INFORMATION TECHNOLOGY SECURITY POLICY

The University of Redlands financial, administrative, and instructional systems are accessible through the University's network. As such, they are vulnerable to security breaches that may compromise confidential information and expose the university to losses and other risks.

At the University of Redlands, security is critical to the physical network, computer operating systems, and application programs and each area offers its own set of security issues and risks. Confidentiality and privacy, access, accountability, authentication, availability, and system and network maintenance are components of a comprehensive security policy. This policy identifies key concerns and issues faced by the University community at the application, system, and network level, and strives for a balance between the University's desire to promote and enhance the free exchange of ideas and its need for security of critical information and systems.

This document will:

1. Identify the elements of a good security policy;
2. Explain the need for Information Technology security;
3. Specify the various categories of Information Technology security;
4. Indicate the Information Technology Security responsibilities and roles; and
5. Identify appropriate levels of security through standards and guidelines.

This document establishes a central security policy and direction for the University of Redlands. Individual departments are expected to establish standards, guidelines and operating procedures that adhere to and reference this policy while addressing their specific and individual needs.

1. Information Technology Security Elements

The elements of a good security policy include:

- Confidentiality and Privacy
- Access
- Accountability
- Authentication
- Availability
- Information technology system and network maintenance policy

Confidentiality refers to the University's needs, obligations and desires to protect private, proprietary and other sensitive information from those who do not have the right and need to obtain it.
Access defines rights, privileges and mechanisms to protect assets from access or loss.
Accountability defines the responsibilities of system and network users.
Authentication establishes password and authentication policy.

Availability establishes hours of resource availability, redundancy and recovery, and maintenance downtime periods.
Information Technology system and network maintenance describes how both internal and external maintenance people are allowed to handle and access technology.

2. Need for Information Technology Security

The University and all members of the University community are obligated to respect and protect confidential data. Financial records, student records, certain employment-related records, library use records, attorney/counselor-client communications, health services records, and certain research and other intellectual property-related records are, subject to limited exceptions, confidential as a matter of law. Many other categories of records, including faculty and other personnel records, and records relating to the University's business and finances are, as a matter of University policy, treated as confidential.

Systems (hardware and software) designed primarily to store confidential records (such as Ellucian Colleague and ADP system) require enhanced security protections and are controlled systems to which access is closely monitored. Networks provide connection to records, information and other networks, and also require security protections. The use of University Information Technology assets in other than a manner and for the purpose of which they were intended represents a misuse of resources and, possibly, a violation of law. Please refer to the University's Policy for the Responsible Use of Information Technology for more information.

3. Security Categories

This policy applies to the following categories of security:

- **Computer system and applications security**: Servers, desktops, laptops, peripherals, operating systems, applications, and data
- **Physical security**: The premises occupied by Information Technology Services (ITS) personnel and equipment
- **Operational security**: Environment control, power equipment, operational activities
- **Procedural security**: Established and documented security processes for ITS staff, vendors, management and individual users
- **Network security**: Network communications equipment and personnel

4. Information Technology Security Responsibilities and Roles

Responsibility for guaranteeing appropriate security for applications, systems, networks, and data is assigned to the University of Redlands' ITS personnel, University administrators, deans, directors, and department heads. In many cases, responsibility for designing, implementing and maintaining security protections will be delegated to ITS staff, but the dean, director or department head will retain responsibility for ensuring compliance with this policy. In addition to management and ITS staff, the individual user is responsible for the information technology equipment and resources under his or her control.

5. Information Technology Standards and Guidelines

Confidentiality and Privacy

The University and all members of the University community are obligated to respect and protect confidential data. There are, however, technical and legal limitations on our ability to protect confidentiality. For legal purposes, electronic communications are no different than paper documents. Electronic communications are, however, more likely to leave a trail of inadvertent copies and to be seen in the course of routine maintenance of computer systems.

The University may permit incidental personal use of computer resources. The University does not monitor the content of personal Web pages, email or other online communications. However, the University reserves the right to examine computer records or monitor activities of individual computer users (a) to protect the integrity or security of the computing resources or protect the University from liability, (b) to investigate unusual or excessive activity, (c) to investigate apparent violations of law or university policy, and (d) as otherwise required by law or urgent circumstances. In limited circumstances, the university may be legally obligated to disclose information relating to business or personal use of the computer network to governmental authorities or, in the context of litigation, to other third parties.

Access

No one may access confidential records unless specifically authorized to do so. Authorized individuals may only use confidential records for authorized purposes. The University's Policy for the Responsible Use of Information Technology requires that members of the University community respect the privacy of others and their accounts, not access or intercept files or data of others without permission, and not use another person's password or access files under false identity. Violators of any of these rules are subject to discipline consistent with the general disciplinary provisions applicable to University personnel and students.

