive data at least monthly. Where possible, remove sensitive data from the system. If it cannot be removed, sensitive data must be encrypted or protected using another appropriate authorized mechanism.

6.2.7 Manage Users and Privileged Accounts (Phase 2)

Change any privileged password when an employee who knows said password leaves. Make sure that you can associate activities performed with elevated privileges with an identifiable authentication event and specific individual.

6.3 VULNERABILITY MANAGEMENT

6.3.1 Vulnerability Scanning (phase 2)

ACS/Network Operations will scan devices on a regularly scheduled basis. Firewall rules must allow for comprehensive scanning from ACS/Network Operations scanning machines. Systems must have no real high-level vulnerabilities.

6.3.2 Blocking (Phase 2)

In order to protect the sensitive data on these systems, a designated party will block devices from using the Internet or intranet on detection of critical vulnerabilities, unless prior arrangements have been made to mitigate any risk.

6.4 REQUIREMENTS FOR SPECIFIC SERVICES

6.4.1 Web Server

6.4.1.1 Protect Against Malicious Software (Phase 3)

Test third-party and custom applications for common web security issues (see the OWASP top ten at <http://www.owasp.org/>) and repair. Monitor third-party applications and Web frameworks for patches and vulnerabilities. Patch any vulnerability within a week.

6.4.1.2 Preserve System Integrity (Phase 3)

In order to detect compromise or defacement, use change detection software to monitor static Web content and Web server configuration for unauthorized changes.

6.4.1.3 Use Secured Authentication (Phase 2)

Where technically possible, use campus Single Sign-On services to authenticate, selecting appropriate authentication mechanisms for the application.

6.4.1.4 Limit Access (Phase 2)

Restrict Web service to the smallest audience possible, using both authentication and firewall rules.

Effective: 6/5/2007

Supersedes: 6/1/2004

Issuing Office: [Academic Computing Services \(ACS\)/Administrative Computing & Telecommunications \(ACT\)](#)

6.4.2 File Server

6.4.2.1 Use Secured Authentication (Phase 2)

Use non-trivial authentication to enforce user and access control to the network service and the files within. Restrict access to authorized clients and users.

6.4.2.2 Limit Access (Phase 2)

Restrict file service to the smallest audience possible, using both authentication and firewall rules.

6.4.2.3 Protect Against Malicious Software (Phase 2)

Scan all shared files for viruses on at least a weekly basis.

6.4.2.4 Encrypt Data Transfer (Phase 2)

Employ transport-level encryption when transferring unencrypted sensitive data.

6.4.3 Mail Server

6.4.3.1 Protect Against Malicious Software (Phase 2)

Employ technology such as spam filtering and blacklists to limit malicious e-mail delivery. Block risky file types (see Appendix C). Scan mail folders for viruses at least weekly to locate e-mail viruses that escaped the initial scan. Scan all e-mail file attachments for viruses.

6.4.3.2 Encrypt Mail Transport/Delivery (Phase 3)

Employ transport-level encryption between mail clients and mail servers. Encrypt mail delivery whenever possible.

7. STANDARDS FOR CLIENTS CONNECTED TO, OR PART OF, LIFE-SUSTAINING MEDICAL EQUIPMENT, TREATMENT DELIVERY SYSTEMS, SUPERVISORY CONTROL AND DATA ACQUISITION (SCADA), AND HEAVY MACHINERY CONTROL SYSTEMS

Devices must meet the standards for “clients that participate in sensitive activities” outlined above as well as the standards below.

7.1 Enable Logging (Phase 2)

Collect logs as outlined in section 5.2.4, but retain them for at least six months.

7.2 Scan for Vulnerabilities (Phase 2)

Devices connected to the campus network or to the Internet must be scanned weekly using a credentialed Foundstone scan. Systems must have no real high-level vulnerabilities.

7.3. Protect Against Malicious Software (Phase 2)

To prevent the unauthorized installation of malicious software, Internet-connected clients must never run as a user with administrative capabilities.

7.4 Configure Host-based Firewall Software (Phase 2)

Devices connected to the campus network or to the Internet must have host-based firewall rules that limit the outgoing traffic to only established traffic, and limit administrative access to specified administrative

Effective: 6/5/2007

Supersedes: 6/1/2004

Issuing Office: [Academic Computing Services \(ACS\)/Administrative Computing & Telecommunications \(ACT\)](#)

machines. Configure devices to only establish connections with servers connected to or part of Life-Sustaining Medical Equipment, SCADA, and heavy machinery control systems through a bastion host.

Clients may talk directly to servers connected to or part of Life-Sustaining Medical Equipment, SCADA, and heavy machinery control systems if both systems are exclusively, and only ever, connected to a common private network.

7.4.1 Additional Health Sciences Standards (Phase 2)

Devices must have a designated UCSD Health Sciences IS contact.

8. STANDARDS FOR SERVERS CONNECTED TO, OR PART OF, LIFE-SUSTAINING MEDICAL EQUIPMENT, TREATMENT DELIVERY SYSTEMS, SUPERVISORY CONTROL AND DATA ACQUISITION (SCADA), AND HEAVY MACHINERY CONTROL SYSTEMS

Devices must meet the “standards for servers that participate in sensitive activities” outlined above as well as the standards below.

