

INFORMATION SECURITY AWARENESS POLICY

1. Purpose

Effective information security requires a high level of participation from all members of the University. This policy defines responsibilities and roles for instilling information security awareness among all information resource owners, managers, service providers and users.

2. Scope

This policy affects all users of the University's information resources.

3. Policy standards and guidelines

- a. All must be well informed of their responsibilities as Information Owners, Managers, Users, and Service Providers.
- b. In cooperation with the training office, the University Information Security Officer is responsible for managing a University training and awareness program for all members of the University community and for consulting with members of the University on information security issues.
- c. Training classes and materials should be offered to instill the importance of appropriate information handling and to explain the implications of this Policy.
- d. Training should include specific information on the use of security precautions such as encryption, anti-viral tools, backup procedures, physical security and awareness of social engineering tactics.
- e. The University Information Security Officer is responsible for maintaining the [Information Security Web site](#), which makes the information security resources described in this Policy available to the University community.
- f. Managers and Deans are responsible for seeing that their employees and faculty take advantage of available security awareness resources.
- g. Information Owners and Service Providers must become familiar with standard information security principles and procedures as they apply to the information resources under their care.

4. Definitions

- a. ***Information resource.***
This term includes information in any form and recorded on any media that is collected by or generated by any University User. Information resources also include all computing, networking and communications equipment and software that are used for information processing and storage that are owned by the University or used by the University under license or contract.

b. ***Information Owners.***

Information Owners are those members of the University community who have the primary responsibility for particular information. One becomes the Information Owner either by designation or by virtue of having acquired, developed, or created information resources for which no other party has information ownership. For example, for purposes of this Policy, the Library Director is the Information Owner of the library catalogs and related records; and the Registrar of the University is the Information Owner of student academic records. Faculty members are considered the Information Owners of their research and course materials; students are considered the Information Owners of their own work.

The term Information Owner as used here does not imply ownership in any legal sense, such as a holder of a copyright or patent. In this context, Information Owner means only the person with primary responsibility for an information resource.

c. ***Users.***

All members of the University community are “Users” of OLLU’s information resources, even if they do not have responsibility for managing the resources. Users include: students, faculty, staff, alumni, contractors, consultants, volunteers, and temporary employees.

d. ***Service Providers***

Service Providers are those offices, units, departments and individuals that manage significant information resources and systems for the purpose of making those resources available to others. They include the University’s Library, Instructional and Technology Services, the School of Business ECIS department and labs, the office of Alumni/Development, Communications and Marketing, Finance and Payroll, Student Finance, Human Resources, Planning, Research and Effectiveness, the Bookstore, University Police, and most Student Services and Enrollment Management offices.

e. ***Managers.***

Managers are those who oversee daily operations and the activities of other employees or users in a University office, unit or department.

5. Compliance

- a. All University department heads and administrators are responsible for monitoring employee and faculty compliance with this policy.
- b. Violations of this policy will be taken seriously and may result in disciplinary action according to standard University procedures.

6. Revision History

Version 1.0.0 Nov. 2006

Recommended by Administrative Council, Spring 2007