Business Continuity Management

ROWAN UNIVERSITY POLICY

Title: *Business Continuity Management Policy*
Subject: *Information Security*
Policy No: *ISO:2013:09*
Applies: *University-Wide*
Issuing Authority: Senior*Vice President for Information Resources and Technology and Chief Information Officer*
Responsible Officer: *Director of Information Security*
Adopted: *07/01/2013*
Last Revision: *07/02/2018*
Last Reviewed: *07/02/2018*

I. PURPOSE

A.This policy describes the Rowan University Business Continuity Management program, which is proactive and iterative in its approach to assess potential threats and ensure appropriate and resilient arrangements are in place. The Program is required to support the safety of our employees and secure critical resources (people, systems and locations) required to continue key business processes and minimize impacts in a timely, structured, and cost-effective manner, in the event of a business interruption incident.

B. Business Continuity Management's primary objective is to enable the executive and senior management to continue to manage and operate their business under adverse conditions, by leveraging appropriate resilience strategies, recovery objectives, and business continuity and crisis management plans.

II. ACCOUNTABILITY

Under the direction of the President, the Chief Information Officer, Director of Information Security, schools and business units, the Information Security Office (ISO) shall implement and ensure compliance with this policy.

III. APPLICABILITY

This policy applies specifically to all employees, deans, officers and directors of the University. Furthermore, management's accountability extends to ensuring all aspects of its Business Continuity Management's activity incorporate third party service providers and vendors.

IV. DEFINITIONS

Business Interruption - an event, whether anticipated or unanticipated, which disrupts the normal course of business operations within the university.

V. POLICY

A. Business Continuity Management Framework

Management will apply a consistent, University-wide approach to business continuity management through:

a. Governance
b. Education and Awareness

c. Analysis
d. Recovery Strategy and Plan
e. Maintenance
f. Outsourcing and Third Party Service Providers
g. Testing and Quality Assurance
h. Monitoring and Control

1. Governance
   Management will maintain an organizational structure that allows for the appropriate oversight and ownership of The University's Business Continuity Management activities at University-wide and business unit levels. The Information Security Office (ISO) will set University-wide strategy, policy, tools, guidelines, and standards, review business continuity activities, and co-ordinate University-wide threat /risk assessments, strategy and readiness reporting. Ultimate responsibility for implementing Business Continuity Management practices and developing business-specific policies and protocols rests with the executive and senior management of each business area. All lines of businesses must ensure that their policies address any unique regulatory or business requirements within their jurisdiction.

2. Education and Awareness
   The Information Security Office will communicate Business Continuity Management policies and processes to all business units and implement appropriate employee awareness and training programs to promote the understanding of all related policies, standards and guidelines.

3. Analysis
   On an annual basis, each school and all business unit must assess their risk tolerance and sensitivity to an interruption by completing the Business Impact Analysis ("BIA") process to establish a University-wide criticality ranking. This criticality ranking must be submitted to the Information Security Office for independent validation and approval. The criticality ranking establishes recovery targets and the rigor of business continuity activities. The following criteria (high, medium, low) are used for criticality ranking:

Ranking	**Criteria**
High	• Business functions are critical and must be recovered quickly (0-6hrs Maximum Downtime Tolerance). • Failure of business functions would have a significant operational, financial and/or reputational impact on The University. • Business functions are sensitive to interruptions and contain intricate and complex procedures and processes with multiple points of failure. • Heavy reliance on systems and/or external service providers.
Medium	• Business functions are moderately critical and recovery requirements are less demanding (7-48hrs Maximum Downtime Tolerance). • Failure of business functions would have a moderate operational, financial and/or reputational impact on The University. • Business functions are less sensitive to interruptions and experience changes less frequently. • Moderate reliance on systems and/or external service providers.

Low	• Business functions are of low complexity and recovery timeframes could be lengthy (>48hrs Maximum Downtime Tolerance). • Outages would have a minimal operational, financial and/or reputational impact on The University. • Business functions have minimal dependency on systems and/or external service providers.

