UNIVERSITY OF MIAMI

UNIVERSITY OF MIAMI POLICY AND PROCEDURE MANUAL

TITLE: Information Security Policy
REFERENCE: Revised
CATEGORY: Information Technology
PAGE: 1
SUPERSEDES: Version 2
APPROVER: Jacqueline A. Travisano
Executive Vice President
Chief Operating Officer
Business and Finance
VERSION: 3
EFFECTIVE: November 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, which 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:

The information security policy establishes a University-wide approach to information security. Information security supports and fosters the academic and business interests of the university. This policy is intended to ensure the confidentiality, integrity, and availability of information resources and data; reduce the risk of information loss by accidental or intentional modification, disclosure, or destruction. It preserves the University's rights and remedies in the event of such a loss by implementing best practices, current industry standards, along with effective and appropriate controls.

II. SCOPE:

This policy applies to all University employees, faculty, students, contractors, guests, consultants, temporary employees, and other users, including all personnel affiliated with third parties who have access to University information technology resources.

III. POLICY:

Information Security exists to further the mission of the University. The University comprises large and diverse populations requiring access to information systems. University management is committed to safeguarding those resources while recognizing academic freedom. Although intrinsic tension exists between the free exchange of ideas and information security and can manifest itself in some circumstances, the following identified framework is intended to promote the best balance possible between information security and academic freedom.

University management may become aware of situations that could place the University's facilities, employees, critical business and academic processes, critical business and

academic information, and intellectual property at risk or harm. These situations include, but are not limited to:

- Knowledge of existing or potential violations of University policy and procedure, legislative or industry required standards for protection of information.
- Knowledge of a situation that may potentially place the University's critical business and academic information or intellectual property at risk of being lost, altered, or unavailable.
- Terminated employees or other business representatives who continue to have access to facilities or Information Technology resources once access is no longer warranted.
- Changes to user access needs (e.g., employees who transfer to another department and employee promotions).
- Processes that may place the University's information at risk.
- Unsolicited requests for University's information from internal/external sources (e.g., questionnaires or third parties requesting organization financial and bio-data).
- Physical security or safety concerns.

All units must establish minimal requirements and best practices for the security domains listed below where appropriate. University management must ensure that employees are complying with security policies, standards, and guidelines.

Physical Security:

Physical security measures for controlling access to electronic information resources through physical means, including disaster controls, physical access controls, device and media controls, and procedural controls over financial instruments and maintenance records must be in place.

Access to data network facilities and other sensitive areas must be provided based on the principle of least privilege and the user's responsibilities.

Personnel Security:

The recruitment process must include control measures and security provisions. Appropriate background checks of individuals applying for employment, depending on the position and its associated responsibilities within the organization, must be conducted. Formal policies, procedures and processes must be in place to ensure all personnel who have access to sensitive information have the required authority as well as appropriate clearance. Upon employment all faculty and employees must be informed of and agree to the protection of confidential information.

Logical Security:

Access to data network resources must be controlled on the basis of "least privilege" and need to know. Adequate security must be provided to ensure the protection and maintenance of integrity, confidentiality and availability over the systems and information.

Third-party Applications and Data Centers:

Third-party applications, e.g. "cloud services" and third-party data centers that store or process University data protected under a legislative regulation, industry requirement or University policy must submit a third party audit report that covers the vendor's internal technology design and

operating controls. An audit report is an attestation to a service provider's internal controls as they relate to security, availability, processing integrity, confidentiality and privacy. A recognized security standard audit report or attestation applicable to the services provided must be obtained prior to conducting business and must be resubmitted as required.

Communications Security:

It is important to establish an efficient flow of information without compromising the integrity and confidentiality of such information. The University of Miami may share information with University employees, students, contractors, guests, consultants, temporary employees, and partner organizations which have a legitimate role. The University may also share information with non-partner organizations as required by law or by court orders/subpoenas. The appropriate information sharing protocol for each case must be established.

Systems Development:

All systems developments must comply with the information security policies of the University. All systems developments must include security issues in their consideration of new developments or modifications.

Risk Management:

A risk management program must be put in place to identify and mitigate risks to IT systems and to Protected Data throughout University systems. Risk assessments must be conducted periodically to identify and reduce possible threats to University information security. An assessment of risks must be conducted for each information system to ensure it is secured appropriately in a cost effective manner.

Disaster Recovery and Contingency Planning:

Disaster Recovery and contingency plans must be developed for dealing with emergency situations in the event of damage, failure, and/or other disabling events that could impact the critical business and academic processes and the information systems that support such processes. See Separate Policy Statement.

Security Incident Management:

Information Technology security incident response policy and procedures must be developed for dealing with security events that may require the full participation of Information Technology technical personnel as well as divisional leadership to manage the outcome properly. See Separate Policy Statement

Security Awareness, Training and Education:

All information resource users must be made aware of policies regarding access to, and appropriate use of University information resources, and especially of the need to guard Protected Data. Unit leaders play an important role in fostering an environment in which all members of the University community are "security aware." In particular cases, employees may need to receive formal security training. Unit leaders should periodically remind their employees to re-read this policy and the other IT security policies applicable to them and to understand the role they play in protecting University information resources.

University of Miami Guidance for Managing Third-party Access:

It is important to maintain the security posture of the University of Miami network infrastructure and only allow third-parties access to what is needed as part of their business/academic relationship with the University. Access by third parties must be controlled and only granted where there is a justified business/academic need. A risk assessment must be conducted to

determine if the security controls in place will meet the security requirements of the University. If feasible, security controls must be defined clearly in the contract language.

System Security Plan Policy:

Systems Security plans must be developed and documented for all IT FISMA related systems in accordance with NIST SP 800-18. Plans must be reviewed and updated when major system changes occur or at least once every three years.

IV. DEFINITIONS:

- **University:** "University" refers to the University of Miami as a whole and includes all units.
- **University Member/Affiliate:** Anyone associated with the University of Miami including, but not limited to, employees, students, contractors, guests, consultants, temporary employees, and any other users who have access to University resources.

V. PROCEDURE:

Information Security Privacy and Policy Council:

- Forwards proposed policies and recommendations for changes in policy as needed to the senior officials of the university, to the Academic Deans Policy Council, to the Information Technology and Advisory Committee or its successor, and to the Faculty Senate as appropriate.
- Responsible for promulgating University-wide policy to address the different domains identified within this policy.

University Member/Affiliate:

- Responsible for following policy requirements as required by their role.

Chief Information Security Office:

- Responsible for regular review of the Information Security Policy. The review will occur annually or when significant changes occur.

Responsible Vice President or Information Technology designee:

- Responsible for reviewing and approving or denying exception requests.
- Responsible for reviewing exceptions yearly.
- Responsible for monitoring the enforcement of the policy.

Violations:

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