Passwords help protect against misuse by restricting use of University systems and networks to authorized users. Each authorized user is required to create a unique password that is to be protected by that individual and not shared with others, is difficult to crack, is changed on a regular basis, and is deleted when no longer authorized. Please check the guidelines in the University's Password Policy.

Information Technology Services will ensure that controls are in place to avoid unauthorized intrusion of systems and networks and to detect efforts at such intrusion. ITS may utilize systems that monitor these controls for unexpected conditions, anomalies, and successful and unsuccessful access to systems, networks, and applications, to ensure that only authorized users are connected to the network.

University controlled information systems will have access policies that define access rights and privileges and protects assets and data from loss or inappropriate disclosure by specifying acceptable use guidelines for users.

Management for each area will also ensure that administrative access procedures include provisions for alternative administrative access in the event that the primary access holder is incapacitated or otherwise unable to perform required administrative activities.
Access to controlled University systems will be granted by department management and documented using the University's Computer Account Request Form. Users will only be granted access to specific application functions as required by the position and approved by department management. The Computer Account Request Form must be signed by the Department Head, ITS Database Administrator, ITS Director of Enterprise Services, and ITS Executive Director for controlled system access approval.

Accountability

Individual users are responsible for ensuring that others do not use their system privileges. Users must take care in protecting their usernames and passwords from eavesdropping or careless misplacement. Passwords are never to be given to someone else. Individual users will be held responsible for any security violations associated with their usernames.

ITS staff is responsible for reviewing the audit logs and identifying potential security violations. The ITS staff is responsible for establishing the security and access control mechanisms (such as usernames, passwords, logging, etc.) and may be held accountable for any security breaches that arise from improper configuration of these mechanisms.

Each user permitted to access a controlled system is to be made aware of the access policy for that system. Management will provide this information to the employee when first granting access and make the employee aware of the auditing capability in place to verify compliance.

All controlled systems must maintain audit logs to track usage information to a level appropriate for that system. All user sessions and all failed connection attempts must be logged. For user sessions, the following will be recorded: user, source IP, session start time/date, and session end time/date. For failed connection attempts, the number of attempts must also be recorded. Management has the discretion to determine whether additional logging is necessary.

Audit logging may also apply to networks. Logging of network traffic flow and access is a standard practice. If inappropriate use of the network is suspected, and management so requests, ITS may authorize specific traffic logging on portions of the campus network.

If University staff believes a security incident has occurred, they will immediately notify their management. Management will assess the potential implications of the incident, notify Information Technology Services, and take any remedial and necessary action. All audit logs will be immediately duplicated and moved to secure media for further analysis.

Before adding new software to University computers and networks, system defaults should be carefully reviewed for potential security holes and passwords shipped with the software should be changed. Downloading software, particularly software that is not job-related or endorsed by the administration, may introduce security risks and must be approved by ITS.

Authentication

Authentication and data encryption will be implemented for all systems that send or receive sensitive data or when it is critical that both parties know with whom they are communicating. The decision of whether to encrypt data should be made by the professional system administrator responsible for the particular application being distributed, with the knowledge of the appropriate dean, director, or department head.

Availability

Mission critical systems are expected to be available at all times except during published scheduled maintenance periods. An announcement will be sent out to the University community in advance of any scheduled outages. Critical systems and networks are documented in the University's Disaster Recovery Plan which details redundancy and recovery procedures. It also includes contact information for reporting system outages.

Backup of data will be well-documented and tested. Details are outlined in the ITS Backup Policy. Backups of mission critical data are maintained in secure off site storage to guard against the impact of disasters.

Information Technology Systems and Network Maintenance

In the course of doing business, Information Technology Services and departments may contract for all or some system and network local or remote maintenance or support. Representatives of these contracted companies must follow all University policies.

Departments are expected to work with ITS in establishing appropriate guidelines for application, network, and system access. It is the responsibility of the contracting department to inform the contractor of all appropriate policies and, in addition, to provide oversight of the contractor and contractor representatives during the time they have access to university resources.

Reporting Violations

Owners or managers of computer, network or applications systems, as well as users of these systems, have the responsibility to report any apparent violations of law, university policy or department policy to local management and Information Technology Services whenever such violations come to their attention.

Owners and managers of department computing, network and applications systems shall make available to management and users of the systems guidelines for reporting security violations. These guidelines will provide specific guidance on what, when, where, to whom, and within what timeframe the violation should be reported and a copy will be filed with Information Technology Services.