OIT	Information Technology Standard

Document Title:		
Standard for IT Security Roles and Responsibilities		
Approved By:	**Version:**	**Date:**
IT Council	1.0	March 14, 2007

Introduction

The Board of Regents' Information Technology policy and Section 12-112 of the Education article of the Maryland Code require that each institution within the University System of Maryland adopt policy that assigns roles and responsibilities with regard to information technology security.

Every member of the university community is responsible for the protection of the electronic data, applications, computer systems, networks, and accounts under their control. Users are expected to exercise the level of care appropriate to the sensitivity of the data stored on university systems and networks.

Roles and Responsibilities

All members of the university community play a role in the protection of the university's data and Information Technology resources. In particular:

- The Vice President/Chief Information Officer, with consultation from appropriate advisory groups, is responsible for the development and maintenance of university-wide information security standards, the implementation of those standards on university systems, and verification of compliance with those standards. The Office of Information Technology is responsible for the coordination of the university's Information Security Program which includes deployment of protective measures, incident management and investigation, and promotion of security awareness

- University Administrators (including Vice Presidents, Deans, Chairs, Directors.) within the university are responsible for identifying the resources necessary to coordinate information technology security within their unit. This includes the designation of an IT security contact that shall serve as a conduit for security information between the unit and the Office of Information Technology for purposes such as incident reports. Administrators are responsible for maintaining effective security within their organization.

- Individuals whose duties include network administration, programming, and system operation at the university are responsible for implementing measures to minimize the probability of a security incident involving systems and programs under their control. Such measures include the use of virus protection software, installation of vendor security updates, adherence with university security standards, and the monitoring of systems to detect anomalous activity. Incidents resulting in the potential or actual compromise of university computing resources must be promptly reported to the Security Officer in the Office of Information Technology.

- Individual users of the university network including those who access the network remotely are responsible for protecting their workstations, accounts, and passwords from unauthorized use and shall comply with the Policy for the Acceptable Use of Information Technology Resources.

Modification

- This standard will be reviewed and updated annually or as needed based on the recommendations of the Vice President/Chief Information Officer.

Version History

Version #	Date	Description of Changes	Revised By
1.0	3/14/07	Final document approved by IT Council	N/A