UNIVERSITY OF MIAMI

UNIVERSITY OF MIAMI POLICY AND PROCEDURE MANUAL

TITLE: Change and Incident Management
REFERENCE: Reformat
CATEGORY: Information Technology
PAGE: 1
SUPERSEDES: POL-UMIT-A145-008-01
APPROVER: David Ertel
Interim Senior Vice President
Business and Finance
VERSION: 2
EFFECTIVE: May 16, 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:

The change and incident management policy is critical to Information Technology's ability to maintain a stable and secure data network environment throughout the University of Miami. This policy establishes responsibility and authority for change and incidents, and for disseminating that information to users who rely on network resources and services. The policy also sets requirements for managing changes and incidents to the production environment. Through this process, the University of Miami works to minimize any interruptions to operational functions and improve system reliability, security, and integrity.

II. SCOPE:

This policy applies to anyone who makes changes to information technology systems and/or makes changes to machines that containing protected data throughout the University of Miami.

III. POLICY:

Information Technology changes and incidents must be properly managed to ensure information resources are protected against unauthorized changes throughout a system's life cycle. The following minimal change and incident management requirements must be followed:

- A formal written change request must be submitted for all changes, both scheduled unscheduled. Change approval/authorization steps must be appropriate to the magnitude, risks and criticality of the change.
- A review of the request must be performed to determine any potential failures, and negative impact on any of the information technology services and/or resources.

- All changes must be formally approved by appropriate leadership before proceeding with the change. Except in urgent situations, the originator of a change may not serve as a technical assessor or managerial reviewer of that request even if otherwise qualified to do so.
- A configuration management log must be maintained for all changes
- All configuration changes must be tested and include assurances that implementation of the change will not cause any malfunctions to occur. End user experience testing is required.
- The change process requires post implementation validation of proper functioning of the change solution after it is in use.
- The use of protected data in a test environment should be avoided whenever possible and when not possible then strict access controls to the test environment must be implemented.

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 administrators.
- **Change:** Any modification to information technology systems i.e. computer systems, hardware, software, applications, and network components that affects the most current system baseline. This includes but is not limited to application installations and upgrades, operating system upgrades, configuration changes, web page modifications, and patch installations. It does not include files written by the computer user, other data files, e-mail messages and similar files provided they do not include any executable instructions or otherwise modify systems or operating software.
- **Current System Baseline:** The current system baseline represents the configuration of a system (the operating system, applications and configuration settings in place) at the time any change takes place.
- **Change Management:** The process for controlling modifications to hardware, software, firmware and documentation to ensure the information resources are protected against undocumented modifications before, during, and after system implementation.
- **Incident:** Unplanned occurrence causing system malfunction and/or service interruption.
- **University:** “University” refers to the University of Miami as a whole and includes all units.
- **Data Custodian:** The person responsible for, or the person with administrative control over, granting access to an organization's documents or electronic files while protecting the data as defined by the organization's security policy or its standard IT practices.
- **Protected Data:** Any data governed under Federal or State regulatory or compliance requirements such as HIPAA, FERPA, GLBA, PCI/DSS, Red Flag, and FISMA as well as data deemed critical to business and academic processes which, if compromised, may cause substantial harm and/or financial loss.
    - **HIPAA:** The Health Insurance Portability and Accountability Act of 1996 with the purpose of ensuring the privacy of a patient’s medical records.

- **FERPA:** The Family Educational Right and Privacy act of 1974 with the purpose of protecting the privacy of student education records.
- **FISMA:** The Federal Information Security Management act of 2002 recognizes the importance of information security to the economic and national security interests of the United States and as a result sets forth information security requirements that federal agencies and any other parties collaborating with such agencies must follow in an effort to effectively safeguard IT systems and the data they contain.
- **GLBA:** The Gramm-Leach-Bliley Act, also known as the Financial Services Modernization Act of 1999, contains privacy provisions requiring the protection of a consumer's financial information.
- **PCI/DSS:** Payment and Credit Card Industry Data Security Standards is guidance developed by the major credit card companies to help organizations that process card payments prevent credit card fraud, hacking and various other security issues. A company processing card payments must be PCI compliant or risk losing the ability to process credit card payments**.**
- **Red Flag:** A mandate developed by the Federal Trade Commission (FTC) requiring institutions to develop identity theft prevention programs.

V. PROCEDURE:

Change Requestor:

- Responsible for following the change control process and implementing the proposed solution.
- Responsible for all supporting change and incident management documentation including but not limited to, scope with acceptance sign off, test plan with results and user sign off, project/task plan, risk and impact analysis, live plan and post live implementation and issues assessment. Documentation should be available for a period of one year.

Data Custodian:

- Must be part of the change approval process
- Must be notified immediately of any incidents

Chief Information Security Office:

- Responsible for regular review of the Change and Incident Management Policy. The review will occur annually or when significant changes occur.

Responsible Vice President or Information Technology designee:

- Responsible for approving installation, modifications, and removal of all information technology throughout the University of Miami.
- 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.

Other Applicable Policies:
System Administrator Policy

Enforcement:

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