

OLLU INFORMATION SECURITY GOVERNING POLICY

Introduction:

In order to fulfill its stated mission, the University is committed to providing secure resources that protect the integrity, availability and confidentiality of information while maintaining its accessibility.

Policy:

Each member of the University community is responsible for the security and protection of information resources over which he or she has control. Resources to be protected include networks, computers, software, data, storage devices and paper records. The physical and logical integrity of these resources must be protected against threats such as unauthorized intrusions, malicious misuse, theft, physical damage, or inadvertent compromise. Activities outsourced to off-campus entities must comply with the same security requirements as in-house activities.

Roles And Responsibilities:

Responsibilities range in scope from security controls administration for a large system to the protection of one's own access password and of the files and storage devices under one's own control. A particular individual often has more than one role.

Administrative Officials (individuals with administrative responsibility for campus organizational units [e.g., unit heads, deans, department chairs, principal investigators, directors, or managers] or individuals having functional ownership of data and other information) must:

- identify the information resources within areas under their control;
- define the purpose and function of the resources and ensure that requisite education and documentation are provided to the University as needed;
- establish acceptable levels of security risk for resources by assessing factors such as:
 - how sensitive the data is, such as research data or information protected by law or policy,
 - the level of criticality or overall importance to the continuing operation of the University as a whole, individual departments, research projects, or other essential activities;
 - how negatively the operations of one or more units would be affected by unavailability or reduced availability of the resources,
 - how likely it is that a resource could be used as a platform for inappropriate acts towards other entities,
 - limits of available technology, programmatic needs, cost, and staff support;

- for systems and processes in support of University business administration, ensure compliance with relevant legal requirements, such as FERPA and HIPAA;
- ensure that requisite security measures are implemented for the resources;
- comply with the separate University Information Security Awareness Policy to ensure that users and employees in their units are familiar with security policies and practices.

Providers (individuals who develop, manage, and operate University information resources, e.g. project managers, system designers, application programmers, or system administrators) must:

- become knowledgeable regarding relevant security requirements and guidelines, as detailed in the separate Information Security Awareness Policy;
- analyze potential threats and the feasibility of various security measures in order to provide recommendations to Administrative Officials;
- implement security measures that mitigate threats, consistent with the level of acceptable risk established by administrative officials;
- establish procedures to ensure that privileged accounts are kept to a minimum and that privileged users comply with privileged access agreements;
- for systems in support of University business administration, establish procedures to implement relevant legal requirements, such as FERPA and HIPAA;
- communicate the purpose and appropriate use for the resources under their control.

Users (individuals who access and use University information resources) must:

- become knowledgeable about relevant security requirements and guidelines, as detailed in the separate Information Security Awareness Policy;
- protect the resources under their control, such as access passwords, computers and other storage devices, paper documents, and data they download.

Insufficient security measures at any level may cause resources to be damaged, stolen, or become a liability to the University. Therefore, responsive actions may be taken. For example, if a situation is deemed serious enough, a computer posing a threat will be blocked from network access until the security deficiency is remedied.

Key Security Elements:

Logical Security:

Computers must have the most recently available and appropriate software security patches, commensurate with the identified level of acceptable risk. For example, installations that allow unrestricted access to resources must be configured with extra care to minimize security risks.

Adequate authentication and authorization functions must be provided, commensurate with appropriate use and the acceptable level of risk.

Attention must be given not only to large systems but also to smaller computers which, if compromised, could constitute a threat to campus or off-campus resources, including computers maintained for a small group or for an individual's own use.

Physical Security:

Appropriate controls must be employed to protect against theft, unauthorized access, or accidental damage to resources, commensurate with the identified level of acceptable risk. These may range in scope and complexity from extensive security installations to protect a room or facility where server machines are located, to simple measures taken to protect a User's display screen or filing cabinets.

Privacy And Confidentiality:

Applications and office procedures must be developed and devices must be used so as to protect the privacy and confidentiality of the various types of data they process, in accordance with applicable laws and policies.

Users who are authorized to obtain data must ensure that it is protected to the extent required by law or policy after they obtain it. For example, when sensitive data is transferred from a well-secured mainframe system to a User's location, adequate security measures must be in place at the destination computer or portable device to protect this "downstream data".

As outlined in the Policy for Acceptable Use of University Computer and Communication Resources, technical staff assigned to ensure the proper functioning and security of University electronic information resources and services are permitted to search the contents of electronic communications or related transactional information. For example, security staff scanning of network traffic to detect intrusive activities is permitted to ensure compliance with laws and policies. The Vice President for LITS must approve of any such monitoring activities.

Compliance With Law And Policy:

Campus departments, units, or groups should establish security guidelines, standards, or procedures that refine the provisions of this Policy for specific activities under their purview, in conformance with this Policy and other applicable policies and laws. Information resources used in support of University business administration must comply with the provisions of applicable local, state and federal legal requirements.

Security related policies that apply to all University information resources include, but are not limited to, the Policy for Acceptable Use of University Computer and Communication Resources and the Information Security Awareness Policy. In addition

to any possible legal sanctions, violators of this Policy may be subject to disciplinary action up to and including dismissal or expulsion, pursuant to University policies, collective bargaining agreements, codes of conduct, or other instrument governing the individual's relationship with the University. Recourse to such actions shall be as provided for under the provisions of those instruments.

Resources:

Contacts:

Questions about this Policy or other University information resource policies may be directed to the Vice President for LITS.

Questions about information security requirements may be directed to the Director of Network/Telecommunication, who also acts as the University Information Security Coordinator.

Report information or data security incidents to: "nts@lake.ollusa.edu"

Related Documents:

Policy for Acceptable Use of University Computer and Communication Resources
Information Security Awareness Policy

Spring 2007
Recommended by Administrative Council