UNIVERSITY OF MIAMI

UNIVERSITY OF MIAMI POLICY AND PROCEDURE MANUAL

TITLE: Business Continuity and Disaster Recovery

REFERENCE: Revised

CATEGORY: Information Technology

PAGE: 1

SUPERSEDES: POL-UMIT-A135-006-01

APPROVER: David Ertel
Interim Senior Vice President
Business and Finance

VERSION: 2

EFFECTIVE: May 1, 2017

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.

I. PURPOSE:

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.

II. 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.

III. 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.

IV. 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.

V. PROCEDURE:

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.

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.

Violations:

Violations of this policy will be addressed by the procedure applicable to the individual.

Other Applicable Policies:

- University of Miami Disaster Preparation and Recovery Plan

Enforcement:
Chief Information Security Officer or designee (CISO) is responsible for monitoring the enforcement of the policy.