General Information Technology Policy Information & Guidance

Introduction and Context

Academic Freedom is central to the mission of higher education. Therefore, the University of the Pacific respects and encourages the free exchange and debate of ideas, including electronic interchanges and all manner of electronic inquiry and publishing in a manner that complies with University policy and law. Within this context, the University provides access to Computing and Communications Resources to students, faculty, staff and other members of the University community to support the instruction, research and service missions of the University. Use of these resources should follow the same standards of common sense, courtesy, and restraint in the consumption of shared resources that govern the use of other University facilities and services.

The protection of confidential, sensitive, and proprietary information is critically important to the University. Therefore, it is essential that students, faculty, staff and administrators take steps to appropriately safeguard such information. Such safeguards must recognize University community members' rights of free speech, free inquiry and access to one's own information.

The University does not condone messages of hate, bigotry, violence or intimidation directed at any individual or group, or harassment of any kind. Allegations of such harassment or threats will be thoroughly investigated by the University. If such allegations are verified the University will take corrective pursuant to University policy.

The University is a non-profit, tax-exempt organization and, as such, is subject to a number of pieces of legislation regarding sources of income, political activities, use of property, etc. The University prohibits use of University information and information technology resources for partisan political activities, where such use is prohibited by laws and prohibits use for unauthorized commercial purposes.

The University operates a complex data processing environment and telecommunications network located in three cities in northern California. The use of modern information technology entails both benefit and risk. The Information Technology (IT) policies are designed to reduce those risks to an acceptable level and to maximize the benefits to all Users. Importantly, The IT policies are not intended to "lock down" the University's information resources and systems to authorized University users, but rather provide reasonable protection so that information can be shared appropriately and employed effectively in the pursuit of the University's goals. The IT policies will help ensure the confidentiality, integrity and availability of University information and information technology resources for all members of the University community.

Scope

The IT policies and their supporting documents apply to all users of the information technology environment at the University of the Pacific, including faculty, staff, students, contractors, vendors, business partners and other members of the University community. This group, for the purposes of The IT policies, is referred to as Users. For the purposes of The IT policies, the entirety of the University information technology environment and the information and data therein is referred to as Computing and Communications Resources. Computing and Communication Resources include, but are not limited to computers, networks, software, databases, information and records, services, facilities and access methods.

Sanctions

It is the responsibility of each User to understand his or her privileges and responsibilities under theses Information Technology Policies and to act accordingly. Users failing to abide by The IT policies may be subject to corrective action up to and including, dismissal, expulsion, and/or legal action by the University. While technical corrective action, including limiting user activity or removing information, may be taken in emergency situations by authorized Information

Technology staff, other corrective action, technical and/or non-technical, will be taken in accord with applicable University policies and procedures.

Exceptions

Exceptions to the IT policies will only be granted if an appropriate justification for the exception is approved and the person responsible for that area of information management, the appropriate Information Administrator, accepts the additional risk and/or responsibilities posed by the exception. To apply for an exception to an IT policy, the requestor will prepare a written request for the exception (email is acceptable), along with a justification, and deliver the request to their unit's head information technology official (if any) for consideration. That official, working with others as appropriate, will advise the requestor on alternatives that comply with policy. In any case, if compliance with policy cannot be secured at the unit level, the request should be forwarded to the Chief Information Officer (CIO). The CIO will work with the requestor, appropriate unit IT personnel and the Information Security Analyst (University IT Security Officer - see Roles and Responsibilities) to find an alternative that complies with current policy. If the matter cannot be promptly resolved to the satisfaction of all parties, the request for exception will be presented to the full Information Strategy and Policy Committee (ISPC) along with appropriate analysis by the University IT Security Officer and unit IT leadership. The ISPC is the final arbitrator of all exceptions to security policies. The University IT Security Officer will maintain a record of all exception requests, their resolution and any accompanying documentation. This record will be made available to the ISPC to assist in the review and revision process for The IT policies.

Roles and Responsibilities

Information Strategy and Policy Committee (ISPC)

6.3.4 Information Strategy and Policy Committee (ISPC) (J, U) Approved by Cabinet June 11, 2001, Approved by Academic Council September 13, 2001, Revised August 2002, Approved by Academic Council September 12, 2002. Revised by Cabinet December 6, 2004, revised and approved by Academic Council December 9, 2004, and revised and approved by Cabinet December 20, 2004. Revised by Cabinet May 5, 2006. Approved by Academic Council September 14, 2006.

The Information Strategy and Policy Committee (ISPC) is the primary body to advise the President on the strategic use of information. The committee works collaboratively with various administrative and faculty groups to facilitate the effective and efficient use of information in support of the University's mission and priorities.
The committee has the following responsibilities:

1. To recommend to the Cabinet institutional academic and administrative priorities involving the collection, safeguarding and use of institutional information as guided by the University's mission and priorities.
2. To recommend to the Cabinet institutional initiatives, including the required outcomes and resources, to utilize information to advance the above institutional priorities.
3. To recommend institutional policies on information, including information security policies and information technology policies, to the Cabinet and Academic Council for adoption.

