



# **Information Technology Policies**

Version 12.0  
11/1/09

# INDEX

<b>GENERAL INFORMATION.....</b>	<b>4</b>
INTRODUCTION AND CONTEXT.....	4
ISSUING AUTHORITY .....	4
SCOPE.....	4
SANCTIONS.....	5
EXCEPTIONS .....	5
ABOUT THIS DOCUMENT.....	5
REVISIONS.....	5
<b>INFORMATION TECHNOLOGY POLICIES – SUMMARY .....</b>	<b>6</b>
<b>ROLES AND RESPONSIBILITIES .....</b>	<b>7</b>
INFORMATION STRATEGY AND POLICY COMMITTEE (ISPC) .....	7
INFORMATION SECURITY ANALYST / UNIVERSITY IT SECURITY OFFICER .....	7
SECURITY ADMINISTRATOR / SYSTEMS ADMINISTRATOR .....	8
<b>ENTERPRISE INFORMATION MANAGEMENT ORGANIZATION.....</b>	<b>9</b>
INFORMATION ADMINISTRATOR (DATA STEWARD) .....	9
INFORMATION BROKER .....	9
INFORMATION USER.....	9
<b>INFORMATION TECHNOLOGY POLICIES .....</b>	<b>10</b>
1. INFORMATION SECURITY POLICY .....	10
<i>Issues Addressed.....</i>	<i>10</i>
2. ACCOUNTABILITY POLICY.....	11
<i>Issues Addressed.....</i>	<i>11</i>
3. INFORMATION MANAGEMENT POLICY .....	12
<i>Information Classifications .....</i>	<i>12</i>
1. <i>Public Information.....</i>	<i>12</i>
2. <i>Restricted Access Information .....</i>	<i>13</i>
3. <i>Confidential Information.....</i>	<i>13</i>
<i>Issues Addressed.....</i>	<i>14</i>
4. SEGREGATION OF SYSTEMS POLICY .....	15
<i>Issues Addressed.....</i>	<i>15</i>
5. ACCESS CONTROL POLICY .....	16
<i>Issues Addressed.....</i>	<i>16</i>
6. NETWORK ATTACHED SYSTEM SECURITY POLICY .....	17
<i>PURPOSE OF POLICY .....</i>	<i>17</i>
<i>SCOPE OF POLICY.....</i>	<i>17</i>
<i>EXCEPTIONS TO THE POLICY .....</i>	<i>18</i>
<i>RESPONSIBILITIES.....</i>	<i>18</i>
<i>NETWORK SECURITY .....</i>	<i>19</i>
7. ACCEPTABLE USE POLICY .....	21
A. <i>Support of the University’s Mission.....</i>	<i>21</i>
B. <i>Secure Use .....</i>	<i>21</i>
C. <i>Respectful Use.....</i>	<i>22</i>
D. <i>Cooperative Use .....</i>	<i>22</i>
E. <i>Sanctions.....</i>	<i>23</i>
8. ELECTRONIC MASS COMMUNICATIONS POLICY .....	24
3. <i>AUTHORIZATION FOR RESTRICTED MASS COMMUNICATIONS.....</i>	<i>25</i>
4. <i>RESTRICTED MASS COMMUNICATIONS GUIDELINES .....</i>	<i>25</i>
5. <i>MESSAGES FROM PACIFIC TO THE EXTERNAL COMMUNITY .....</i>	<i>25</i>
9. BUSINESS CONTINUITY PLANNING POLICY .....	27

<i>Issues Addressed</i> .....	27
10. REMOTE ACCESS POLICY .....	28
<i>Issues Addressed</i> .....	29
11. EXTERNAL TRUSTED NETWORK SECURITY POLICY .....	29
<i>Issues Addressed</i> .....	29
12. COMPUTING AND COMMUNICATIONS CONFIDENTIALITY POLICY .....	30
13. TELECOMMUTING POLICY .....	33
<i>Pacific Telecommuting Agreement</i> .....	35
14. NETWORK SCOPE OF SERVICE POLICY.....	43
15. TECHNOLOGY ACQUISITION COORDINATION POLICY .....	45
16. EMERGENCY NOTIFICATION POLICY .....	47
17. PRIVACY POLICY .....	50

## **General Information**

### ***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. These policies are designed to reduce those risks to an acceptable level and to maximize the benefits to all Users. Importantly, these 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. These policies will help ensure the confidentiality, integrity and availability of University information and information technology resources for all members of the University community.

### ***Issuing Authority***

President, University of the Pacific

### ***Scope***

These 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 these policies, is referred to as Users. For the purposes of these 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 these Information Technology Policies and to act accordingly. Users failing to abide by these 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 Information Technology 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 Information Technology 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 page 6) 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 these policies.

## **About this document**

This document is intended to be a framework for the inclusion of all University wide policies concerned with Information Technology, broadly written. This includes, Information Management, Information Administration, and IT Security Policies, amongst others. The name of this document is not intended to limit its scope of content or fully characterize that content. The Chief Information Officer serves as steward of this document. The actual policies that follow are in bold face following the word "**POLICY.**" All other text is provided to clarify the intent of the policies and provide critical and, sometimes, detailed guidance and/or direction to those who may implement or need to interpret the policies. In some cases, the explanatory material may set goals or courses of action in the spirit of the policy. These goals and directions may require continuing effort and, over time, significant resources. In summary, this document, its policies and explanatory material form an interrelated body of work that helps provide a context for the successful application of Information Technology to teaching, learning and administration.

## **Revisions**

The issuing authority may revise and/or amend these policies. The ISPC will institute a regular process for periodic review of these policies. Academic Council will review all policy changes prior to submission to the issuing authority. However, to keep applicability current, more frequent revisions to the explanatory material may be necessary. Revisions to the explanatory material will be reviewed and approved by the ISPC. The Academic Council and/or University legal counsel, as appropriate, will review any significant changes. Both policy and explanatory revisions will be communicated to the University community as appropriate.

## Information Technology Policies – SUMMARY

1. Information Security – Academic and business information resources are critical assets of the University and must be appropriately protected.
2. Accountability - Individual accountability must be maintained on all University computing and communications systems.
3. Information Management - All University information must have an associated Information Administrator (IA) who is responsible for its proper management and security, including its appropriate classification.
4. Segregation of Systems - University systems, applications, and databases designated for student or public use must be physically and/or logically isolated from systems used for normal administrative activities as appropriate to ensure system and data integrity.
5. Access Control - The integrity, confidentiality and availability of the University's information resources will be protected by logical and physical access control mechanisms commensurate with the value, sensitivity, risk of loss or compromise and ease of recovery of these resources.
6. Network Attached System Security Policy - The University will take all prudent and reasonable measures to secure the systems that are attached directly to its internal network and indirectly to the external Internet.
7. Acceptable Use - The University's Computing and Communications Resources shall be used securely, respectfully, cooperatively in support of the University's Mission.
8. Electronic Mass Communications - Members of the University community are encouraged to use email, the web and other forms of electronic mass communication to facilitate the efficient and effective presentation and delivery of information.
9. Business Continuity Planning - Each academic department or administrative unit that provides critical services based on information technology will document, develop, implement, and periodically test continuity plans.
10. Remote Access - Remote access to University systems and information will be appropriately provisioned and/or controlled to ensure required security.
11. External Trusted Network Security – The University will not implement any dedicated connection between the University's network and the network of an external entity prior to conducting a formal risk assessment.
12. Computing and Communications Confidentiality - The University will treat all of its individual User information, User activity, and User communications as Confidential Information as defined in its Information Management Policy.
13. Telecommuting Policy - University of the Pacific supports properly managed telecommuting where there are mutual benefits to the University and the employee and may require it in exceptional situations.
14. Network Scope of Service Policy - The University is not a public Internet Service Provider, operates a private secure network solely for the benefit of its user community, including authenticated guests, for activities aligned with the mission of the university and does not provide its network services to those outside this community.
15. Technology Acquisition Coordination Policy - All significant purchases, leases, gifts, loans, renewals and contracts for new, used or upgraded Information Technology goods, services and implementations, shall occur in coordination with the Office of Information Technology in a timely manner across the schools and campuses.

## **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 Organization

### ***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.

# **Enterprise Information Management Organization**

## ***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 Information Technology 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.

# Information Technology Policies

## 1. *Information Security Policy*

**POLICY: Academic and business information resources are critical assets of the University and must be appropriately protected.**

Any person who uses or provides information resources has a responsibility to appropriately maintain and safeguard these assets. This policy is designed to protect both information stored on or accessed through University Computing and Communication Resources and those resources themselves. These resources include information resources and intellectual property owned by others whose rights must also be protected.

Information security is the protection of data against accidental or malicious destruction, modification or unauthorized disclosure. Information will be protected based on its value, confidentiality, and/or sensitivity to the University and the risk of loss or compromise. Information security management enables information to be shared while ensuring protection of that information and its associated computing and communications assets. The University is responsible for ensuring appropriate controls are in place to preserve these security objectives.

Information is useless if it cannot be accessed and/or used to advance the academic and business interests of the University. Therefore Information security also involves guarding against unauthorized withholding (e.g., denial of service).

The University has a multitude of points of access to its data – dozens of departments and three campuses. Because numerous administrative units and academic departments are responsible for the processing and storage of information, each is also the steward of significant information assets owned by the University. The University relies upon each campus, department and individual system administrator to preserve and protect those assets in an appropriate, consistent and reliable manner. Security controls provide the necessary physical, logical and procedural safeguards to accomplish those goals.

### Issues Addressed

This policy addresses the need to make users and providers of information aware that they have a responsibility to appropriately safeguard the University's information assets as they would other resources. The unauthorized disclosure, destruction or prolonged unavailability of the University's information or information technology could harm the University, its students, its employees and other members of the University community.

## 2. **Accountability Policy**

**POLICY: Individual accountability must be maintained on all University computing and communications systems.**

A University Computer System is defined for the purposes of this and other Information Technology Policies as any University-provided computer, workstation or server – either stand alone or networked – that processes, stores, receives or transmits University information, or information entrusted to the University by a third party. In general, access to University Computer Systems and networks is provided through the use of individually assigned unique computer identifiers, known as userIDs. Each individual is responsible and accountable for all activity performed under his/her userID(s). The ISPC has the authority to grant exceptions and define the accountability mechanism for those computer systems whose access and use cannot reasonably be controlled through use of an individual userID.

Access to protected resources is granted to userIDs. This access is based on an individual userID, or to a groupID containing individual userIDs. Group-IDs are commonly used in role-based security models. It is, therefore, critically important that unique userIDs be assigned to specific individuals, and that these userIDs not be shared ensuring that the controls in place perform as they are intended. This will ensure the accountability of all individuals accessing the University's protected resources.

UserID based accountability should be required for any network-based service, but may be impractical for non-networked, public access, or kiosk-type installations. In private areas (research laboratories, faculty offices, etc.), sign-on procedures to use non-networked services may interfere with normal operations. In non-networked situations such as these, regular audit of local information and/or appropriate physical access restrictions may be substituted for userID access. It is highly recommended that the Information Security Analyst be consulted.

### Issues Addressed

Accountability, is an element of security. By requiring each individual to sign on using a unique userID, activity can be attributed to a particular individual. This auditability provides management with information regarding who performed what activity on what information resources. It can also be used to help resolve system or network problems by providing more complete usage information.

### 3. **Information Management Policy**

**POLICY: All University information must have an associated Information Administrator (IA) who is responsible for its proper management and security, including its appropriate classification.**

Information, like other assets, must be properly managed during its lifecycle, from its creation, during authorized use, to proper disposal. As with other assets, not all information has the same use or value, and therefore requires different levels of protection. Just as it is unwise to underprotect a very sensitive document, it is expensive and wasteful to overprotect non-sensitive information. This policy is intended to require appropriate controls for the management of University information resources.

All information will have an Information Administrator (IA) established who will be responsible (perhaps through delegation) for assigning the initial information classification, and who will make all of the decisions (perhaps through delegation) regarding controls, access privileges of Users, retention requirements and daily decisions regarding information management pertaining to that particular information. The Information Security Analyst (ISA) can provide a periodic high-level impact analysis on the information to determine its relative value, risk of compromise, possible legal issues, etc. Based on common sense or the results of an assessment, information should be classified into one of the information classifications discussed below.

The classification will inform the Information Administrator and the Information Security Analyst, and help determine the appropriate level of protection of the information and its associated application software commensurate with the value of the information in that classification. It is important that controls be designed and implemented for both the information and software. It is not sufficient to classify and control information alone. The software, and possibly the hardware, on which the information and/or software reside, must also have proportionate controls for the classification of information that the software manipulates. The Information Administrator is responsible for determining the classification of the information. Working with the Information Security Analyst and the application development team, appropriate controls for the information, software, and possibly the hardware must be developed.

