REVISION HISTORY

Revision No.	Revision Date	Authors	Description of Changes
01	07/16/2013	Ravi D Singh Executive Director, Quality Control, UMIT Connie Barrera Executive Director, IS and Compliance, UMIT	New Document

APPROVED BY

This Policy is established for Policies pertaining to information technology by the approval signatures below.

Name	Title	Signature	Date
Timothy Ramsay	Chief Information Security Officer	*SIGNATURE ON FILE*	26 Jul 2013
Steve Cawley	Chief Information Technology Officer	*SIGNATURE ON FILE*	26 Jul 2013

Information Security exists to further the mission of the University. The University is comprised of large and diverse populations with evolving needs related to information technology resources and data. University management is committed to safeguarding those resources while protecting and promoting academic freedom. Although intrinsic tension exists between the free exchange of ideas and information security, and can manifest itself in some circumstances, the requirements that follow have been identified to promote the best balance possible between information security and academic freedom.

PURPOSE:

This policy establishes a framework for developing policies that will:

- Be consistent with applicable laws, ethical norms, and accepted best practices
- Support the mission of IT and the University at large
- Achieve accountability by providing clear roles and responsibilities
- Define how IT conducts business

SCOPE:

This policy applies to all University employees, faculty, students, contractors, guests, consultants, temporary employees, and any other users with any responsibility regarding creation of and compliance with University policies.

DEFINITIONS:

- **Policy:** A statement of management philosophy and direction, established to provide guidance and assistance to the IT community in the conduct of various functional responsibilities.

- **Procedure:** a guideline or series of interrelated steps taken to help implement the policy.

- **Policy Initiator**: any faculty, staff member, or student who identifies a university-level issue, develops and submits a new or changed policy proposal.

- **Policy Owner**: the appropriate IT Officer (CIO, AVP, etc.) whose jurisdiction covers the subject matter of the policy.

- **Stakeholder**: the individual(s) or entity who will be impacted by the policy in some way.

- **Policy Administrator**: the CISO of IT Security or designee.

POLICY:

- New policies or changes to existing policies may be initiated, proposed and submitted to the policy owner by any member of the University.

- New policies or changes to existing policies will be reviewed and content validated by stakeholders and appropriate subject matter experts to ensure accurate, relevant and complete content.

- New policies and changes to existing policies must be approved and accepted by the senior IT Executive Committee or designee to become official.

- Policies will be independently maintained from supporting documents including but not limited to procedures, standards and guidelines.

- A current policy template must be used whenever drafting a new policy and/or updating policies at least yearly or when major changes occur to the environment.

- Any campus/business unit/departmental Policies must reference any applicable University-wide policies.

- To ensure ready access to University policies, the University will maintain an official Policies web page with the most current approved version of all policies and links to applicable supporting documents (i.e. procedures, standards, guidelines, etc.). The documents on the Policies web page will constitute the official electronic depository and serve as the sole source of retrieval. Therefore, separate copies of the policies must not be posted on alternate websites. Instead, links to the Policies web page should be used to direct individuals to any given policy from other web pages.

- Policies shall be reviewed every two years from the effective date and if necessary will be revised. Documentation of the biennial assessment will be maintained in the IT central files located in the IT office.

- If modifications are not required during the review process, the policy document will be signed by the authorized reviewer on the front page with the comment 'Reviewed, Revision not Required'. One year from date of signature, the policy document shall be reviewed and published as a new version regardless of any new changes.

RESPONSIBILITIES:

Policy Initiator:

- Identifies, proposes and submits new policies or revisions to existing policies.

Policy Owner:

- Reviews the new policies or revisions to existing policies submitted by the Policy Initiator.
- Validates the policy draft and its content by consulting with various subject matter experts and stakeholders.
- Evaluates and seeks to minimize the likely impact of the new or revised policy on the members of the University community

Stakeholders:

- Provide input on policy content and advice on any risk/impact that should be considered before the Policy is approved.

Policy Administrator:

- Proactively coordinates policy review and creation of new policies.
- Disseminates and seeks feedback regarding new or revised policies from stakeholders and subject matter experts.
- Prepares and submits final drafts to the senior Executive Committee or designee for final approval.
- Maintains copies of all signed IT policies and policy revisions.
- Places an electronic copy on the official Policy web site.
- Supports communication, implementation and training of all policies.

Executive Committee or designee:

- Approves and accepts the new or changed policy for it to become effective.

EXCEPTIONS:

Any requests for exceptions to this policy must be submitted in writing and will be reviewed on a case by case basis. Exceptions shall be permitted only after written approval from the Vice President of Information Technology or designee. This list of exceptions shall be reviewed annually and cancelled as required.

SANCTIONS:

Accounts and network access may be administratively suspended with or without notice by the University as per existing university regulations and due process, when, in the University's judgment, continued use of the University's resources may interfere with the work of others, place the University or others at risk, or violate University policy.

Known violations of the policy will be addressed by disciplinary policies and procedures applicable to the individual.

All known and/or suspected violations must be reported to the applicable Systems Administrator, who will report, as appropriate, to the applicable department. All such allegations of misuse will be investigated by the appropriate University administrative office with the assistance of the Department of Information Technology and the Department of Human Resources.

Penalties may include:

- Suspension or termination of access to computer and/or network resources;
- Suspension or termination of employment, to the extent authorized by other university published policies and procedures;
- Suspension or termination of contract computer and/or network services; or
- Criminal and/or civil prosecution.

ENFORCEMENT:

Chief Information Security Officer of designee (CISO) is Responsible for monitoring the enforcement of the policy.