The Committee includes the following members, appointed annually by the President as appropriate:

Provost, Chair
Academic Council Chair or Chair-Elect
[Faculty IT Committee, replacing TLC] Chair or Chair-Elect
Staff Advisory Council Chair or Chair-Elect
One representative from the Division of Business and Finance nominated by the Vice President for Business and Finance

One representative from the Division of Student Life nominated by the Vice President for Student Life
One representative from the Division of University Advancement nominated by the Vice President for University Advancement
One representative from the Dugoni School of Dentistry, other than staff directly responsible for IT, nominated by the School Dean
One representative from the McGeorge School of Law, other than staff directly responsible for IT, nominated by the School Dean
ASUOP President or Vice President
Associate Provost/Chief Information Officer, non-voting, ex-officio
Assistant Provost for Planning, non-voting, ex-officio

Appointments are made annually by the President. The Provost chairs the Committee. The Committee reports as appropriate through unit representatives to their units.

Information Security Analyst / University IT Security Officer

The University, through the CIO and with concurrence of the ISPC, will designate a person as the University Information Security Analyst (ISA) or University Security Officer. For the execution of ISA duties, the Information Security Analyst reports directly to the Chief Information Officer. This person will be responsible for developing, deploying, maintaining and evolving the security architecture, processes and procedures, and providing advice on the development of security standards for the University. In doing so, consistency with the broad policy objectives laid out by the ISPC along with an understanding of the changing security risks faced by the University will be maintained. In this capacity, the ISA must continually develop and maintain both his/her own security skills as well as those of other security staff so they can expertly evaluate new security threats to the University and develop countermeasures when appropriate. The ISA is the security advisor and consultant for the University but has no direct control over academic or administrative systems. The ISA should be able to provide all University academic and business units with security risk assessments and provide, or assist with, the development and deployment of protective measures. It is the responsibility of the ISA to monitor University-wide security tools, investigate breaches of security controls in a timely manner, and report findings to the Chief Information Officer (CIO) and the appropriate head information technology official in the relevant school or administrative unit. Major security issues or incidents with policy implications will be brought to the attention of the ISPC. The ISA will maintain a record of all Information Technologies Policies exception requests, their resolution and any accompanying documentation. The ISA is furthermore charged with the ongoing education of the University's users to keep them aware of and compliant with security requirements.

Security Administrator / Systems Administrator

A Security Administrator (SA) is any University User who owns a userID that allows that individual to administer security controls, userIDs, access rights or information access for others. Security administrators have the responsibility to review and ensure the currency of the access rights associated with Information Administrator's information assets, and, as appropriate, implement security requirements, access criteria, backup/restore procedures, disaster recovery and business continuity requirements for information assets.

Information Administrator (Data Steward)

An Information Administrator (IA) or Data Steward is a university executive, unit manager, administrative or academic program head or other faculty member who is responsible for a University information resource. In general, stewardship of a University Information resource involves a number of responsibilities, some of which are listed below. Because this list is wide ranging and several items may require special skills or inordinate amounts of time on details, it is expected that the IA may, as appropriate, delegate some or all of the tasks to others. The point of this section is to clarify that Information Administrators have certain responsibilities and need to see that action is taken commensurate with those responsibilities.

IA responsibilities include, but are not limited to:

Maintain compliance with security policies and standards in coordination with the Information Security Analyst,
Establish the initial data classifications (refer to Policy #3 of this document for definitions) and periodically review data classifications to ensure they meet academic and administrative needs,
Ensure security controls are in place commensurate with data classifications,
Provide information as needed to facilitate review of, and ensure currency of, the access rights associated with the Information Administrator's information assets, determine security requirements, access criteria, backup/restore, disaster recovery and business continuity requirements for their information assets,
Sponsor changes to existing applications or new applications to meet academic or administrative needs of the work unit or academic department,
Perform or delegate the following within the same academic or administrative unit:

a. Approve access requests received from other academic and administrative units. If this approval authority is delegated to another individual, he/she should be in the same academic department or administrative unit as the Information Administrator,
b. Approve the disclosure of information,
c. Take action in response to notifications received concerning security violations against the information assets they own.

Information Broker

An Information Broker obtains data from various data sources and transforms them into information. The Broker adds value by using structured procedures to give the raw data meaning in the context of the University needs. The Broker works with Information Administrators and Users to maintain and share a model of the data elements. The Broker also helps to anticipate and respond to Users' changing information needs. The Brokers are responsible for the security of the information entrusted to their care and maintaining compliance with security policies and standards by coordinating with the Information Security Analyst.

Information User

Any User of Computing and Communication Resources who is authorized by the University to use or access University information resources managed by an IA. All Users have a responsibility to adhere to the University Acceptable Use Policy and all other applicable IT Policies. Information Users exercise, as a requirement of their authorization and/or job, exceptional care in their use and stewardship of restricted access and confidential information.