REVISION HISTORY

<table>
<thead>
<tr>
<th>Revision No.</th>
<th>Revision Date</th>
<th>Authors</th>
<th>Description of Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>11/04/2013</td>
<td>CISO</td>
<td>Populate Into Standard Template</td>
</tr>
</tbody>
</table>

APPROVED BY

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
<th>Signature</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connie Barrera</td>
<td>Executive Director, Information Security and Compliance</td>
<td>Signature on file</td>
<td>12/04/2013</td>
</tr>
<tr>
<td>Tim Ramsay</td>
<td>Chief Information Security Officer</td>
<td>Signature on file</td>
<td>12/04/2013</td>
</tr>
</tbody>
</table>
PURPOSE:

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.

Information Technology Business Continuity Planning is critical to ensuring that in the event of a significant system interruption, the University can effectively recover information technology data and resources that enable business and academic processes. The Business Continuity and Disaster Recovery Policy establishes a framework for developing IT business continuity and disaster recovery plans.

SCOPE:

This policy applies to all University employees, faculty, students, contractors, guests, consultants, temporary employees, and any other users with any responsibility for Information Technology business continuity and disaster recovery processes.

DEFINITIONS:

- **System Administrator**: An individual who performs network/system administration duties and/or technical support of network/systems that are accessed by other people, systems, or services. Only full-time and permanent part-time employees of the University and/or third party vendors approved by IT may function as system/network administrators and/or data custodians.

- **University**: “University” refers to the University of Miami as a whole and includes all units.

POLICY:

Information Technology Comprehensive Business Continuity and Disaster Recovery Plans (“IT Continuity Plans”) must be developed that address disruptions to normal academic and business operations. These plans must be consistent with the broader University of Miami master plan and at a minimum must be reviewed and tested annually to ensure their viability during recovery. The plans must address recovery of information resources, personnel, processes, and applicable IT facilities for all campuses and sites.

These plans are designed to reduce the disruption to critical business and academic processes and the supporting information resources that may result from natural disasters and other events impacting the confidentiality, integrity and/or availability of such resources. All aspects of potential outages, ranging
from human error, equipment failure, utility failure, and natural disasters must be taken into account in a comprehensive planning document. These plans must be a combination of both preventative as well as recovery controls. System administrators and data custodians must be part of the planning process. The plans must:

- Be updated and tested no later than June 1st of each year with the results of the test documented.
- Remain up-to-date to include any software, hardware or application changes.
- List roles responsibilities and communication strategies in the event of a disaster.
- Be delivered and aggregated centrally to the Information Technology CIO.

**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 responsible Vice President or Information Technology designee of the respective campus. The list of exceptions shall be reviewed annually and cancelled as required.

**IMPLEMENTATION:**

**School/Division Leadership:**
- Responsible for requiring and supporting IT continuity and disaster recovery programs in their respective areas, and helping to assure that IT continuity and recovery measures are carried out in conjunction with other non-IT continuity and disaster recovery efforts

**System Administrator:**
- Responsible for planning and testing IT business continuity and disaster recovery plans.

**Chief Information Security Office:**
- Responsible for regular review of the IT business continuity and disaster recovery policy. This review will occur annually or when significant changes occur.

**Responsible Vice President or Information Technology CIO:**
- Responsible for reviewing and approving or denying exception requests.
- Responsible for reviewing exceptions yearly.
- Responsible for monitoring the enforcement of the policy.

**Individuals covered by this policy:**
- Responsible for taking reasonable steps to protect University computers and other IT resources assigned to them in the event of a pending disaster.
- Responsible for assuring that no steps taken by them in the aftermath of a disaster knowingly interfere with disaster recovery efforts
SANCTIONS:

Accounts and network access may be administratively suspended with or without notice by the University when, in the University's judgment, continued use of the University's resources may interfere with the work of others, places the University or others at risk, violates University policy, or interferes with disaster recovery efforts.

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

All known and/or suspected violations, or knowing interference with disaster recovery efforts must be reported to the applicable Systems Administrator, who will report, as appropriate, to the applicable Technology 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.

OTHER APPLICABLE POLICIES:

- University of Miami Disaster Preparation and Recovery Plan

ENFORCEMENT:

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