8.1 Enable Logging (Phase 2)

Collect logs as outlined in section 5.2.4, but retain them for at least six months.

8.2 Restrict Network Connectivity (Phase 2)

Do not connect devices directly to the campus network or the Internet. Configure such devices so that they cannot directly communicate with any outside host. Necessary communication can be accomplished using a bastion host to exchange data.

If connected through a bastion host, ACS/Network Operations will scan devices on a regularly scheduled basis using a credentialed vulnerability scan. Systems must have no real high-level vulnerabilities.

8.3 Configure Host-based Firewall Software (Phase 2)

Limit outgoing traffic using the host-based firewall to only allow necessary communication with clients meeting the client specification that have no Internet connectivity, and/or with the bastion host.

8.3.1 Additional Health Sciences Standards (Phase 2)

Devices must have a designated UCSD Health Sciences IS contact.

9. STANDARDS FOR VIRTUAL MACHINE(VM) HOST SYSTEMS THAT SUPPORT IMAGES THAT ARE CONNECTED TO, OR PART OF, LIFE-SUSTAINING MEDICAL EQUIPMENT, TREATMENT DELIVERY SYTSTEMS, SUPERVISORY CONTROL AND DATA ACQUISITION (SCADA), AND HEAVY MACHINERY CONTROL SYSTEMS

Host systems must meet the “standards for servers that participate in sensitive activities” outlined above. Guest systems must meet the minimum standards.

9.1 Preserve System Integrity (Phase 2)

Verify and repair the integrity of the operating system, applications and VM software at least weekly using change detection software.

9.2 Limit Services (Phase 2)

Do not offer any services on the host system other than VM management software. Limit access to VM management software to only authorized administrative machines or approved VPN infrastructure as necessary.

9.3 Restrict Network Communications (Phase 2)

The VM virtual network interface and host operating system must enforce network security rules to limit inappropriate communication between virtual machines and/or the host.

Effective: 6/5/2007

Supersedes: 6/1/2004

Issuing Office: [Academic Computing Services \(ACS\)/Administrative Computing & Telecommunications \(ACT\)](#)

APPENDIX A – DEFINITIONS

1. SENSITIVE ACTIVITIES

For the purposes of this document, Sensitive Activities are defined as anything that involves the storage, entry, processing, transmission, or viewing of Sensitive Data.

2. SENSITIVE DATA

Sensitive Data is any data that is regulated by law or limited by contractual agreements between the University and other business partners.

3. CRITICAL VULNERABILITIES

A Critical Vulnerability is one where an exploit or proof-of-concept code is publicly available or being actively exploited.

4. FAMILY EDUCATIONAL RIGHTS AND PRIVACY ACT (FERPA)

FERPA covers all student data. We may disclose without consent, "directory" information such as a student's name, address, telephone number, date and place of birth, honors and awards, and dates of attendance as long as we honor the students disclosure preferences from Tritonlink. If any data is present that has been flagged for non disclosure or the disclosure option is not checked and enforced then the data is considered sensitive.

5. GRAMM-LEACH-BLILEY ACT (GLBA ACT)

The GLB Act, officially known as The Financial Modernization Act of 1999 includes privacy provisions to protect consumer information held by financial institutions. Because of the student loan activity, the University is considered a financial institution under the GLB Act. Family Educational Rights and Privacy Act (FERPA) compliance places the University in compliance with FTC privacy rules under the GLB Act.

6. CALIFORNIA PUBLIC RECORDS ACT CODE 6250-6270

The Act mandates public access to records held by the University. The Act also provides exclusions for access to certain types of records or data. Examples of data that are excluded include personal payroll/employee data such as state and federal tax withholding. The Act requires that we protect the privacy and integrity of this data and its use at the University.

7. CALIFORNIA STATE SENATE BILL SB 1386

SB 1386 requires that we disclose any unauthorized access to SSN, DL#, financial account or credit card number in combination with any password that would permit access to the individual's financial account.

8. HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 (HIPAA)

HIPAA is a federal law establishing national standards that provide for the privacy and security of an individual's health information. Information created or received by a health care provider or health plan that includes health information or health care payment information plus information that personally identifies the individual patient or plan member.

Personal identifiers include: a patient's name and email, web site and home addresses; identifying numbers (including Social Security, medical records, insurance numbers, biomedical devices, vehicle identifiers and license numbers); full facial photos and other biometric identifiers; and dates (such as birth date, dates of admission and discharge, death).

9. PAYMENT CARD INDUSTRY (PCI) STANDARDS

The PCI standard is a contractual agreement between the University and our merchant bank. The agreement covers our handling of credit card numbers, magnetic stripe contents, CVC numbers, and expiration dates. In addition to the standards outlined above for sensitive systems, PCI requires additional security and has its own set of standards that must be met.

