**COMPUTING SERVICES**
**Section: 135-3 EXHIBIT B**
Effective: 01/17/2012
Supersedes: 04/15/2010
Review Date: TBD
Issuance Date: 01/17/2012
Issuing Office: Administrative Computing & Telecommunications (ACT)

***EXHIBIT B***

## UCSD MINIMUM NETWORK CONNECTION STANDARDS

### 1. IMPLEMENTATION

As of January 1, 2010, all standards are in effect. We have retained effective dates for historical purposes.

### 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 Administrative Computing and Telecommunications/IT Infrastructure via the UCSD Hostmaster (see Appendix D for information). ResNet machines must be registered with ResNet instead. 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 (Effective January 1, 2008)

In addition to registration with ACT, register specified Health Sciences devices 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 (Effective January 1, 2005)

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 ACT/IT Infrastructure and comply with all required mitigation.

### 2.3 Protect Against Malicious Software (Effective January 1, 2005)

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. Where machines are University-owned, the responsibility for ensuring protective software is updated ultimately rests with the department or laboratory. The responsibility for these tools on personally-owned devices rests with the individual owner

### 2.4 Limit Services (Effective January 1, 2005)

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 (Effective January 1, 2005)

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.

Note that ACT/IT Infrastructure provides network-based firewalls to departments and units. Groups should contact ACT/IT Infrastructure for information on how to apply that layer of security. Existence of network firewalls does not obviate the need for host-based firewalls.

### 2.6 Use Complex Passwords (Effective January 1, 2005)

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 (Effective January 1, 2008)

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 (Effective January 1, 2008)

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

### 2.8 Do Not Run Unauthenticated Email Relays (Effective January 1, 2005)

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.

### 2.9 Do Not Allow Uncontrolled Access to Proxy Services (Effective January 1, 2005)

Proxy services are not allowed on the campus network unless they have been approved by ACT/IT Infrastructure 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 (Effective January 1, 2008)

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 (Effective January 1, 2008)

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 (Effective January 1, 2008)

When a 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 that follow.

### 3.1 Prevent Accidental Disclosure of Sensitive Information (Effective January 1, 2008)

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 (Effective January 1, 2008)

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 (Effective January 1, 2010)

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.

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

### 4.1 Restrict Network Access (Effective January 1, 2009)

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 (Effective January 1, 2008)

Apply firmware updates promptly when available.

### 4.3 Protect Embedded Data (Effective January 1, 2008)

When a 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 (Effective January 1, 2008)

- 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 (Effective January 1, 2008)

Configure the host-based firewall to block all incoming connections by default. Incoming connections through the host-based firewall can be 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.

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.

#### 5.2.2 Patch and Update Software (Effective January 1, 2008)

Apply security patches within two weeks of availability.

#### 5.2.3 Protect Against Malicious Software (Effective January 1, 2008)

Anti-spyware software, if it is available for the platform, must be run. Available anti-virus and anti-spyware logs must be reviewed on at least a weekly basis. Where machines are University-owned, the responsibility for ensuring protective software is run and logs are reviewed ultimately rests with the department or laboratory. The responsibility for these actions on personally-owned devices rests with the individual owner. 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 (Effective January 1, 2008)

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 (Effective January 1, 2008)

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 (Effective January 1, 2009)

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 (Effective January 1, 2008)

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 (Effective January 1, 2008)

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

#### 5.4.2 Blocking (Effective January 1, 2008)

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.

### 5.5 Additional Health Sciences Standards (Effective January 1, 2008)

Only secured email servers should be used to exchange sensitive data. 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 (Effective January 1, 2008)

- 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 (Effective January 1, 2008)

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 (Effective January 1, 2008)

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 (Effective January 1, 2008)

Apply security patches within a week of availability.

### 6.2.4 Enable Logging (Effective January 1, 2009)

Enable logging for the operating system, web server, and applications that 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 time.ucsd.edu, an Active Directory domain controller, or another accurate time source.

### 6.2.5 Limit Services (Effective January 1, 2009)

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 (Effective January 1, 2009)

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 (Effective January 1, 2008)

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 (Effective January 1, 2008)

ACT/IT Infrastructure will scan devices on a regularly scheduled basis. Firewall rules must allow for comprehensive scanning from ACT/IT Infrastructure's scanning machines. Systems must have no real high-level vulnerabilities.

### 6.3.2 Blocking (Effective January 1, 2008)

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 (Effective January 1, 2009)

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 (Effective January 1, 2009)

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 (Effective January 1, 2008)

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

#### 6.4.1.4 Limit Access (Effective January 1, 2008)

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

### 6.4.2 File Server

#### 6.4.2.1 Use Secured Authentication (Effective January 1, 2008)

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 (Effective January 1, 2008)

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

#### 6.4.2.3 Protect Against Malicious Software (Effective January 1, 2008)

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

#### 6.4.2.4 Encrypt Data Transfer (Effective January 1, 2008)

Employ transport-level encryption when transferring unencrypted sensitive data.

### 6.4.3 Mail Server

#### 6.4.3.1 Protect Against Malicious Software (Effective January 1, 2008)

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 (Effective January 1, 2009)

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 (Effective January 1, 2008)

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

### 7.2 Scan for Vulnerabilities (Effective January 1, 2008)

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 (Effective January 1, 2008)

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 (Effective January 1, 2008)

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 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 (Effective January 1, 2008)

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 (Effective January 1, 2008)

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

### 8.2 Restrict Network Connectivity (Effective January 1, 2008)

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, ACT/IT Infrastructure 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 (Effective January 1, 2008)

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 (Effective January 1, 2008)

Devices must have a designated UCSD Health Sciences IS contact.

## 9. STANDARDS FOR VIRTUAL MACHINE(VM) HOST SYSTEMS THAT SUPPORT IMAGES OF HOSTS THAT ARE CONNECTED TO, OR PART OF, LIFE-SUSTAINING MEDICAL EQUIPMENT, TREATMENT DELIVERY SYSTEMS, 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 (Effective January 1, 2008)

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

### 9.2 Limit Services (Effective January 1, 2008)

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 (Effective January 1, 2008)

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.