#### Information Classifications

Information may be classified according to its value, sensitivity, or risk of loss or compromise. The Information Administrator, who may be advised by the Information Security Analyst, determines the classification levels. The classification level helps determine the degree of security standards to be applied and followed by the Information Administrators, Security Administrators, Information Brokers, and Information Users.

The three levels generally used to classify University information are:

Public Information  
Restricted Access Information  
Confidential Information

#### 1. **Public Information**

Public Information is any information prepared, owned, used or retained by the University for the purpose of public release and which is not specifically exempt from the disclosure requirements of law.

Generally, only documents specifically created for the public, (e.g., press releases, brochures), are considered public information. Release of “public” documents should not impair the University’s ability to fulfill its mission, nor should such release damage the reputation. All other information should be classified as Restricted Access or Confidential. Any unclassified information should be

assumed to be at least Restricted Access, and be accordingly protected until the proper information classification can be determined and verified.

Examples of Public Information could include but are not limited to:

Published University marketing brochures  
Published curriculum information  
Public notices of University public events such as concerts and sporting events  
Employment opportunity bulletins  
University approved Internet web site information

## 2. Restricted Access Information

The controlling factors for Restricted Access Information are those of confidentiality and integrity. This type of information requires protection from disclosure or alteration by unauthorized persons. Restricted Access Information is restricted to individuals who have been authorized for that information. In most cases access will be limited to specifically authorized University faculty, staff and students. This classification allows access by non-University users (such as prospective students or vendors) when authorized by the appropriate Information Administrator.

The sensitive nature of some types of Restricted Access information may be difficult to recognize because it is often integrated into daily work and/or course assignments or may be handled by a number of users. Other types of Restricted Access information may appear to be more obviously sensitive because they have a rather restricted audience. Either way, it is important to maintain the confidentiality and integrity of this information, regardless of whether it is maintained in a paper or electronic form.

Examples of Restricted Access Information could include but are not limited to:

University course materials, including on-line media where materials should be restricted rather than public \*\*.  
Extended education and online course materials \*\*.  
Prospective student status information accessible to that student.  
Administrative information exchanged with vendors using electronic protocols.  
Research studies being performed in association with other universities \*\*.  
Student and registration information accessible online to that student.  
University organizational charts and job descriptions.  
Approved and widely communicated University business plans.  
Curricula changes or graduation requirements prior to approval.  
University Policy or Procedure Manuals.  
Reports, files or working papers concerning daily academic and administrative activities \*\*.  
Financial statements prior to public announcement or release.  
Travel plans of University faculty or staff.  
Information pertaining to strategic business decisions such as college expansion, new academic programs being considered, etc.

\*\* This policy is to be interpreted to be consistent with the University's Intellectual Property Policy.

## 3. Confidential Information

Confidential Information is the strictest data classification used by the University and requires maximum control. Depending on the nature or contents of the Confidential Information, disclosure or alteration of this type of information could cause great harm to an employee, student or the University. Confidential Information requires safeguarding, either due to the requirements of law or because of the mandates of prudent and reasonable practices. Access to Confidential Information is limited to specifically authorized individuals of the University and denied to all others, unless and until directed by an officer of the University and upon advice of legal counsel of the University.

Examples of Confidential Information include but are not limited to:

Employee Medical Records

Student information such as grades, medical information, etc.

Student and employee Social Security Numbers

Payroll data

Administratively maintained employee data such as residence address information, employment history, performance reviews, etc.

Alumni and donor information.

Patient records.

## Issues Addressed

There is a need to establish management responsibility and accountability for University Information resources. Unauthorized release or alteration of Restricted Access or Confidential information could have many consequences, ranging from the mundane loss of productivity to extremely serious legal consequences. The compromise of any classified information has the potential to impair the University's ability to competently and efficiently implement its mission. Release or alteration of medical records could discredit the University's reputation.

#### **4. Segregation of Systems Policy**

**POLICY: - University systems, applications, and databases designated for student or public use must be physically and/or logically isolated from systems used for normal administrative activities as appropriate to ensure system and data integrity.**

It is the intent of this policy to enhance the University's information technology security environment by requiring, where possible, the segregation of systems used solely for administrative purposes from those used solely for academic, student or general public access. To the extent possible, systems designated for academic or public use should be hosted on different computer systems than those designated for administrative use only. The computing and communications environment should be architected to prevent accidental or intentional harm to the University's administrative production computing environment or the compromise of restricted or confidential University information. Firewalls or other similar devices should be used to further isolate administrative systems.

This policy is not intended to restrict appropriate access to information by legitimate users, especially web-based access. It is likewise not the intent of this policy to preclude systems that use (and even allow updating of) administrative data in public applications. The intent is to require consideration be given to possible security gains through system architecture. This policy will have the greatest impact on campus administrative systems and will have little to no effect on systems involving teaching and learning.

#### **Issues Addressed**

Academic and administrative systems face competing expectations that bear on security. On the one hand, there is an expectation of readily available information. On the other hand, confidentiality of personal information requires the highest level of protection of systems from unauthorized or inappropriate access. Standard security practice is to isolate administrative systems that primarily contain restricted and confidential information from those that primarily contain public information or are otherwise used in an academic setting.

## 5. **Access Control Policy**

**POLICY: The integrity, confidentiality and availability of the University's information resources will be protected by logical and physical access control mechanisms commensurate with the value, sensitivity, risk of loss or compromise and ease of recovery of these resources.**

Information Administrators are responsible for determining who should have access to protected information resources within their jurisdiction, and what type of access privileges will be granted. These access privileges should be granted in accordance with the User's role or assigned responsibilities. Information Administrators must direct their Security Administrator(s) to grant the appropriate access privileges. Likewise, it is incumbent upon the User's manager and/or the Information Administrator to direct the Security Administrator to remove access to information resources when a User's need no longer exists or their privilege ends. Access privileges generally involve the ability to view data, create new data, change existing data, delete data and/or run programs against data.

Physical access to data centers, wiring closets, and servers containing Restricted Access or Confidential Information must be physically secured from unauthorized access. Servers containing Public Information should be appropriately secured.

### **Issues Addressed**

Access control is the primary means by which security objectives of the University are achieved. Access control mechanisms are designed and implemented to reduce unauthorized access to acceptable risk levels. The compromise of any sensitive information resource has the potential to impede the University's ability to competently and efficiently achieve its mission.

## **6. Network Attached System Security Policy**

**POLICY: The University will take all prudent and reasonable measures to secure PacificNet and the systems that are attached directly to it and indirectly to the external Internet.**

*Note that the line above is University Institutional Policy and that what follows is University Operational Policy. Both are approved by the Information Strategy and Policy Committee (ISPC).*

### **PURPOSE OF POLICY**

The internal data network and the external Internet are tremendously powerful tools in academia, facilitating the free exchange of ideas and instant access to a wealth of information. Likewise they are excellent business tools empowering University employees to gather information, improve internal and external communications, and increase efficiency in its business relationships.

It is the purpose of this Policy to protect the network of information technology and communication systems of the University from accidental, intentional or unauthorized access, damage, hackers, viruses and other threats. This protection is essential to serving two goals. It preserves the integrity of the Network itself while at the same time maintaining and nurturing open access to information for Pacific community important to the pursuits of a vibrant academic culture. In addition, this Policy aims at providing network security that complies with Federal, State and Local law, protecting the University from all forms of liability, protecting the confidentiality of the information of users, and ensuring academic freedom. It is also the purpose of this Policy to provide a detailed framework for the development of Network Security Standards that are consistent with this policy and the mission and priorities of the University.

Pacific provides a network of information technology to ensure an effective information infrastructure that supports the mission of the University with respect to teaching, learning, research and administration. The University network is however vulnerable to attack, improper use, viruses and other forms of interferences with potential crippling effects on the network, users and data. The specific purpose of this policy is therefore to provide reasonable network security that protects the network, the University, and users while at the same time promoting the mission of the University. Pursuant to the mission of the University, no network security system should exceed what is reasonably necessary to provide adequate protection in accordance with this policy. The implementation of this policy should not unreasonably interfere with the basic or essential functions or needs of the different units, colleges or and schools of the University. Given that the information technology needs of the different units, campuses and schools differ, any Network Security Standards must be developed in consultation, cooperation and collaboration with the information technology Administrators of these units.

### **SCOPE OF POLICY**

Except as otherwise herein stated, this policy applies to the following:

1. Any person who attaches any computer or electronic device to the network.
2. All university computers and electronic devices attached or connected directly, indirectly, remotely or by any other means to the network.
3. All individually owned computers and electronic devices that are attached directly, indirectly, remotely or by any other means to the network.
4. All other computers or electronic devices of whatever description and irrespective of their relationship to any person if any connection whatsoever to or with the network is sought.

## EXCEPTIONS TO THE POLICY

This network security policy does not apply to the following:

1. Individually owned computers, devices or individual network systems of faculty, students, staff or other users who opt not to be attached to or otherwise linked directly or indirectly to the University network. No implementation of this Policy should interfere with the freedom of such users to communicate, by means of an independent connection to the Internet, with the University, users or devices attached to the network.

2. Individually owned computers or other electronic devices for which temporary access to the network is sought if such computers or electronic devices are determined by the Systems/Security Administrators to be at current OS patch levels and have adequate up-to-date anti virus software. Temporary access is defined as 24 hours or less.

3. Laptops and other devices brought by visiting scholars, conference attendees and other temporary visitors to Pacific who cannot be presumed to comply with established Security Standards. The Systems/Security must develop an appropriate secured environment in order to provide access to the University network for such visitors.

4. Any other device that cannot meet the established Security Standards if the Systems/Security can provide a reasonable and cost-effective alternate secured environment for connectivity.

## RESPONSIBILITIES

1. The Academic Council (from the General IT policies) shall have the responsibility for approving all Information Technology Policies, amendments or the modifications of such Policies. Note that Security Standards are operational procedures and not policy. Also note that all institutional policies, including IT policies, are approved by Cabinet as they affect the entire University, not simply the Academic Division.

2. The Information Strategies and Policies Committee (ISPC) shall have the responsibility for developing and/or approving Network Security Policies and the necessary implementing Network Security Standards. It is also the responsibility of the ISPC to ensure that Network Security Standards do not unreasonably interfere with smooth and effective functioning of the different units, campuses or schools of the University.

3. It is the responsibility of OIT, the Systems/Security Administrators and Information Security Analyst (University Information Security Officer) to implement Network Security Standards after consultation with affected groups and hearings, as appropriate, with the Academic Council. Note that it is OIT and the CIO that are held accountable by the University for network security.

4. The Chief Information Officer, working through the University Information Security Officer, shall have the ultimate responsibility for ensuring compliance with the IT Policies including the Network Security Standards.

5. Faculty, Staff, Students and other authorized Users are prohibited from attempting to circumvent or subvert any measures adopted pursuant to this policy and the Network Security Standards. Users have the responsibility of complying with this policy and its implementation.

## NETWORK SECURITY

**1) Network Security Standards (Security Standards) to be established by the ISPC.** The Information Security Analyst (University Information Security Officer) will propose and maintain a set of Network Security Standards for servers, desktops, laptops and other devices that may be connected to PacificNet. These standards will derive from best IT security practice, carefully balance the need for security with the need for openness and transparency in an academic environment and be approved by the Information Strategies and Policies Committee (ISPC). Should the tension between openness and security in specific situations be irresolvable at the technical level, the ISPC will make a general policy revision or a specific exception.

It is the responsibility of the Systems/Security Administrators to see that Security Standards are maintained on systems that they are charged to oversee. The Security Standards can be found at [www.pacific.edu/securitystandards](http://www.pacific.edu/securitystandards). Non-conforming systems will not be provided network access based solely on financial hardship. .

**2) Scope of the Network Security Standards.** Notwithstanding any requirements or limitations imposed by this policy on the Network Security Standards the following are prohibited:

**a)** Unauthorized scanning of any network connected device beyond checking for compliance with vulnerability and Network Security Standards.

**b)** Unauthorized access to personal files, confidential and other protected data or unauthorized, scanning, monitoring, copying or spying on files on any computer or any network connected device of the University, faculty, students, staff or other authorized users. See the Computing and Communications Confidentiality Policy for details.

**3) Compliance.** The Chief Information Officer, working through the University Information Security Officer, must establish procedures for ensuring compliance with these provisions by Information Technology Administrators responsible for carrying out this policy. Systems, including PCs (user laptops and desktops), that do not conform to Pacific's security standards may be prohibited from full access to PacificNet and/or may be provided a class of service that appears to be technically outside of PacificNet.

**4) Removal.** Except as indicated above, systems, including PCs (user laptops and desktops), that do not conform to Pacific's Security Standards and/or encounter security issues may be taken off PacificNet or have their access limited without prior notice. Compliance may be periodically assessed using ISPC approved methods and any systems deemed in a state of non-compliance may be removed from PacificNet. No detection of a disruptive Network connected device or a device that fails to meet the Network Security Standards through a vulnerability scan shall justify any actions prohibited by University Policy.