Effective: 6/5/2007

Supersedes: 6/1/2004

Issuing Office: [Academic Computing Services \(ACS\)/Administrative Computing & Telecommunications \(ACT\)](#)

APPENDIX B – EXCEPTIONS

Departments, units, or individuals unable to comply with the UCSD Minimum Network Connection Standards but wishing to connect to the campus electronic communications network must identify resources that will assist them (on an ongoing basis) in becoming compliant. Devices that do not comply with the minimum standards are subject to exclusion from the campus network.

Departments, units, or individuals who believe their devices require configurations that do not comply with the UCSD Minimum Network Connection Standards may request connection to the campus electronic communications network on an exceptional basis. The exception process will involve other mitigation of the risks that the UCSD Minimum Network Connection Standards address.

Questions about the UCSD Minimum Network Connection Standards or the exception process may be addressed to: security@ucsd.edu.

Effective: 6/5/2007

Supersedes: 6/1/2004

Issuing Office: [Academic Computing Services \(ACS\)/Administrative Computing & Telecommunications \(ACT\)](#)

APPENDIX C – RISKY FILE TYPES

File Extension	Description
.ani	Windows animated cursor file security vulnerability. Possible buffer overflow in Windows
.bat	Batch files are often malicious
.bmp	Windows bitmap file security vulnerability. Possible buffer overflow in Windows
.cab	Possible malicious Microsoft cabinet file
.cer	Dangerous Security Certificate (according to Microsoft Q883260)
.chm	Compiled help files are very dangerous in email
.cmd	Batch files are often malicious
.cnf	SpeedDials are very dangerous in email
.com	Executable DOS/Windows programs are dangerous in email
.cpl	Control panel items are often used to hide viruses
.cur	Windows cursor file security vulnerability. Possible buffer overflow in Windows
.exe	Executable DOS/Windows programs are dangerous in email
.hlp	Windows help file security vulnerability. Possible buffer overflow in Windows
.hta	HTML archives are very dangerous in email
.ico	Windows icon file security vulnerability. Possible buffer overflow in Windows
.ins	Windows Internet Settings are dangerous in email
.its	Dangerous Internet Document Set (according to Microsoft Q883260)
.job	Task Scheduler requests are dangerous in email
.jse*	JScript Scripts are dangerous in email
.lnk	Eudora .lnk security hole attack
.mad	Microsoft Access Shortcuts are dangerous in email
.maf	Microsoft Access Shortcuts are dangerous in email
.mag	Microsoft Access Shortcuts are dangerous in email
.mam	Microsoft Access Shortcuts are dangerous in email
.maq	Microsoft Access Shortcuts are dangerous in email
.mar	Microsoft Access Shortcuts are dangerous in email
.mas	Microsoft Access Shortcuts are dangerous in email
.mat	Microsoft Access Shortcuts are dangerous in email
.mau	Dangerous attachment type (according to Microsoft Q883260)
.mav	Microsoft Access Shortcuts are dangerous in email
.maw	Microsoft Access Shortcuts are dangerous in email
.mda	Dangerous attachment type (according to Microsoft Q883260)
.mdz	Dangerous attachment type (according to Microsoft Q883260)
.mhtml	MHTML files can be used in an attack against Eudora
.pif	Shortcuts to MS-Dos programs are very dangerous in email
.prf	Dangerous Outlook Profile Settings (according to Microsoft Q883260)
.pst	Dangerous Office Data File (according to Microsoft Q883260)
.reg	Windows registry entries are very dangerous in email
.scf	Windows Explorer Commands are dangerous in email
.scr	Windows Screensavers are often used to hide viruses
.sct	Windows Script Components are dangerous in email
.shb	Shortcuts Into Documents are very dangerous in email
.shs	Shell Scrap Objects are very dangerous in email
.tmp	Dangerous Temporary File (according to Microsoft Q883260)
.vbe	Visual Basic Scripts are dangerous in email

.vbs	Visual Basic Scripts are dangerous in email
.vsmacros	Dangerous Visual Studio Macros (according to Microsoft Q883260)
.vss	Dangerous attachment type (according to Microsoft Q883260)
.vst	Dangerous attachment type (according to Microsoft Q883260)
.vsw	Dangerous attachment type (according to Microsoft Q883260)
.wmf	Windows Metafile security vulnerability
.ws	Dangerous Windows Script (according to Microsoft Q883260)
.wsc	Windows Script Host files are dangerous in email
.wsf	Windows Script Host files are dangerous in email
.wsh	Windows Script Host files are dangerous in email
.xnk	Microsoft Exchange Shortcuts are dangerous in email
.zip	Compressed and packaged files used to distribute many virus/trojans
.txt.exe	Attachments using multiple extensions
filename.{1CE8B2C9-EAEF-43fc-8218-F092E4F94A47}	Format of Windows Class Identifiers (CLSID) The CLSID will not usually be displayed to the user. Windows may run the program that is associated with the CLSID if the user attempts to open the file.

Effective: 6/5/2007

Supersedes: 6/1/2004

Issuing Office: [Academic Computing Services \(ACS\)/Administrative Computing & Telecommunications \(ACT\)](#)

APPENDIX D – RESOURCES

Password guidelines: <http://www-no.ucsd.edu/services/netusername.html>

Host registration: <http://www-no.ucsd.edu/ono-cgi-bin/etherform/etherform.pl>