## RESEARCH AFFAIRS ORU and Reporting Department IT Guidelines
## November 2010

We support the secure use, processing, storage, and transmission of digital information and media among the UC San Diego research community, including administration, staff, faculty, students, extramural participants, and a worldwide audience interested in UC San Diego's research enterprise.

Our goal is to ensure data integrity, usability, confidentiality, appropriate access levels, and security for all supported units including Organized and Multi-campus Research Units, the Conflict of Interest office, the Office of Contract and Grant Administration, the Technology Transfer Office, the Animal Welfare Program, the Research Ethics Program, Embryonic Stem Cell Research Oversight, Postdoctoral and Visiting Scholar Affairs, Research Proposal Development Services, and the Natural Reserve System, in addition to the central Office of Research Affairs.

### Services and Associated Guidelines Available to Reporting Departments



### *A) Access Controls, Access Privilege Levels, and Passwords*

When workstations and laptops need to be reconfigured from out of the box settings, a system administrator/IT support person is needed. Built-in accounts that come standard on Windows systems, such as guest and administrator, must be

reconfigured by a system administrator to prevent unauthorized access to data and unwanted control over the system.

Computer systems, whether Windows-based, Unix-based (e.g. Macintosh) or Linux based have built-in levels of privilege, establishing, by level, what changes may be made to the system. The highest level of privilege is that of administrator which allows for installation and execution of new software and running of scripts. Workstations for end users of workstations should be set at a system privilege level that is adequate to perform daily computer tasks. This ensures that malignant software entering from a website or email message will not automatically gain access to an end users' system through administrator privileges.

Access to workstations and servers must be controlled through the use of passwords and authenticated through the campus active directory (AD). Passwords must be a minimum of 8 characters, and contain complex (at least one number and one uppercase character) configurations. It is recommended that passwords be changed at least every 90 days. Passwords should not be shared, written down, or visible to others.

System Administrators are strongly encouraged to take advantage of the campus active directory and Group Policy Object (GPO) to automate and standardize the enforcement of password policies.

To ensure the continuous operation of campus web applications, and the integrity of the processes and services running on those servers, access to databases and web application servers should be restricted to system administrators and developers.

### *B) System Configuration*

Windows, Mac, and Linux systems have settings, referred to as local security policy in Windows, that control what users may do at each access level. These settings must be configured by the system administrator and, as in the case of passwords, can often be remotely administered by the administrator for the user. Workstations, laptops, and servers should be configured to allow essential business functions and have other unnecessary features, functions or settings turned off or locked down to avoid unintended use.

Ports and Services should be limited to those needed for the productive use of the desktop, laptop, or server.

**a. Firewalls**

There are two kinds of firewalls: host-based and router-based. These firewalls control what network traffic can occur between computers, including the internet, and communication between desktops, laptops, printers, wireless devices, and servers. Both types should be in place, with each properly

configured. Host-based firewalls should be configured by a system administrator, and router-based by a system administrator in conjunction with the campus ACT (Academic Computing and Telecommunications) Firewall team (firewall@ucsd.edu).

**b. Services**

In addition to frequently updating and patching software it is important to limit the number of services running on workstations and servers. Services are resident computer programs that run on a computer in support of system and other application software. Sometimes the services are essential to the smooth operation of a workstation, laptop, or server. Other times having an unnecessary service running, represents a vulnerability. Limiting the number of services that run on a device decreases the number of open ports on network devices, thereby reducing the risk that future vulnerabilities will be exploited.

**c. Ports**

Communication between computers occurs via ports which are channels through which data can travel in and out of a computer. Because a computer has to carry out multiple transactions at a time, there are multiple ports dedicated to particular types of communication between computers and devices. Ports that are left open but not needed, should be disabled or firewalled to prevent unwanted data and software from invading a computer or server.

## *C) System Software Updates ("patches")*

Campus workstations and servers must be regularly updated with system and software updates. Depending on the sensitivity of the data on the systems the timeframe considered timely for applying system patches may range from three days to two weeks.

System administrators may support this activity by direct updates or, by configuring the system to automatically download and install patches.

## *D) Email and Calendaring*

The recommended solution for all campus email communication and calendaring is the UCSD campus AD Exchange server. The service is provided at no charge to departments and ORUs, is fully supported by ACT, and it is a robust and reliable solution for communication and scheduling from campus computers or handheld devices and the internet.

## *E) Network Configuration and Security*

Whenever possible, networks should be administered using the UCSD AD. The campus AD provides secure control of domains and subdomains on campus allowing for granular configuration and system administration at the local subdomain or organizational unit level.

By using the campus Active Directory, many routine system and user administration tasks can be accomplished remotely, with minimal direct intervention at the workstation or machine level.

### *F) Unencrypted Sensitive Information, PII, Student Data, and Medical Records*

Sensitive information, also known as Personal Identity Information (PII) is defined as: an individual's first name or initial, and last name, in combination with one or more of the following:

1. Social Security number (SSN)
2. Drivers license number or State-issued identification card number
3. Account number, credit card number, or debit card number in combination with any required security code, access code, or password such as expiration date or mother's maiden name that could permit access to an individual's financial account

This definition of electronic PII is not dependent on where the information is stored. Electronic personal identity information may exist on, but is not limited to, hard drives, magnetic tape, optical disks, diskettes, hand held computing devices, etc.