**5) Intrusions.** If for any reason whatsoever a Network connected device is intruded in a manner prohibited by University IT Policy, the user must be notified as soon as possible and all technically feasible steps must be taken by the Information Administrators to identify the intruder and/or the source of such intrusion. Appropriate University disciplinary measures may be taken if the intruder is a Pacific user or Administrator. Disciplinary measures are addressed in the General Information section of these University IT polices under Sanctions and in the Acceptable Use Policy under Sanctions.

**6) Prior Security Review required before attachment.** All systems, iP enabled hardware and computers (not including end-user computers, i.e. laptops and desktops) must undergo a Security

Review by the University Information Security Officer before being attached to PacificNet. This is an audit requirement.

**Definition:**

Security Review: A review of matters at hand, looking at best security practice and established security standards. The Information Security Analyst (University Information Security Officer), and/or his/her designee, conducts the review. Such reviews may include, but are not limited to:

Contract review – determine confidentiality & privacy requirements (if applicable)

Application process review - application identification, trust identification, data flow

Data classification review - confidential, restricted access, or public

Risk assessment review – impact on the campus of going forward or not going forward

Security configuration review – check relative to established security benchmarks

Access controls review – check against audit requirements

Network services identification - port scan to determine firewall configurations

Vulnerability Identification - vulnerability scan against known attack vectors

Remediation planning – Helping remove the barriers to going forward

## 7. **Acceptable Use Policy**

Revision approved by Academic Council, February 8, 2007, Administration, March 19, 2007

**POLICY: The University's Computing and Communications Resources shall be used securely, respectfully, cooperatively in support of the University's Mission.**

**Definition:** *Computing and Communications Resources* include all electronic technology used to store, copy, transmit, or disseminate visual, auditory, and electronic information as well as the information contained therein. This includes, but is not limited to, computers, networks, phones, fax machines, copiers, PDAs, cell phones and the information contained in them.

### A. Support of the University's Mission

The University provides Computing and Communications Resources to faculty, students, staff and others solely for the purposes of supporting teaching, learning, scholarship, service and administration within the context of the University's mission.

1. 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 University Computing and Communications Resources for commercial purposes or financial gain not authorized under University Policy, partisan political activities not part of a class assignment, and for any activity prohibited by law.
2. Incidental personal use of Computing and Communications Resources, within the guidelines of this policy, is considered appropriate. Such permissible incidental personal use does not include hosting, ASP (Application Service Provider), ISP (Internet Service Provider), WSP (Wireless Service Provider) or other services for third parties. Incidental personal use does not include activities for financial gain unless such activities are authorized under University Policy. Incidental personal use does not include the use of institutional data which may be contained in or extracted from institutional computing and communications systems. Personal use is not incidental if it incurs a direct cost to the University.
3. Use of Pacific's Computing and Communications Resources by students, living on campus, in support of approved experiential learning and/or in support of their duties as compensated employees is explicitly authorized, so long as such usage does not violate any part of this policy.

### B. Secure Use

Users of University Computing and Communications Resources are responsible for taking appropriate steps to safeguard University and personal information, as well as University facilities and services.

1. Passwords and other authentication and authorization codes, cards or tokens assigned to individuals must not be shared with others. Authorized Users must not provide access to unauthorized users. Passwords should be chosen carefully to lessen the possibility of compromise. Users are responsible for all activity that takes place under their UserID(s).
2. Activity that may compromise the system integrity or security of any on or off-campus system is prohibited. This includes any type of unauthorized access or hacking.

3. Unauthorized monitoring of individual User activity, information and communications is prohibited. See the University's Computing and Communications Confidentiality Policy.
4. Users must ensure the security of restricted, confidential, proprietary, licensed, copyrighted or sensitive information entrusted to their care or that may come into their possession. Security includes, as appropriate, protection from unauthorized disclosure, modification, copying, destruction or prolonged unavailability. Unless approved by the University Security Officer, users must not store non-university personal identification numbers including, but not limited to, Social Security Numbers, Credit Card Numbers, or Drivers License Numbers on unsecured devices or media, for any period of time.

### C. Respectful Use

University Computing and Communications Resources should be used in a manner that respects the rights of others.

1. Users must abide by all local, state and federal laws. This includes all applicable Copyright laws and license agreements, especially software license agreements.
2. Users must abide by the University's Policy Against Sexual and Other Unlawful Harassment. That Policy prohibits verbal and visual conduct of a harassing nature. Threatening, obscene or other offensive messages or graphics that would be deemed inappropriate in other contexts are prohibited.
3. Users must not attempt to represent themselves as someone else, mask their identity, or engage in computing or communication activities using another User's UserID or other electronic credentials. Use of University resources for illegal conduct is prohibited.
4. Users accessing off-campus systems must additionally abide by the rules, regulations and acceptable use policies of those external systems. Given that User action may reflect on the University or the User themselves, ethical behavior, courtesy, civility and good etiquette is highly recommended.
5. Users are prohibited from using the logos, word marks or other official symbols of The University of the Pacific without authorization from Pacific's Marketing and University Relations. This specifically includes any such usage in connection with electronic systems, services and communications, both internal and external. This does not include the usage on physical or electronic letterhead when used for official University business.

### D. Cooperative Use

Users of University Computing and Communications Resources are expected to cooperate so that all Users may make maximum use of facilities and services in a shared environment.

1. The University provides Computing and Communications Resources to facilitate business and academic activities of the University. Incidental personal use must not interfere with University business and academic activities. This includes personal activities that use bandwidth, occupy storage space, or slow down processing of systems, networks, or other resources needed for University business and academic activities.
2. Users must not knowingly engage in activities that would impede the activities of others including the internal or external distribution of junk email (a.k.a. Spam),

chain mail, viruses, worms, remote controllers or other malicious code, or other unofficial and/or unsolicited distributions, especially to persons you do not know.

3. Users should refrain from using sounds or visuals that may be disruptive to others in shared facilities.
4. Users may not connect any device to PacificNet or the phone system that compromises security or impacts performance for others. This includes, but is not limited to, the connection of wireless access points, switches, hubs, routers, or auto dialers, not authorized by the Office of Information Technology.
5. All Users share the responsibility of seeing that University Computing and Communications Resources are used securely, respectfully, cooperatively, ethically, and for their intended purposes. If policy questions arise or if suspected policy violations are encountered, Users should take no unilateral action, but must promptly notify and/or cooperate with the appropriate University officials. Contact [ITsecurity@pacific.edu](mailto:ITsecurity@pacific.edu)

## E. Sanctions

It is the responsibility of each User to understand his or her privileges and responsibilities regarding Acceptable Use and to act accordingly. Users failing to abide by the University's Acceptable Use Policy (AUP) 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. In particular, students who violate this policy will be referred to Judicial Affairs for judicial review.

## 8. **Electronic Mass Communications Policy**

Revisions approved by Administration, Nov 12, 2007

**POLICY: Members of the University community are encouraged to use email, the web and other forms of electronic mass communication, within established guidelines, to facilitate the efficient and effective presentation and delivery of information.**

*Note that the line above is University Institutional Policy and that what follows is University Operational Policy. Both are approved by the Information Strategy and Policy Committee (ISPC).*

### 1. DEFINITIONS

University Community – all members, of the following groups: faculty, staff and any other employees, students, emeriti faculty, alumni, donors and prospective students.

All – ‘All’ in what follows means all or a significant portion or segment of the indicated group. It is not confined simply to mean ‘each and every one.’

Mass Communications – The sending of communiqués, especially email, to All members of a group or multiple groups

Open Mass Communication – Mass Communications within one’s administrative domain. This includes faculty sending communications to their classes, administrators sending to their employees, schools sending to their faculty, staff or students. Open Mass Communication does not require authorization beyond that imposed by the policy and procedure within individual units, if any.

Restricted Mass Communication – Mass Communication across community or administrative domains. For example, all students at Pacific (not all students at Law) or all faculty at Stockton (not all faculty in the College), all staff of Pacific (not just all staff at Dental).

Institutional Spam – Unauthorized and/or inappropriate Mass Communications.

### 2. BACKGROUND

The University community is encouraged, where appropriate, to move away from paper based communications and utilize electronic communications. There is a rising need to be more efficient and effective with internal communications and a rising need to deliver more and higher quality information to virtually everyone encountering the University.

The University also recognizes the sensitivity of our community to receiving unsolicited email, institutional spam. However, the University, from time to time, has academic, business and emergency needs that require Mass Communications.

Finally, the evolving security and legal landscape require Pacific to communicate with care.

### 3. AUTHORIZATION FOR RESTRICTED MASS COMMUNICATIONS

See definition above for Restricted Mass Communications. Note especially that Open Mass Communication as defined above does not require authorization beyond that imposed, if any, by the individual units

#### Communications to All Campuses

Entire Community – Executive Assistant to the President or Vice President working on behalf of the University President

#### Communications to the Stockton Campus and selected mailings affecting all three campuses:

All Students – Any Cabinet member

All Staff/Employees – Director of Human Resources or the VP for Business & Finance

All Faculty – Provost

All Alumni – Director of Alumni Relations

All Prospective Students – Associate Provost, Office of Enrollment

Within the Guidelines below, the Office of Marketing and University relations operates under a general authorization to 1)perform mass electronic communications as it deems necessary and 2) to act as a proxy for any group desiring such communications.

### 4. RESTRICTED MASS COMMUNICATIONS GUIDELINES

a.) No routine restricted mass communications. Communications broadcast to all these groups should not be routine. Information should be critical and time sensitive. Information that is not critical, not time sensitive or not germane to the University’s mission, should be sent to Marketing and University Relations for inclusion in E-news, entry on the web or other similar unit or institutionally based communication vehicles. E-news is received by voluntary subscription. It is presumed that within an organizational unit, sending of inter group messages not relative to the mission of the University will be regulated by the corresponding management.

b.) No email spamming the community. Communications broadcast to all these groups must specifically apply to all or the vast majority of recipients as a “need to know.” For example, a United Way Campaign. Mass email communication to generate interest in niche issues or limited interest issues, like a trip to another country by a club, is specifically prohibited. Information that is not universally required should be sent to Marketing and University Relations for inclusion in E-news, entry on the web or other similar communication vehicles.

### 5. MESSAGES FROM PACIFIC TO THE EXTERNAL COMMUNITY

a.) Messages must conform to the CAN-SPAN Act.

It is generally a poor practice to send unsolicited email to anyone inside or outside the community, but especially if there is not an existing relationship with Pacific. However, whether the mail is solicited or un-solicited, pre-existing relationship or not, if it is sent to the external community, it must comply with the CAN-SPAM act.

[Source Wikipedia] The CAN-SPAM Act of 2003 (15 U.S.C. 7701, et seq., Public Law No. 108-187, was S.877 of the 108th Congress), signed into law by President Bush on December 16, 2003, establishes the United States' first national standards for the sending of commercial e-mail and requires the Federal Trade Commission (FTC) to enforce its provisions. The acronym CAN-SPAM derives from the bill's full name: Controlling the Assault of Non-Solicited Pornography And Marketing Act of 2003

CAN-SPAM defines spam as "any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service (including content on an Internet website operated for a commercial purpose)." It exempts "transactional or relationship messages." [...]

The bill permits e-mail marketers to send unsolicited commercial e-mail as long as it contains all of the following:

- 1) an opt-out mechanism;
- 2) a valid subject line and header (routing) information;
- 3) the legitimate physical address of the mailer; and
- 4) a label if the content is adult.
- 5) The content is exempt if it consists of:
  - a) religious messages;
  - b) content that broadly complies with the marketing mechanisms specified in the law [...]

If a user opts out, a sender has ten days to cease sending spam but they are not required to remove the address. The legislation also prohibits the sale or other transfer of an e-mail address after an opt-out request. [...]

b.) Messages from Pacific to the external Community should, if possible and appropriate, be sent by a third party.

Even if such mass mailings conform to the CAN-SPAM act, the University risks being black-listed if recipients see what Pacific sends as SPAM. If a third party is used for a mass communication, a sample copy should be sent to an on-campus address for quality control and data retention purposes.

c.) Distribution lists should be used. Mass email lists should not be built on the email system itself, but rather using an email exploder service. A distribution list service is currently available from the Office of Information Technology (OIT) for bulk email using moderated/unmoderated and open/closed discussion lists. However, this section is not to be construed as suggesting the construction of distribution lists exempts one from this policy. It does not.

d.) Anti-phishing steps must be taken. Mass internal or external communications that lead the recipient to a web site that may ask for personally identifiable information must not provide a live URL linked to the sight. Such communications should simply advise the recipient to visit the site. For example, "Your housing bill is ready. Please visit your account through insidePacific."

## 6. VIOLATION OF THIS POLICY

If you believe an email you received from a Pacific.edu address may violate this policy, please send it to the IT Security Officer, ITsecurity@pacific.edu. Continued violation of this University Policy may result in suspension of email privileges, pending a full investigation.

## 9. ***Business Continuity Planning Policy***

**POLICY: Each academic department or administrative unit that provides critical services based on information technology will document, develop, implement, and periodically test continuity plans.**

Continuity plans, also known as Business Continuity Plans, enable the critical academic and administrative functions of the University to continue in the event a local disaster renders a facility unusable or inaccessible for an extended period. This policy is intended to ensure that plans are in place that will, in turn, ensure that University Computing and Communications Resources are appropriately prepared to enable the University to continue to fulfill its mission and commitments. This policy applies to central systems and systems in the various units, including desktop computers that support key University functions.

Disaster recovery planning for Computing and Communications Resources is a part of overall business continuity planning. Business continuity may also involve alternative facilities, personnel or processes and may or may not involve information technology. In some cases, where information technology is not a critical part of ongoing activities, the loss of Computing and Communications Resources may involve only slight changes to the way academic or administrative functions are performed. In other cases, the University may have no practical alternative but total and rapid restoration of affected information technology resources.

Disaster recovery for Computing and Communications Resources involves, in part, making appropriate system and data backups, storing copies of critical information off site, and arranging for alternative and/or replacement resources, including systems and their associated operating facilities. It is expected that all University members, especially, Information Administrators and/or their designated Security Administrator, will ensure that systems under their stewardship are appropriately backed up and that back-up copies are appropriately stored in alternative locations. Recovery from backups must be tested from time to time, but at least annually. Critical information, as identified by the Information Administrators, should be backed up in such a manner as to be recoverable in a timely manner at an alternate operational facility. Business continuity plans ensure that mission critical activities, in this case, that use information technology, can continue. These plans should be tested at least annually.

It is recognized that rapid and simultaneous recovery of all systems and services may not be economically feasible, especially for all classes of disasters. Schools and major administrative departments will therefore provide for disaster recovery and business continuity within a given scope and duration, on a system-by-system basis, by priority; all determined jointly by the Information Administrators and, if appropriate, the ISPC. It is recognized that business continuity and disaster recovery plans and procedures are contingent on identifying specific requirements, receiving appropriate University resource prioritization and adequate funding. Those units that need assistance in developing continuity plans can work with OISR and/or their School's technology organization.

### **Issues Addressed**

The unavailability of critical information and systems would harm the University's ability to fulfill its mission.

## 10. **Remote Access Policy**

**Policy: Remote access to University systems and information will be appropriately provisioned and/or controlled to ensure required security.**

The teaching, learning and administrative environment of the University extends beyond the bounds of the campus and beyond the confines of the University's Intranet domain. Faculty, staff, students, and other Users must have the means to communicate and utilize University information resources from off-campus locations. In most cases, individuals desiring remote access to the University will do so through the Internet using the services of an Internet Service Provider (ISP). The expense and risk of acquiring this external channel for remote access is normally borne by the User.

Remote access security when using an ISP may be limited to secure protocols embodied in web browsers and University servers or may be a function of user installed encryption software. The University's perimeter firewall or other security devices may control certain types of remote access from the greater Internet. Even so, some on-campus systems may require further firewalls or similar devices to enhance their security when accessed remotely.

While secure web protocols may be sufficient for most access to sensitive information, some remote access activities may require greater levels of security between the University's most secure systems and a User's remote system. In these cases, Information Administrators, working with the Information Security Analyst, may require additional authentication, authorization and encryption software and/or hardware before authorization is granted to remotely access the information they steward. For example, a secure, authenticated and encrypted virtual private network (VPN) might be set up between the User's remote system and the University's secure network and/or systems. Information Administrators, the Information Security Analyst and those responsible for systems and services must take steps, where possible, to prohibit unauthorized remote access to information resources that require remote access authorization.

The University has, and will, architect its Computing and Communications Resources in a way that provides appropriate on campus system and network security. However, the security of that environment may be endangered by unauthorized connections to the University's trusted network or to systems attached to that network. Connections inside the campus firewall, for example, direct remote modem connection to campus servers or individual workstations are not permitted except by specific arrangement with the Information Security Analyst. These direct telephone connections create additional access points to the network and increase vulnerability to the entire University network. Concurrent connection of a workstation to the internal local area network and to a modem connection through the telephone system permits the "bridging" of networks and increases the possibility of security breaches. When there is a demonstrated need for direct connection to workstations or other systems on the University network, which cannot be met in any other way, the appropriate Security Administrator, will coordinate installation of the connection and/or appropriate software and ensure that the configuration and connection meets appropriate security requirements.

This policy is not intended to prohibit the use of on-campus wireless connections to the University Network. This policy is also not intended to prohibit the University from offering ISP services as appropriate to its mission. Should the University choose to offer such remote access services, the Information Security Analyst will work with others to insure such services meet appropriate security requirements. Note that the procedure for exceptions to this policy is detailed under "Exceptions", earlier in this document (see Table of Contents).

## Issues Addressed

Inappropriately controlled remote access to University Computing and Communications Resources represents a serious threat to the University's electronic information and networked systems.

### 11. ***External Trusted Network Security Policy***

**POLICY: The University will not implement any dedicated connection between the University's network and the network of an external entity prior to conducting a formal risk assessment.**

Extranets are dedicated networks connecting one trusted entity with another trusted entity. While extranets are extraordinarily powerful communications tools, they can represent very serious security exposures if the "trusted" partner's own security is lax. A trusted connection with another entity extends the University's network to include that entity and all of the security flaws that may be present in their network.

Formal risk assessments will provide the University administration with a better understanding of the level of additional risk involved in a trusted or semi-trusted connection to a partner organization. By identifying security weaknesses in a partner organization, the University can better identify protective measures it can take to preserve the security and integrity of the University's network, or determine that the connection simply is not worth the risk. Minimum acceptable security standards must be agreed upon in writing (through a contract or other instrument) prior to the connection being implemented. Note that it may be possible to make such a connection on the perimeter firewall and therefore accept no larger risk than connection to the general Internet.

A less-than-secure trusted partner poses an additional unique threat in that any unauthorized activity performed over the connection is difficult to investigate, as the University would not normally have the right to audit or monitor the partner's systems. The University could be placed in the compromising position of having to choose between depending on another organization to deduce the source of unauthorized activity, or shutting down a valuable business connection to that organization.

The Information Security Analyst can perform formal risk assessments unless he or she deems it necessary to bring in outside assistance. The project sponsors would cover the cost of external assistance unless otherwise arranged.

## Issues Addressed

The threats the University faces in maintaining a trusted connection to another organization with less than acceptable security standards are at least equivalent to the threats that the University would face were its own network that insecure (which it essentially becomes by extending trust to the other organization's facilities).

## 12. **Computing and Communications Confidentiality Policy**

Revisions approved by Administration, Nov 12, 2007

**POLICY: The University will treat all of its individual User information, User activity, and User communications as Confidential Information as defined in its Information Management Policy.**

*Note that the line above is University Institutional Policy and that what follows is University Operational Policy. Both are approved by the Information Strategy and Policy Committee (ISPC).*

### **Definitions:**

**Confidential information** – Confidential Information is defined by Pacific's Information Management Policy and repeated here for convenience:

Confidential Information is the strictest data classification used by the University and requires maximum control. Depending on the nature or contents of the Confidential Information, disclosure or alteration of this type of information could cause great harm to an employee, student or the University. Confidential Information requires safeguarding, either due to the requirements of law or because of the mandates of prudent and reasonable practices. Access to Confidential Information is limited to specifically authorized individuals of the University and denied to all others, unless and until directed by an officer of the University and upon advice of legal counsel of the University.

### **Ownership of Confidential Information:**

Confidential Institutional Information is owned by the University

Confidential Private Information is owned by the User.

**Computers** – this means desktop, laptop and all other computing hardware, media and communication devices or systems that can store data

### **Ownership of Computers:**

Institutional Computers are owned, leased or provided by the University

Private Computers are owned, leased or provided by the User.

**Privacy** – The expectation that Confidential Private Information will not be disclosed to anyone other than its owner.

**1) Users should not assume they are anonymous or have absolute protection from disclosure.** Modern communications and computing systems may monitor, record or maintain certain User information (like directory information or files), User activity (like web sites visited) and User communications (like Email) as a normal part of their operation. Authorized Security Administrators / Systems Administrators in the normal course of operations, maintenance or problem diagnosis may have access to User information, User activity and User communications. As a result of this normal maintenance activity, information, activity or communications discovered to be in potential violation of University policy may be discovered. This information will be disclosed to the appropriate University official(s) and may ultimately result in investigation and/or corrective action (as defined under Enforcement).

**2) Users should be aware that backups and copies of information may exist and may be retained for indeterminate periods of time, regardless of whether that information is 'deleted' by the User**

**3) The University will not routinely monitor User information, User activity or User communications without a user's consent. However, the University reserves the right to**

**investigate suspected violations of University Policies by monitoring or reviewing individual User information, User activity or User communications on any of its Institutional Computers.** Authorization for any such monitoring must be obtained in writing from both the Information Security Analyst (The Security Officer) and the Chief Information Officer. Such authorization will be done in concert with the appropriate University officials and/or University counsel. In general, authorization will not be given for purposes relating simply to employee performance. For example, accusations of excessive web surfing are a management issue, not an issue sufficient to warrant monitoring. In addition, monitoring requests from non-University entities, including law enforcement, must additionally be cleared through University counsel. Requests, in writing, by an individual to have their own information, activity and communications monitored can be honored by the appropriate system administrator and/or the Information Security Analyst.

**4) Emergency steps can be taken.** If in the judgment of the appropriate University officers or management, it is necessary to protect the integrity of its Computing and Communications Resources against unauthorized or improper usage, to protect authorized Users from the effects of unauthorized or improper usage under the University's Acceptable Use Policy, to provide for the security and/or safety of its community members, to assure university policy compliance, or otherwise to protect the fiscal or management integrity of the institution, the University (through its Security Administrators) reserves the right to restrict, or permanently limit, any User activity, to inspect, copy, remove or otherwise alter any information on Institutional Computers, to inspect, copy, or remove User communications on Institutional Computers and to do so without notice to the User.

Emergency action on Private Computers is limited to removal from the network unless the action is part of a legal process. As per the Sanctions (See Table of Contents) of these policies, in addition, technical action may be taken in emergency situations by authorized Information Technology staff, other corrective action, technical or non-technical, will be taken in accord with applicable University policies and procedures.

**5) Normal Human Resource and student judicial policies will be used for non-emergency cases of suspected policy violation.** Today, students, faculty and staff depend on information technology to perform their duties and meet expectations. If non-emergency IT policy infringement problems arise they must be resolved in a consistent manner and utilize established University investigative and disciplinary channels and procedures. The CIO and Information Security Analyst (Security Officer) will work with the appropriate general University officials and appropriate School or administrative unit officials in these matters. The Security Analyst may also address this process with incident response procedures.

**6) IT staff will not take unilateral action outside an emergency.** The intent of the previous two paragraphs is to insure that, except in an emergency, information technology staff members do not take unilateral action restricting user activity and/or action outside of established University processes. An emergency situation occurs when the integrity or security of systems is at stake, when a user's usage is seriously impacting the usage of others, or when the University has been placed in a position of immediate harm to its image or immediate legal liability. Simply having the potential for these conditions may be grounds for prompt process, but does not constitute an emergency. If a question arises about whether a situation is or is not an emergency, the Information Security Analyst and/or the CIO should be consulted.

**7) Users should be aware that the University has no control over the content of information servers on the external Internet and does not routinely monitor inbound traffic for content.** Please be informed that some information on or from the Internet may be personally offensive and/or unsuitable for certain audiences. User discretion is advised.

**8) Users of computers, even if the University provides them, are responsible for insuring that their systems are properly backed up and that the information contained therein is appropriately safeguarded to maintain security, confidentiality and policy compliance.** Viruses, Trojan horses, worms, password breakers, packet observers, remote controllers and other malicious software may exist in the University electronic environment. Be aware that these

programs may be dangerous and/or capable of compromising confidential information. Take appropriate precautions including keeping anti-virus software up to date. In general, never run or access a program or received file unless the content is known in advance and the source is trusted.

**9) The information in Private Computers is considered Confidential Private Information.**

The courts (a three Judge Panel of the U.S. Court of Appeals for the Ninth Circuit in San Francisco upheld an earlier decision of the U.S. District Court of the Northern District of California) have ruled that students have “a legitimate, objectively reasonable privacy expectation” concerning data on their computers even though it may be connected to a University network.

By extension , Pacific employees, whose authorized jobs involve computer maintenance and security, must gain documented permission from the owner before accessing not just student computers, but any Private Computer.

**Note:** Users are responsible for maintaining proper back-ups of their data, including, but not limited to, data files, applications, license keys and documentation. Although a rare occurrence, University service personnel are not responsible for any loss of data that may occur as a result of owner authorized activities. This is to be documented as part of the permission process (above).