Wherever possible, business processes should be revised so that storage of PII is not required. Additionally, in instances where sensitive data is needed for a legitimate business purpose, the PII must be encrypted and the department maintaining the data will need networked devices to be scanned for unencrypted sensitive data on a periodic basis.

There are strict guidelines in place for the storage of student data, such as grades and health data. Whenever possible, these data should not be stored, but if required to do so, data must be encrypted and additionally secured as in the manner for PII.

Information on records retention policies is available at
http://amas.ucsd.edu/Documents/RecordsRetention.pdf

### *G) Application Development*

Developing applications typically requires a significant investment in planning, designing, secure coding, long-term maintenance, technical support, and end user training. Before developing a custom application, consider leveraging an existing campus solution, secure open source alternatives, or an affordable third party solution. If none of these options meets your needs, it is recommended that you consult with ORA IT to discuss how the application will be implemented in accordance with best development practices.

### *H) Routers and Wireless Connections*

The UCSD ACT Wireless team is responsible for supplying and maintaining wireless access to the campus network. Departments and ORUS should not install or maintain their own wireless hubs, routers, or splitters. If you find your unit does not have sufficient connectivity, either via cabled or wireless access, please contact the ACT helpdesk directly, copying your system administrator in case the problem is local.

There are two ways to gain access to the UCSD wireless network: GUEST and AD-PROTECTED. Whenever possible, it is recommended you connect as PROTECTED, as GUEST transmissions are sent unencrypted, in clear text. Login credentials, business, or personal information can be easily intercepted and read in transit between your computer and the wireless network.

System administrator support is required to set up a laptop or other computer for PROTECTED wireless access the first time.

### *I) Printers, Scanners, and Other Peripherals with Routable IP address*

Printers and other peripheral devices connected to your network should be configured such that they are private to your network and not accessible to outside users. This will prevent against unauthorized use and limit vulnerabilities to your network since printers and peripherals are less secure.

The UCSD Minimum Network Connection Standards section 4.1 requires that printers be deployed in private IP space. Printers are typically only used by other internal devices and do not need to be accessed by devices external to the network.

### *J) Remote Desktop and VPN*

Off campus access to campus workstations should only be permitted through the encrypted campus Virtual Private Network (VPN) using AD Authentication. Direct access to campus workstations is not permitted. Personal computers used to access UCSD workstations or servers should be properly updated, with robust virus malware and spyware protection

### *K) Network Documentation*

ORUs and departments should maintain records of workstations, notebook, PDAs, and servers including make, model, MAC address, IP address, software installed and principal user(s). The campus hostmaster should be informed of which computer identities in the AD correspond to which IP and MAC addresses.

### *L) Physical Security*

Computers that store, or allow access to campus data, must be physically secured. Open and unprotected access to the hardware can lead to circumvention of system security and/or destruction or loss of data as well as the potential loss or compromise of physical equipment.

### *M) Hardware Selection and Purchasing Guidelines*

Custom assembled campus systems, and those made by local computer shops, often require significant long term maintenance. It is recommended that computers be purchased from major hardware manufacturers.

Suppliers and computer products offered through Marketplace have been selected through a comprehensive analysis of the products to meet UC IT requirements. It is strongly encouraged that departments utilize Marketplace for their computer hardware purchasing needs.

Departments and ORUs should consult with RAIT before making major hardware purchases to discuss recommended configurations and system values.

### *N) Website Design , Development and Hosting*

Departments are encouraged to consider using the UC San Diego template for standard business websites and hosting their websites in the UC San Diego Content Management System. This is a simple, effective way to manage websites that need to be updated by multiple users, and don't feature interactive media or applications. Regardless of the hosting solution, departments are encouraged to follow the campus style guide, keeping in mind website accessibility. The following resources are available to assist with development:

Web Accessibility Guidelines and Resources
http://blink.ucsd.edu/technology/help-desk/usability/index.html#Accessibility-resources

Web Design Templates
http://cwo.ucsd.edu/toolkit/index.html

Web Design Guidelines
http://cwo.ucsd.edu/toolkit/guidelines.html

Campus Editorial Style Guide
*http://blink.ucsd.edu/sponsor/ACT/staff/portal-services/working/styleguide.html*

### *O) Software Purchasing, Upgrades, and Software Assurance*

Software should be installed by an administrator and centrally tracked to maintain conformance with Campus Licensing Agreements and sound fiscal accounting practices. Whenever possible, software should be acquired via Campus Software Distribution services. It is recommended that software purchased for long term use be purchased

with a Software Assurance option to avoid costly upgrades. Avoid purchasing software for incidental use where a trial version, locally available, or a shareware alternative would suffice. Software should be centrally tracked and maintained in a spreadsheet or database.

It is the Campus Software Policy that software purchased through Academic Computing Services (http://software.ucsd.edu/) not be installed on computers that are not the property of UC San Diego. Should a department decide to purchase software for use on a non campus computer, the software must be purchased from a source other than ACS software, such as the campus bookstore or, for example, Amazon.

### *P) Data Storage and Backup*

Data essential to the business processes and work product of a department should be centrally stored and backed up daily. Non essential personal files, such as mp3 or digital photos, should be stored locally, such that they are not backed up. Personal data stored locally on workstations should be limited so as to not tax either the storage capacity or the performance capabilities of the laptop or workstation.