**10) The information in Institutional Computers is considered Confidential Institutional Information. There is no expectation of privacy on Institutional Computers.** That is, even if the information on an Institutional machine is Private (Owned by the individual, not Pacific) use of an institutional machine waives any privacy rights the user may have in that information (although the information will continue to be treated as confidential).

Pacific employees, whose authorized jobs involve computer maintenance and security, are not required to gain permission from a user (or their designee) before accessing any Institutional Computer for normal maintenance and security purposes.

At Pacific, except in an emergency, any intrusions into institutional computers beyond normal authorized maintenance and security, requires the authorization of the Information Security Analyst (Security Officer), and the appropriate Vice President/Provost in consultation with the Director of Human Resources.

**Note:** Users are responsible for maintaining proper back-ups of their data, including, but not limited to, data files, applications, license keys and documentation. Although a rare occurrence, University service personnel are not responsible for any loss of data that may occur as a result of institutionally authorized activities.

**11) Private Computers that contain Confidential Institutional Information may be subject to e-discovery in legal actions concerning the University.** Such discovery may result in a loss of privacy.

The loss of a Private Computer containing Institutional Information may trigger notification under California Law 1386 as well additional actions under other statutes.

Wherever possible, Private Computers should not be used to store Institutional Information.

### 13. Telecommuting Policy

Approved by Academic Council, February 8, 2007, Administration, March 19, 2007

**POLICY: University of the Pacific supports properly managed telecommuting where there are mutual benefits to the University and the employee and may require it in exceptional situations.**

*Note that the line above is University Institutional Policy and that what follows is University Operational Policy. Both are approved by the Information Strategy and Policy Committee (ISPC).*

Definition of Telecommuting: Telecommuting is a mutually agreed upon work arrangement, not an employee entitlement, benefit or, unless a condition of hiring, a requirement, in which all or some of the work is performed at a non-University worksite. Telecommuting in no way changes the terms and conditions of employment with the University.

Exceptional Situation Provision: In the event the University (via the Cabinet) declares an Exceptional Situation for all or part of a Pacific campus, for example in the event of a natural or man-made disaster or epidemic, the University may require telecommuting for all or a part of those affected for the duration of the situation, unless prohibited by law.

Rationale: The University of the Pacific (“Pacific” or the “University”) recognizes the advantages of utilizing technology to reduce cost, increase productivity, conserve energy, improve safety and contribute to a cleaner environment.

#### Clarifications:

- 1) Unless stipulated in writing as a condition of hiring or required under the above Exceptional Situation Provision, telecommuting is entirely voluntary; a supervisor may not require an employee to telecommute. An Employee may not demand the “right” to telecommute. Telecommuting may or may not constitute the entirety of an employee’s working arrangement.
- 2) Except as required by applicable law, telecommuting does not normally, or automatically, include temporary work at home arrangements due to special circumstances such as illness, dependant care requirements or waiting on a delivery/service call. These situations are handled by arrangements negotiated with the employee’s supervisor within applicable departmental and Human Resources policies.
- 3) Telecommuting is not flextime. That is, work performed under a Telecommuting Agreement must take place according to the schedule established by that agreement. Employees are not free to work according to their own schedule under a Telecommuting Agreement.
- 4) This policy and work arrangement does not apply to those individuals (known as road-warriors) that hold positions that, by their very nature, require significant travel or a preponderance of time away from the University. This policy and these procedures are intended for those individuals (known as telecommuters) that hold positions that would normally be located on campus, but can be successfully performed by telecommuting.
- 5) Given that Pacific highly values personal student-teacher interaction, employees (including teaching faculty) that are engaged wholly, or in part, in site-based course delivery may not automatically be good candidates for telecommuting. Such individuals need specific written authorization from the Dean of their school.
- 6) Except as prohibited by applicable law, unless telecommuting is a condition of hiring, the employee must have worked on campus for at least 90 days. Employees must have and maintain a properly documented record of satisfactory or better Employee Performance Evaluations on file at Human Resources.
- 7) Potential telecommuters must properly execute, and abide by, a Pacific Telecommuting Agreement and other applicable agreements.
- 8) Telecommuting may not be suitable for all employees, positions or situations. Any employee that desires to work via telecommuting must seek authorization from their supervisor and unit head/Dean. Human Resources approval is also required. See the Guidelines for Telecommuting in

Exhibit D. The University reserves the right to approve or disapprove of any telecommuting arrangement in its sole discretion.

*Portions of this policy are excerpted from and/or modeled on work contributed to Educause by the following institutions: Oregon State University, University of California- Riverside, Collin County Community College District, Messiah College, and Columbia University.*

# Pacific Telecommuting Agreement

Approved by Academic Council, February 8, 2007, Administration, March 19, 2007

**Purpose:** This agreement specifies the conditions, requirements and understandings applicable to a telecommuting arrangement between the University of the Pacific (“Pacific” or the “University”) and the undersigned employee.

**Definition:** Telecommuting is a mutually agreed upon work arrangement, not an employee entitlement, benefit or, unless a condition of hiring, a requirement, in which all or some of the work, assigned to a site-based non-teaching Pacific employee, is performed at a non-University worksite.

**Exceptional Situation Provision:** In the event the University (via the Cabinet) declares an Exceptional Situation for all or part of a Pacific campus, for example in the event of a natural or man-made disaster or epidemic, the University may require telecommuting for all or a part of those affected for the duration of the situation, **regardless of normal eligibility detailed below**, unless prohibited by law.

**Eligibility:** **These eligibility requirements may be modified as necessary to comply with applicable law.**

- 1) Unless specifically approved by Human Resources, the employee is not entering this agreement for the purpose of performing temporary work at home due to special circumstances such as illness, dependant care, or waiting on delivery/service.
- 2) Unless telecommuting is a condition of hiring, the employee has worked on-campus for at least 90 days.
- 3) The employee has a properly documented record of satisfactory or better Employee Performance Evaluations on file at Human Resources.
- 4) The employee has executed, and agreed to abide by the indicated applicable agreements below and they are attached to this agreement:

\_\_\_\_\_ University IT Appropriate Use Policy agreement

\_\_\_\_\_ University Remote Access Agreement

\_\_\_\_\_ Data Access Agreement

\_\_\_\_\_ FERPA Policy Agreement

\_\_\_\_\_ Other: \_\_\_\_\_

**Specifications:**

- 1) Designated days and hours when employee is expected to be on the job via telecommuting at the designated worksite:  

---

- 2) Designated worksite location:  

---

- 3) Designated worksite phone number and/or cell-phone number:  

---

**Conditions:**

1) The employee agrees that telecommuting is not an employee benefit, entitlement or requirement, but unless a requirement at the time of hiring, a voluntary, mutually agreed upon work assignment. This work assignment is subject to this agreement, the policies of the University of the Pacific, and any applicable local, state and federal laws.

Exceptional Situation Provision: In the event the University declares an Exceptional Situation (via the Cabinet) for all or part of a Pacific campus, for example in the event of a natural or man-made disaster or epidemic, the University may require telecommuting for all or a part of those affected for the duration of the situation, unless prohibited by law.

- 2) The employee's supervisor attests that this arrangement is in the best interest of the University and the employee and is focused on results. The supervisor indicated below agrees to communicate to the employee, in advance, what assignments or tasks are appropriate to be performed at the telecommuting worksite, and what assessment techniques will be used to measure performance success. The supervisor agrees to tell the employee, in advance, what assignments or tasks are NOT appropriate to be performed at the telecommuting worksite and/or must be performed on campus. This is to be documented in writing and attached to this agreement as Exhibit B. Exhibit B may be modified, by written and attached addendum, from time to time in the sole discretion of the employee's supervisor, providing the employee is promptly notified. Employee understands and agrees that the University may terminate this Telecommuting Agreement at any time, in its sole and absolute discretion.
- 3) The signatories agree that this telecommuting arrangement cannot disrupt service to the employee's internal or external customers.
- 4) The performance review standards for employees working at telecommuting sites shall be identical to the standards used for campus based employees.
- 5) The employee is responsible for maintaining the same professional, effective communications and efficient workflow among co-workers and customers as they would have were the activities to be conducted on campus. The employee agrees to notify the employee's supervisor and/or the University if the employee's production levels are in any manner diminished as a result of the telecommuting arrangement.
- 6) The employee agrees to adhere to the above specified work schedule and agrees that, because telecommuting is not flextime, work cannot be performed outside the agreed upon schedule without written permission from their supervisor.
- 7) Employee acknowledges and agrees that compensation, including overtime (if appropriate and authorized), on-call policies, leave-permissions and benefits, including leave accruals, remain applicable and are not affected by the telecommuting policy, except to the extent the policy impacts actual time worked or the ability to participate in other activities during on-call status. Employee agrees to properly record and report all hours worked in accordance with applicable law. Income taxes will be withheld based on the location of the employee's administrative unit, not on the location from which the employee telecommutes. Employee is solely responsible for consulting with their tax advisor with respect to other tax consequences.
- 8) Employee acknowledges and agrees that, if employee is an FLSA non-exempt employee, employee shall not work overtime unless prior written approval is obtained from the appropriate supervision. Failure to obtain prior approval for overtime may result in the termination of this agreement and/or disciplinary action.
- 9) Employee will be covered by workmen's compensation laws for all work-related injuries that occur only in the designated worksite during the designated days/hours (as indicated above). Since the work site and home may be one and the same, worker's compensation will NOT apply to non-job related injuries that might occur in that worksite.
- 10) Employee agrees to maintain a safe, ergonomically sound and professional worksite. To ensure that safe working conditions are maintained, Pacific retains the right to inspect the employee's workplace at reasonable and mutually agreed upon times.
- 11) Pacific is not liable for any injuries to family members, visitors and others at the employee's telecommuting worksite and the employee agrees to hold Pacific harmless for such injuries. Note that the employee is NOT covered by the University when commuting to/from campus on days the employee is working on campus. Pacific is not responsible for any damages to the employee's telecommuting worksite

that may result from activities under this agreement. Employee agrees to maintain appropriate insurance to cover any such incidences.

12) Employee acknowledges and agrees that employee's homeowner's policy may not cover injuries arising out of, or relating to, the business use of the home. Employee understands and agrees that employee is solely responsible for obtaining an endorsement to their homeowners/tenants liability policy to cover bodily injury and property damage to all third parties arising out of or relating to the business use of their home. Employee understands and agrees that if employee lives in rental property, employee's lease may not permit business use of the premises. Employee understands and agrees that employee is solely responsible for determining whether employee meets zoning requirements and/or needs a business license, and for meeting such requirements.

13) The employee's supervisor will verify that the employee has the appropriate hardware, software, supplies and network connectivity to meet job requirements at the telecommuting worksite. Financial Liability is determined by a case by case negotiation between the telecommuting employee and the employee's unit head or Dean. The results of that negotiation are attached to this agreement as Exhibit A.

Emergency Provision: In the event the University declares an emergency for all or part of a Pacific campus, for example in the event of a natural or man-made disaster or epidemic, the University may require telecommuting for all or a part of those affected for the duration of the situation, unless prohibited by law. Under these circumstances, the University agrees to reimburse the employee for any direct out of pocket expense resulting from a mandate. **All reimbursable expenses must be pre-approved and documented in Exhibit B.**

14) Pacific is not responsible for the telecommuter's worksite, including but not limited to, operating costs, maintenance, property or liability insurance or other incidental expenses or private property. Since the telecommuting arrangement is voluntary, items provided by the employee at the telecommute site are not considered to be necessary business related expenses. In particular, unless a determination is made by the University that provision of such items is a necessary business related expense. Pacific has no responsibility or liability for Employee supplied items listed in Exhibit A

15) Items supplied by Pacific, as detailed in exhibit A, are to be used for University business ONLY and must not be used by other members of the employee's family or any other unauthorized person.

16) Except for normal hardware and software maintenance (including required upgrades) or repair (due to circumstances beyond control of the employee), and except as specified in paragraph 14. above, the employee acknowledges financial responsibility and liability for items supplied by the University as specified in Exhibit A. Pacific urges its telecommuters to check with their insurance agents regarding appropriate coverage for the loss or theft of University supplied items. Pacific may pursue recovery from the employee, at the employee's expense, for Pacific property, lost, damaged, destroyed or stolen. Employees may be required to bring the hardware and software in for normal maintenance and repair.

Exceptional Situation Provision: In the event the University (via the Cabinet) declares an exceptional situation for all or part of a Pacific campus, for example in the event of a natural or man-made disaster or epidemic, the University may require telecommuting for all or a part of those affected for the duration of the situation, unless prohibited by law. Under these circumstances, the University agrees to reimburse the employee for any direct out of pocket expense resulting from a mandate to telecommute. **All reimbursable expenses must be pre-approved and documented in Exhibit B.**

17) University Policy on Intellectual Property (IP) and Copyrights is not affected by telecommuting. IP and Copyrights not covered by University Policy and/or the Faculty Handbook arising from the work of the employee at any worksite, including the telecommuting worksite, are the property of the University of the Pacific. Any agreements to the contrary must be attached to this agreement as Exhibit C.

18) The employee will promptly notify their supervisor when unable to perform work from the telecommuting worksite due to failure of hardware, software, communications connectivity, or any other disruptive cause. The employee recognizes that they may be assigned other work and/or required to work on campus. Permanent disruption will terminate this agreement.

19) All work done at a telecommuting worksite is considered official University business. All records, documents and correspondence, codes, programs or other information in either electronic or paper form, created or obtained under this Agreement are, by this Agreement, the property of the University of the Pacific (except that Faculty ownership of information is governed by the Faculty Handbook) and must be

safeguarded and returned to the University upon termination of this Agreement. Release or destruction of data, information and/or records will be done only in accordance with University Policy, applicable local, state and federal laws and with the knowledge and agreement of the employee's supervisor.

20) The employee agrees that their personal vehicle will not be used for University business unless explicitly authorized in writing by their supervisor.

21) Pacific will not reimburse telecommuters for travel expenses to and from the campus to which the telecommuter reports administratively (their home campus). If travel to one of the other two campuses is necessary, Pacific will reimburse the traveler for the either the distance from the telecommuting worksite or the distance from their home campus, whichever is less.

22) Employees entering into this telecommuting agreement may be required to forfeit use of an on-campus personal worksite and/or share an on-campus worksite to maximize Pacific's use of space.

23) All Signatories below agree to the terms of this agreement, a copy of which shall be maintained in the employee's permanent Human Resources file.

**Term and Termination:**

1) Telecommuting eligibility (date and time), the term of this agreement, will: initiate on \_\_\_\_/\_\_\_\_/\_\_\_\_ at \_\_\_\_\_PST and will terminate on \_\_\_\_/\_\_\_\_/\_\_\_\_ at \_\_\_\_\_PST.

Renewal or extension requires execution of a new agreement.

Exceptional Situation Provision: In the event the University declares (via the Cabinet) an Exceptional Situation for all or part of a Pacific campus, for example in the event of a natural or man-made disaster or epidemic, the University may require telecommuting for all or a part of those affected for the duration of the emergency, unless prohibited by law.

2) This agreement will automatically terminate if its terms and conditions are violated by any of the signatories below.

3) All Telecommuting arrangements are granted on a temporary and revocable basis. This agreement can be terminated at any time, for any reason, upon written notice, by any of the signatories below or their successors.

4) The University retains sole and absolute discretion to terminate this Agreement at any time. In addition, should the employee's supervisor leave the University's employment, this agreement is automatically terminated and may or may not be re-executed at the option of the new supervisor.

5) Unless specified in Appendix A, the termination of this agreement does not obligate the University in any way for employee expenses associated with discontinuing telecommuting, including costs for commuting, ISP contracts, employee equipment leases or any other expense.

6) Upon termination of this agreement any items provided by Pacific as indicated in Exhibit A will be returned to the University within 5 working days.

**This agreement:**

1) The employee agrees that all obligations, responsibilities, terms and conditions of employment with Pacific remain unchanged, except those obligations and responsibilities specifically detailed in this agreement.

2) This agreement supersedes any verbal agreement or understanding relative to telecommuting.

3) This agreement represents the full and complete understanding of the terms and conditions associated with telecommuting. Any additions or changes to this agreement can only be made, in writing, by mutual consent of the signatories and attached to this agreement. However, Pacific reserves the right to modify this agreement on a temporary basis and/or to terminate the agreement in its sole and absolute discretion.

4) This agreement does not constitute a contract of employment, and should not be interpreted as creating a contract of employment, either expressed or implied. The employment relationship between Pacific and the employee is one of employment at will, and may be terminated by either party at any time, with or without notice and with or without cause.

## **Pacific Telecommuting Agreement Signature Page**

**Employee:** I hereby affirm by my signature that I have read and understand the Pacific Telecommuting Agreement (this document) and agree to abide by all provisions, policies and attachments.

Employee \_\_\_\_\_ Date: \_\_\_\_\_

**Supervisor or Department Chair:** I hereby affirm that I will appropriately manage the above employees telecommuting according to the terms and conditions of this agreement.

Supv./Chair \_\_\_\_\_ Date: \_\_\_\_\_

Exceptional Situation Provision: In the event the University declares (via the Cabinet) an Exceptional Situation for all or part of a Pacific campus, for example in the event of a natural or man-made disaster or epidemic, the University may require telecommuting for all or a part of those affected, unless prohibited by law. **In such an instance, the following signatures are not required.**

**Unit Head or Dean:** I hereby authorize the above employee and supervisor to begin and maintain a telecommuting work arrangement according to the terms and conditions of this agreement.

Unit Head/Dean \_\_\_\_\_ Date: \_\_\_\_\_

**Human Resources:** I have reviewed this employee's file for eligibility and the documentation provided with this agreement for appropriateness and approve this telecommuting work arrangement according to the terms and conditions of this agreement.

Human Resources \_\_\_\_\_ Date: \_\_\_\_\_

### Exhibit A, Financial Responsibility Distribution

ITEM	Pacific		Employee	
	Supplied	Cost to Pacific	Supplied	Cost to Employee
<b>Hardware:</b>				
<b>ISP and Phone Service:</b>				
<b>Software:</b>				
<b>Furniture:</b>				
<b>Supplies:</b>				

Employee's signature \_\_\_\_\_ Date \_\_\_\_\_  
 Unit Head/Dean signature \_\_\_\_\_ Date \_\_\_\_\_

Note: Be sure to address any issues or expenses associated with both the beginning and ending of telecommuting.

**Exhibit B, Agreed upon Assignments, Tasks, Goals and Deliverables**

*Instructions to the supervisor: Please indicate below what assignments, tasks, goals and deliverables are expected to be performed at the telecommuting worksite, and what assessment techniques will be used to measure performance success. Also indicate what assignments or tasks are NOT appropriate to be performed at the telecommuting worksite and/or must be performed on campus. This exhibit can and should be modified, by written and attached addendum, from time to time as necessitated by changing circumstance. The telecommuting employee must be promptly notified of any changes.*

Employee's signature \_\_\_\_\_ Date \_\_\_\_\_

Supervisor/Department Chair's signature \_\_\_\_\_ Date \_\_\_\_\_

## **Exhibit C, IP and Copyright Agreements**

*Instructions to supervisor: University Policy on Intellectual Property (IP) and Copyrights is not affected by telecommuting. IP and Copyrights not covered by University Policy and/or the Faculty Handbook arising from the work of the employee at any telecommuting worksite, are the property of the University of the Pacific. Any agreements to the contrary must be attached to this agreement.*

## 14. Network Scope of Service Policy

Approved by Academic Council, 2007, Administration, August 13, 2007

**Policy: The University is not a public Internet Service Provider, operates a private secure network solely for the benefit of its user community, including authenticated guests, for activities aligned with the mission of the university and does not provide its network services to those outside this community.**

*Note that the line above is University Institutional Policy and that what follows is University Operational Policy. Both are approved by the Information Strategy and Policy Committee (ISPC).*

### Definitions:

**User Community** are all those individuals that fall under Pacific's Business Rules that define the provision of service by status. The User Community may, and usually does, contain Authenticated Guests.

**Authentication** is a process used to identify a person to a computer or network system, commonly through validation of an ID and password. Authentication at Pacific involves having a PacificNet ID and password.

**Authorization(s)** are what an authenticated individual has the rights to do. Authorizations often depend on status, but may be fine-grained and relate to the specific person.

**Status** is the current standing relative to the University. For example, Student, Faculty, Staff member, Alumni, Authenticated Guest or Vendor. A person may have more than one status.

**Authenticated Guest** is an individual that is not an employee, student, alum or some other established category of Pacific community user. This category of user is intended for temporary access to Pacific's systems and services. Pacific does not supply its systems and services to Guest users on a long-term basis. Temporary workers, including those working for temp agencies are Authenticated Guests. Authenticated Guests must agree at login to be subject to the IT Policies of Pacific, including the Associated Use Policy (AUP). Background checks may be required depending on duties as required by Human Resources.

**Vendor** is an authenticated Pacific user that is included as part of the Community on a long term basis by virtue of the **Exception Clause** below. That is, they are an employee of a third party that has a formal arrangement with Pacific. To get the required PacificNet ID and Password, a vendor must agree in writing to be subject to the IT Policies of Pacific, including the Associated Use Policy (AUP) and agree to a background check to be conducted by HR at their or their company's expense. If a person is no longer associated with the third party, their Vendor status and credentials are revoked. Temporary workers, where salary is paid to a temp agency (and not directly to the person) are not considered vendors, but Authenticated Guests.

1) This policy statement combined with certain technical considerations is designed to insure that Pacific is not subject to CALEA

Communications Assistance to Law Enforcement Act. 1994 legislation that gives law enforcement agencies the right to place wiretaps on digital wireless networks. CALEA also requires wireless and wireline carriers to make their digital networks able to support law enforcement eavesdropping and wiretapping equipment and activities. Higher Education institutions are exempt if they are not judged to be Internet Service Providers (providing services to third-parties), but operate private networks (for their sole benefit).

There are complex technical and policy issues related to the determination of institutional CALEA exemption. OIT will continue to pursue legal clarification of the (private network) technical perspective as required. This policy is intended to maintain clean compliance relative to the provision of services to non-Pacific (third-party) entities such that questions are not raised going forward. However, on this specific issue of the provision of services to non-Pacific entities, some grey area is likely to remain. Because this policy is not intended to prohibit necessary and essential university operations, the following exception process is included:

**Exception Clause:** Provision of service to Vendors or non-Pacific entities can be provided so long as 1) The University obtains a favorable written legal opinion on the provision of the service relative to CALEA, taking into account previous and/or current exemptions and 2) the Cabinet formally approves such provision and 3) the provision of such services passes an initial and periodic technical and security review. The effort necessary to document the request, obtain the legal opinion, present it to Cabinet, secure the installation, including any costs in the process, is the responsibility of the requesting unit.

2) This policy is intended to insure that non-Pacific corporate entities, or their agents, do not (except as above and in 5) below) have access to PacificNet services. These corporations and individuals are often beyond the purview of Pacific's policies and procedures (ex. background checks). Without limitation, some examples of non-Pacific entities are: food service companies, cleaning companies, non-pacific owned book stores, building contractors, or any on-campus organization whose employees are not employees of Pacific.

3) This policy is not intended to block access and services to Authenticated Guests of the University directly engaged in Pacific's mission of teaching, learning, scholarship and administration. (ex. guest lecturers, registered library patrons). Pacific may or may not provide these individuals service on a case by case basis. (ex. One would not expect Pacific to give email service to library patrons.)

4) This policy is not intended to block authorized access to consultants and contractors that require access University IT systems solely for the purposes of deploying or managing those services. It would be expected that those individuals would get Basic IT services (like email) from commercial providers.

5) This policy is not intended to be immediately retroactive for existing situations:

**Grandfather Clause:** Any individuals or organizations that have contracts, agreements, MOUs or understandings with Pacific that would be in violation of this policy are exempt from this policy so long as certain conditions are met. Those conditions are: A) Their contract, agreement or MOU is not renewed, B) their physical location does not change or C) their status does not change (ex. they do not have a change in ownership).

The above notwithstanding, Pacific will conduct a security audit on those falling under this clause and changes may be recommended, or required as permitted by contract, agreement or MOU language.

6) This policy does not prohibit Pacific from offering information technology transport services for computing and communication so long as such transport is logically, if not physically, isolated from PacificNet. For example, OIT might be able to connect construction trailers with available fiber or copper and not be a part of PacificNet. Likewise, transport may take the form of a separate dedicated VLAN with no logical connection to PacificNet. Without access to PacificNet, there is no Internet access.

7) This policy does not prohibit Pacific from supporting these non-Pacific activities with money or personnel, so long as this does not conflict with any of the other terms of this or other Pacific IT Policies.

8) This policy does not prohibit Pacific from using temporary employees that work for employment agencies.

## 15. Technology Acquisition Coordination Policy

**POLICY: All significant purchases, leases, gifts, loans, renewals and contracts for new, used or upgraded Information Technology goods, services and implementations, shall occur in coordination with the Office of Information Technology in a timely manner across the schools and campuses.**

*Note that the line above is University Institutional Policy and that what follows is University Operational Policy. Both were approved by the Information Strategy and Policy Committee (ISPC) on 12/17/07.*

Information Technology (IT) has now permeated virtually every aspect of our academic lives and business processes. Increasing concerns over cost, reliability, security, staffing, business continuity and the management of customer relations is, and will continue to be, moving the various academic and administrative units of the University towards greater interdependence. Individual unit decisions now affect the greater University as never before. We can no longer afford, in terms of dollars, efficiency, or security, uncoordinated action relative to IT. The scope and process of the required policy are outlined below.

### **Scope:**

(1) IT goods and services include, but are not limited to, computers, software, voice, data and video services, cable TV services, mobile phone services, wireless services, voicemail, telephone switch matters or other telephone based service installations or upgrades, IT based administrative services or products, and IT based academic or operational services.

(2) This coordination specifically includes the purchase, lease, renewal or upgrade of any hardware, software or service that might reasonably interface with Banner immediately or in the future as well as any hardware or software that automates or provides administrative functionality.

(3) This coordination specifically includes, but is not limited to, email systems, course management systems, directory services, authentication and authorization services, content management systems, portfolio systems, library systems, web services, and hosting services.

(4) University standards for desktop and server acquisitions fall under the Information Strategies and Planning Committee (ISPC) operational Policy of Technological Diversity and do not require coordination under this policy so long as those acquisition guidelines and established hardware standards are followed. Mass purchases on non-standard desktop equipment need to be coordinated.

(5) For the purposes of this policy, “significant” means goods, services or collections thereof, intended to be utilized by more than one person OR where the cost or value of such is at the Capital level as described in the Business Policies and Procedure’s Manual, or above, including applicable taxes and fees OR where such acquisitions require an agreement or contractual arrangement in excess of one year OR any combination of the above.

6) Regardless of the above, including the exact definition of “significant”, the spirit of this policy is expected to be upheld. Acquisitions that potentially affect other systems, business processes, groups or individuals need to be coordinated appropriately. If there is any doubt or to make sure, contact OIT.

### **Process:**

(1) Planning and notification is required.

- a) Proposals or plans for the activities described above must be brought forward to the appropriate Director in OIT, at the time the decision is first made to investigate or pursue, but no less than 30 days before an offer or contract expires, or is scheduled to renew, or the functionality is required. Note that some contracts renew automatically if 30 to 60 days advance written notice is not provided. The preferred methods of bringing plans and activities forward is:

- i. For schools, to come from the school IT committee, through the Chair, to the Director of Educational Technology Services or Director of Cyber Infrastructure.
    - ii. For the administrative units, to come from the sponsoring unit, through the administrative computing committee structure and/or to the Director of Enterprise Applications.
    - ii. For Athletics, Student Life, or in the case of doubt or the position vacancies and absences, to the CIO for appropriate disposition..
  - b) The appropriate OIT Director and/or the CIO will coordinate, if necessary, with the Information Strategies and Planning Committee, seeking its endorsement and recommendation as appropriate.
  - c) Proper planning is a requirement of these policies. Proposals shall not be brought forward at the last minute, under “emergency conditions,” expiring vendor offers or other unrealistic deadlines
  - d) Prior to execution, all proposals, contracts and licenses that fall under the auspices of this policy are subject to a Security Review by the Information Security Officer, in consultation with Risk Management, as appropriate. As a practical matter, if a proposal is viewed as possibly having security issues, taking it to the Information Security Officer (ISO) first may expedite the process. The ISO will then distribute it to the appropriate OIT Director.
- (2) Cooperation and timely action is required.
  - a) Coordination is working to the spirit of this policy in good faith, regardless of technicalities.
  - b) The OIT staff and/or the CIO will review all significant IT, contracts, agreements, offers or understandings, before they are acted upon by the requesting unit, school or campus.
  - c) OIT will coordinate all the relevant stakeholders and, as soon as possible within the coordination period, as appropriate, create an institutional view and recommendation.
  - d) It is mandated that all applicable parties will distribute all available information in a timely manner that enables appropriate discussion, investigation of alternatives and testing where applicable.
  - e) Close coordination of Purchasing Departments on the three campuses is necessary, and expected, to assure the success of this policy.
- (3) Consequences will occur for non-compliance.
  - a) Failure to coordinate IT acquisitions, through commission or omission, in violation of this policy will be handled as prescribed in Pacific’s Information Technology Policies under Sanctions.
  - b) Failure by the proposal sponsors to act in the timely manner described above will be grounds for possible rejection of the proposal.
  - c) Failure by OIT to act in the timely manner described above will be grounds for acceptance of the proposal following consultation with the CIO, Provost and appropriate Vice President.

## 16. Emergency Notification Policy

**Policy: Participation in the University's electronic Emergency Notification System is mandatory for students and for all individuals with wireless communication devices paid for in whole or part by the University.**

*Note that the line above is University Institutional Policy and that what follows is University Operational Policy. Both were approved by the Information Strategy and Policy Committee (ISPC on 12/17/07).*

### Policy Overview

In the wake of the Virginia Tech shootings, most colleges and universities reviewed their plans for emergency notification. OIT working with Public Safety and the Pacific Alert Team and with the help of Student Life, have implemented an electronic Emergency Notification System available for all current faculty, staff, students and other authorized members of the Pacific Community. All students must participate. Because participation heightens personal safety and the safety of others in the community by providing early communication and information about campus crises and emergencies, all faculty and staff are strongly recommended to participate. Some individuals holding positions of responsibility at Pacific, such as Student Life staff, may be required to participate as are individuals whose phones are sponsored in whole or part by the University. Employees are encouraged to enter both their mobile phone numbers and their home phone numbers so that they may be made aware of campus situations even when they are off campus.

It is not the intent of this policy to suggest that this is the only means of emergency notification to be used by the University. Participation does not constitute any form of guarantee of safety.

### Operational Overview

- 1) Pacific's Electronic Emergency Notification System has two parts. The first part is the actual Notification Message Service. This is provided by a well respected company that is used by many universities. In an emergency, all numbers and email addresses provided are sent the notification.
- 2) The second part of the system is provided by OIT and is used to gather and maintain the contact information. All users with Pacific Net IDs can provide/update their contact information through insidePacific. This method enables participants to update their information, which they will need to do periodically to keep the system current.
- 3) Compliance with this policy will be assessed at key verification points in University business processes (indicated below) as necessary to maximize participation.
- 4) The University will not supply communication devices solely to meet any aspect of this policy. However, if the University pays, in whole or in part, for a person's cell phone, they must participate in this system as defined below.
- 5) OIT, working with Public Safety, will add certain key buildings/individuals to the automated system using campus exchange numbers. These individuals will be responsible for notifying others as appropriate and directed.

### Privacy

Pacific respects the privacy of its community members. The information gathered for this Emergency Notification System is confidential, collected under its own dedicated Privacy Statement Addendum, and is not shared with other applications or systems. See also Pacific's Master Privacy Statement.

## Participation Defined

To participate, individuals must supply a primary contact number. Specifically, it is university policy that students who carry mobile phones and other community members who are provided with University paid mobile phones or are reimbursed in whole or in part for mobile phone charges, must register them with this system as the primary contact number. International numbers are not allowed, but toll based numbers are permitted. Due to inbound trunking limitations on each campus, the respective campus exchange numbers are not allowed (946, 739, 929, etc.). Those individuals without mobile phones will need to register, in good faith, the next best alternate phone number (home, spouse, parent, etc.) and rely on email and/or other notification means as available. Pacific email addresses are pre-populated and users can provide an alternate email address. Users of University supplied cell phones will automatically be enrolled as participants.

Note that while participation is optional for non-students with privately funded communication devices, it is highly encouraged. Some employees in key positions may be required to participate as a condition of employment. All participants must keep their information current and accurate.

## Verification

1) Verify their input. After supplying (or reviewing) their information, self-enrolling participants must programmatically agree to the following statement:

*The information I have provided above is correct to the best of my knowledge. If I carry a wireless communications device, I have provided its number as the primary contact. I understand that failing to keep this information current and accurate puts me at additional risk of not being notified in an emergency. I agree that the University of the Pacific can release the information I have provided to the Notification Message Service in accordance with the University's Privacy Policy for the sole purpose of providing this service. I understand that this notification system is no guarantee of security.*

2) The system will keep the date of last verification. No verification date can be more than 180 days old for staff or one term old for students. Older dates will be blanked, that is, the information set to un-verified. The next time a compliance assessment step is encountered, re-verification will be required before one can proceed.

3) The system will be tested periodically. If it succeeds in contacting a participant, by phone, it will reset their verified date to the date of the test. If the participant cannot be reached, OIT will blank the verified date and send them an email. In theory, if a participant gives accurate information, maintains it and is able to be contacted, they will not be needlessly impeded by compliance assessment steps. If not, the email will read:

*Pacific's Emergency Notification System failed to contact you in its most recent test. This could occur for any number of reasons. However, to ensure that the system has your current information, you are asked to re-verify its accuracy. University policy requires this information to be current and accurate. Please do so immediately by logging on to PacificNet or insidePacific and following the instructions. Thanks for your help in keeping the campus safe.*

*Public Safety*

### **Compliance**

- 1) If a user mandated to participate in the Emergency Notification System under this policy is not participating or a participant is out of compliance, they may be prevented from proceeding from login to PacificNet and/or proceeding from login to insidePacific.
- 2) Supplying false or inappropriate contact information may be grounds for disciplinary action.

### **Termination**

Participation in the Emergency Notification System will automatically terminate for students no less than 90 days after graduation or loss of student status. After graduation or loss of student status, former students may manually opt out of the Pacific Connect through insidePacific if early termination is desired. Participation in the Emergency Notification System for Pacific employees (faculty and staff) will terminate on the day after their employment termination. Other participants, if any, may terminate participation in the Emergency Notification System at any time by blanking out their information in insidePacific.

### **Other Requirements**

- 1) Offices may require mobile phones be set to vibrate, but may not require them to be turned off.

## **17. Privacy Policy**

**Policy: The University will create, maintain and abide by a Master Privacy Statement applicable to all record keeping systems and will amend it with any required unit specific privacy statements.**

*Note that the line above is University Institutional Policy and that what follows, including the Master Privacy Statement, is University Operational Policy. Both are approved by the Information Strategy and Policy Committee (ISPC). Adopted by the Cabinet 2/25/2008.*

### **Privacy Policy Definitions**

Confidential information – Confidential Information is defined by The University’s Information Management Policy and repeated here for convenience:

Confidential Information is the strictest data classification used by the University and requires maximum control. Depending on the nature or contents of the Confidential Information, disclosure or alteration of this type of information could cause great harm to an employee, student or the University. Confidential Information requires safeguarding, either due to the requirements of law or because of the mandates of prudent and reasonable practices.

The University’s Computing and Communications Confidentiality Policy states: The University will treat all of its individual User information, User activity, and User communications as Confidential Information as defined in its Information Management Policy.

Restricted Information – Information with access restricted to individuals who have been explicitly granted authorization to do so.

Private Information – Information owned or controlled by the individual, not the institution.

Personally Identifiable Information – Private information stored with personally identifiable names or numbers. All Personally Identifiable Information is Confidential Information.

Protected Health Information: - The Privacy Rule provisions of the Health Insurance Portability and Accountability Act (HIPAA) of 1996 protects all "individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this information "protected health information (PHI)."

Privacy – The expectation that Personally Identifiable Information will not be disclosed to anyone other than its owner. Privacy is traded for the ability to do business with strangers. Practically speaking, consumers convert their private information to restricted information in return for goods and/or services.

Privacy Statement – The detailed, documented, public face on the University’s stewardship of user information.

Master Privacy Statement – The operational privacy principles the University uses that pertain to all cases.

Master Privacy Statement Addendum – The special or exceptional operational privacy principles the University uses that pertain to a specific case.

Computers – this means desktop, laptop, servers and all other computing hardware, media and communication devices or systems that can store data

### **Privacy Policy Background**

According to Educause’s white paper Privacy, “Traditionally, Congress has chosen not to pass any broad spectrum privacy laws, but to limit the government’s power and target specific issues as they arise. As a result, we have a “quilt” of laws and regulations such as the Fair Credit Reporting Act, the Family Education Rights and Privacy Act, the Cable Communications Policy Act, [the Health Insurance Portability and Accountability Act,] and most recently the Children’s Online Privacy Protection Act [and the Gramm-Leach-Bliley (GLB) Act]. However, what has developed is a standard. The Code of Fair Information Practices was originally developed in 1973 by the Department of Health, Education, and Welfare to limit the government’s access to private information. It has evolved into the standard which both the government and private sectors use to measure privacy policy, and is comparable to international guidelines developed by the OECD (Organization for Economic Cooperation and Development).” The work below covers the requirements of that code. In California, The California Online Privacy Protection Act of 2003, is aligned with the code (alignment is bolded below).

In 2004 the U.S. Department of Health and Human Services (“HHS”) issued the Privacy Rule to implement the requirement of the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”). The Privacy Rule standards address the use and disclosure of individuals’ health information—called “protected health information” by organizations subject to the Privacy Rule — called “covered entities,” as well as standards for individuals’ privacy rights to understand and control how their health information is used.

It should also be noted that issues like identity theft and spam have become serious problems in daily life. As the University increasingly collects personal information as it moves toward its goals of customized and personalized service to its community, privacy concerns will be a significant roadblock unless they are directly and prominently addressed. The University must join the large number of commercial entities that provide comprehensive and visible privacy statements.

### **Privacy Policy Principles**

- 1) The Master Privacy Statement applies to all data on individuals held by the University.
- 2) Privacy Statement Addendums are and will be written:
  - a) when it is necessary to override and/or modify this Master Privacy Statement
  - b) when required by law or contract
  - c) when information falling under this Statement is supplied to third parties
  - d) when units provide health services subject to the HIPAA Privacy Rule
- 3) The Master Privacy Statement is about documenting stewardship of information in record-keeping systems and does not cover ownership or copyright issues.
- 4) It is the University’s policy that there shall be no personal data record-keeping systems whose very existence is a secret.
- 5) Each record-keeping system, as needed by contract, or required by law, will have an associated Privacy Statement Addendum conveniently available to its information contributors. In particular, as applicable and/or required, each online web page will have a Privacy Statement link that covers the personally identifiable information being solicited on that Page.

### **Privacy Statement Addendum Principles**

Where they exist, each Privacy Statement Addendum shall include:

- 1) A unique name for the Privacy Statement Addendum that clearly identifies the Addendum for the intended purpose and/or audience. For example, Admission’s Website Privacy Statement Addendum.
- 2) The full name of the organizational unit sponsoring the Addendum and its current contact information.
- 3) The date this Privacy Statement Addendum took effect and the date it was last updated.
- 4) A statement that this is an Addendum to the University’s Master Privacy Statement and a web reference link back to the Master Privacy Statement.
- 5) What personally identifiable information of the information provider or third party personally

identifiable information is being obtained or collected under this Addendum, directly or through, non-University third parties.

- 6) How the information will be used and/or how it will not be used.
- 7) If different from the provisions of the Master Privacy Statement, with whom the information may be shared and/or with whom the information will not be shared.
- 8) What choices, if any, are available to the information provider regarding how information is or may be obtained, used and/or distributed.
- 9) How the information provider can access, verify, amend the collected information and/or correct any inaccuracies in the collected information.
- 10) The kind of security processes, procedures and policies that are in place to prevent the misuse, alteration or loss of the provided information
- 11) A statement that the University and/or the University organizational unit controlling the Privacy Statement Addendum reserves the right to change it at any time without prior notice or consent, but that if such changes are made, they will be prominently and widely communicated.
- 12) For Privacy Statement Addendums covering information gathered online, a change history for that Addendum will be maintained off the Privacy Statement link on each page that gathers such information.
- 13) In cases where a Business Associate Agreement as described in the HIPAA Privacy Rule is mandated, this should be documented in the Addendum.

Note: All Privacy Statements and Addendums should be reviewed by legal counsel. When providing paper copies to information providers, the information collector must provide the Master Privacy Statement and all the appropriate Privacy Statement Addendums relative to the information being collected.

**Limitations**

Neither this master Privacy Statement nor any of its Privacy Statement Addendums are intended to address all, or fully and accurately prescribe, compliance steps required under the various applicable federal, state and local laws. It is expected that the University will comply with all such laws as determined to be applicable to the University by its legal counsel. Therefore, University compliance with this policy and/or statements should not be considered sufficient to comply with any particular law. The advice of expert counsel is recommended for all compliance issues.

\*\*\*\*\*  
\*\*\*\*\*

**Pacific’s Master Privacy Statement**

Date this Master Privacy Statement went into effect: MM/DD/YYYY

Date this Master Privacy Statement was last updated : MM/DD/YYYY

**Privacy Statement Definitions:**

The University: The University of the Pacific and all its divisions, departments and officially sponsored organizations.

The General Public: Unrestricted readers of, University produced, Printed Materials and Web Site

Personally identifiable information: Individually identifiable information including any of the following:

- (1) A full or partial name
- (2) A home address or other physical address
- (3) An e-mail address or other electronic address
- (4) A telephone number or other communications device number

- (5) A social security number or other identification number
- (6) A date of birth
- (7) Drivers license number
- (8) Credit card or Financial account number
- (9) Any other identifier that permits the physical or online contacting of a specific individual.
- (10) Any information concerning an individual in combination with an identifier described above. In particular,
  - a) for students, this includes all information not designated as Directory information under FERPA.
  - b) for all, Protected Health Information (PHI). The Privacy Rule provisions of the Health Insurance Portability and Accountability Act (HIPAA) of 1996 define PHI as all "individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form of media, whether electronic, paper, or oral."

Does not include non-individual summary information used for statistical purposes. Does not include works of authorship, copyrighted information or electronic communications such as voicemail or email.

Record keeping system: A system designed to collect, organize and store personally identifiable information. Record keeping systems may vary from a simple document, to a spreadsheet to a database and are primarily intended to facilitate administering activities related to the mission of the University.

Information Provider: The individual that provides the information.

Third Parties: Individuals or organizations, not a part of or affiliated with the University.

Provided information: Personally identifiable information given directly to the University by an individual. This information can be about themselves or another individual, like a parent or guardian.

Collected Information: Personally identifiable information that may include directly provided information and/or information obtained from a third party.

Directory Information: Personally identifiable information that: (1) For Students consists of elements defined as not confidential under FERPA. (2) For employees, information defined as not confidential by HR. (3) For everyone, information that the Information Provider explicitly designates as not confidential. Directory information may be freely provided to The University.

Privacy Flag: Students may request that Directory information not be shared with anyone, by asking the Registrar to set the privacy Flag.

## **Introduction**

In the course of fulfilling its mission of teaching, learning and scholarship, the University employs a variety of record keeping systems and collects and uses a variety of information associated with its past, present and future customers, including faculty, staff and students. In addition to observing all applicable privacy and confidentiality laws, the University respects and protects individual privacy through this Master Privacy Statement and, where applicable, a series of Privacy Statement Addendums. Privacy Statement Addendums are specific to the information being collected and/or the specific academic or administrative units that collects it.

## **Privacy Statement Precepts**

In all circumstances, the University will:

- a. Secure all personally identifiable information using appropriate and generally practiced security measures and technology.

- b. Except for Directory Information, consider all personally identifiable information as confidential under its Computing and Communications Confidentiality Policy, sharing it only on a need-to-know basis under the terms of this Master Privacy Statement and any applicable Privacy Statement Addendums.
- c. Directory Information will not be shared with the General Public without its owner’s explicit permission.
- d. Practice good stewardship of Directory Information, using it appropriately under applicable laws, this Master Privacy Statement and any applicable Privacy Statement Addendums..
- e. If it is required to do so, comply with the law or with legal process and disclose personally identifiable information
- f. Retain the right to use personal information in its systems to identify the source of any inappropriate usage of its electronic resources as outlined in its Information Technology Policies: Acceptable Use Policy.
- g. Change this Master Privacy Statement from time to time without prior notice or consent, but if changes are made, that fact will be prominently and widely communicated. A Change history for the Master Privacy Statement will be maintained off the Privacy Statement link on Pacific’s Home Page.
- h. Accept and act on all allegations of Privacy Statement violations addressed to [privacy@pacific.edu](mailto:privacy@pacific.edu).

Unless explicitly stated otherwise in a specific Privacy Statement Addendum, Pacific may:

- i. Share personally identifiable information, on a need to know only basis, with authorized third parties (non-Pacific entities) that provide service to the University and that have contractually agreed to point (a.) above.
- j. Share protected Health Information with authorized third parties as permitted under the HIPAA Privacy Rule solely for the purpose of treatment, payment, or and health care operations.
- k. Not provide personally identifiable information to third parties for any purpose unrelated to the mission of the University without the explicit permission of the information provider or as specified in the HIPAA Privacy Rule. This includes, but is not limited to the marketing of commercial goods or the provision of commercial services.
- l. Share personally identifiable information within Pacific in support of its mission of teaching, learning and scholarship and the administration thereof so long as the Privacy Statement Addendum (if any) under which the information was collected remains in force.
- m. Obtain personally identifiable information from third parties (collected information), solely as necessary to conduct the business of the University, and will treat that information as if it were directly obtained from the person in question.
- n. Request personally identifiable information for the purpose of obtaining access to and/or verifying authorization to use services or facilities of or sponsored by the University, especially by electronic means for electronic services.
- o. Add a consent line to information input sources, like forms or screens, stating that by their agreement their information will be managed under the University’s Privacy Statement and/or a particular Privacy Statement Addendum(s). Failure to sign would halt the associated business process, perhaps resulting in the inability of the University to provide desired services or considerations.

\*\*\*\*\*  
 \*\*\*\*\*  
 \*\*\*\*\*

## Appendix I California Online Privacy Protection Act of 2003

Below is the full text of the applicable parts of the California Online Privacy Protection Act of 2003.

Because Pacific complies with all applicable law, this appendix is University Policy by reference.

Note that this law is very prescriptive as to how privacy policies are to be posted on web sites.

Those units to which this law applies, must write corresponding Privacy Statement Addendums.

### BUSINESS AND PROFESSIONS CODE

#### SECTION 22575-22579

22575. (a) An operator of a commercial Web site or online service that collects personally identifiable information through the Internet about individual consumers residing in California who use or visit its commercial Web site or online service shall conspicuously post its privacy policy on its Web site, or in the case of an operator of an online service, make that policy available in accordance with paragraph (5) of subdivision (b) of Section 22577.

An operator shall be in violation of this subdivision only if the operator fails to post its policy within 30 days after being notified of noncompliance.

(b) The privacy policy required by subdivision (a) shall do all of the following:

- (1) Identify the categories of personally identifiable information that the operator collects through the Web site or online service about individual consumers who use or visit its commercial Web site or online service and the categories of third-party persons or entities with whom the operator may share that personally identifiable information.
- (2) If the operator maintains a process for an individual consumer who uses or visits its commercial Web site or online service to review and request changes to any of his or her personally identifiable information that is collected through the Web site or online service, provide a description of that process.
- (3) Describe the process by which the operator notifies consumers who use or visit its commercial Web site or online service of material changes to the operator's privacy policy for that Web site or online service.
- (4) Identify its effective date.

22576. An operator of a commercial Web site or online service that collects personally identifiable information through the Web site or online service from individual consumers who use or visit the commercial Web site or online service and who reside in California shall be in violation of this section if the operator fails to comply with the provisions of Section 22575 or with the provisions of its posted privacy policy in either of the following ways:

- (a) Knowingly and willfully.
- (b) Negligently and materially.

22577. For the purposes of this chapter, the following definitions apply:

(a) The term "personally identifiable information" means individually identifiable information about an individual consumer collected online by the operator from that individual and maintained by the operator in an accessible form, including any of the following:

- (1) A first and last name.
- (2) A home or other physical address, including street name and name of a city or town.
- (3) An e-mail address.
- (4) A telephone number.
- (5) A social security number.
- (6) Any other identifier that permits the physical or online contacting of a specific individual.
- (7) Information concerning a user that the Web site or online service collects online from the user and maintains in personally identifiable form in combination with an identifier described in this subdivision.

(b) The term "conspicuously post" with respect to a privacy policy shall include posting the privacy policy through any of the following:

- (1) A Web page on which the actual privacy policy is posted if the Web page is the homepage or first significant page after entering the Web site.
- (2) An icon that hyperlinks to a Web page on which the actual privacy policy is posted, if the icon is located on the homepage or the first significant page after entering the Web site, and if the icon contains the word "privacy." The icon shall also use a color that contrasts with the background color of the Web page or is otherwise distinguishable.
- (3) A text link that hyperlinks to a Web page on which the actual privacy policy is posted, if the text link is located on the homepage or first significant page after entering the Web site, and if the text link does one of the following:
  - (A) Includes the word "privacy."
  - (B) Is written in capital letters equal to or greater in size than the surrounding text.
  - (C) Is written in larger type than the surrounding text, or in contrasting type, font, or color to the surrounding text of the same size, or set off from the surrounding text of the same size by symbols or other marks that call attention to the language.
- (4) Any other functional hyperlink that is so displayed that a reasonable person would notice it.
- (5) In the case of an online service, any other reasonably accessible means of making the privacy policy available for consumers of the online service.
- (c) The term "operator" means any person or entity that owns a Web site located on the Internet or an online service that collects and maintains personally identifiable information from a consumer residing in California who uses or visits the Web site or online service if the Web site or online service is operated for commercial purposes. It does not include any third party that operates, hosts, or manages, but does not own, a Web site or online service on the owner's behalf or by processing information on behalf of the owner.
- (d) The term "consumer" means any individual who seeks or acquires, by purchase or lease, any goods, services, money, or credit for personal, family, or household purposes.

22578. It is the intent of the Legislature that this chapter is a matter of statewide concern. This chapter supersedes and preempts all rules, regulations, codes, ordinances, and other laws adopted by a city, county, city and county, municipality, or local agency regarding the posting of a privacy policy on an Internet Web site.

22579. This chapter shall become operative on July 1, 2004.