4. Recovery Strategy and Plan
   All schools and business units must develop an appropriate and resilient recovery strategy and continuity plan. The plan must address the loss or failure of critical people (workforce), systems, locations, processes and suppliers to continue key business processes and must be supported by appropriate arrangements whether in-sourced or outsourced. The level of continuity and recovery capability shall be appropriate to the criticality ranking of the business, considering cost and risk mitigation as part of the strategy. The strategy must consider the nature, scale and complexity of the business to ensure it can reasonably continue to function and meet its various obligations in the event of an interruption.

5. Maintenance
   Deans and Executive Management must review Business Continuity Management plans annually or when a major change to critical people, systems, processes, suppliers or locations occurs. All schools and business units will have appropriate change management processes in place to ensure the plan is current, credible and practical.

6. Outsourcing – Third Party Service Providers
   All continuity and recovery plans are to incorporate appropriate arrangements for the potential failure of third party service providers to meet their obligations. This includes each school and business unit taking reasonable steps to ensuring that it has access to records or resources to allow it to sustain business operations and statutory obligations. Each school and business unit will ensure the recovery plans, testing results and contracts of external service providers, including any significant subcontractors, are sufficient to meet the University's business continuity and recovery requirements. The University's sponsoring school or business unit must ensure that arrangements comply with the Vendor Risk Management Practices established by the Information Security Office.

7. Testing
   Business management and IRT must test Business Continuity and Disaster Recovery Plans annually to ensure arrangements are sufficient to meet required continuity and recovery objectives. The criterion for test success is based on pre-established test objectives and must meet the minimum Business Continuity Management testing standards established by the Information Security Office. The extent of review and testing will be commensurate with the criticality of the business unit.

8. Quality Assurance
   Each school and business unit must implement a quality assurance process to ensure the required continuity, recovery and testing objectives are achieved. All business continuity plans and tests are subject to independent review by the Information Security Office. The Information Security Office along with each school and business unit must ensure appropriate employee education and awareness programs are in place, and staff is familiar with them to support overall resilience of the University.

9. Monitoring and Control

   The Information Security Office (ISO) will monitor and report on the status of University-wide business continuity management activities, plans, protocols and testing to each Dean and the Executive for each business unit on a periodic basis. Additionally, the ISO will provide regular reporting to the Board Risk Committee regarding the state of the University's Business Continuity Management Program and preparedness.

VI. ATTACHMENTS

A. Attachment 1, Roles and Responsibilities

B. Attachment 2, Non-Compliance and Sanctions

By Direction of the CIO:

Mira Lalovic-Hand,
SVP and Chief Information Officer

ATTACHMENT 1

ROLES and RESPONSIBILITIES

1. A. Board of Directors
   The Board Risk Committee will:
   a. Annually review and approve this any substantial changes to this policy.
   b. Maintain a general understanding of the scope of the policy and make inquiries of a responsible senior officer with respect to this policy.
   c. Review reports, as and when presented to the Board Risk Committee by executive management of the University, with respect to the outcome of significant business continuity events and the resulting action plans for mitigating recurrence.
2. Deans and Business Units
   All areas are to ensure that faculty, staff, and management are familiar with incident protocols for emergencies and business disruptions. Deans and Executive management is to ensure compliance to this Business Continuity Management Policy and its supporting standards and guidelines.
3. Information Resources and Technology (IRT)
   IRT is responsible for supporting the information systems and technology requirements of business management's Business Continuity Management activities. This includes supporting the development and implementation of appropriate strategies to recover infrastructure platforms and restore critical applications consistent with business management's continuity and recovery objectives.
   IRT is also responsible for overseeing the creation, execution, and testing of a formal Disaster Recovery (DR) Plan and activities related to the systems and infrastructure it supports on behalf of the businesses.
4. Information Security Office (ISO)
   The ISO is responsible for the oversight of university-wide Business Continuity Management and for making appropriate recommendations to the Board Risk Committee regarding BCP and DR strategies and activities.
5. Legal
   Upon engagement by the sponsoring business, legal supports the risk management objectives of this policy by providing advice and support with contracts impacted by this policy

ATTACHMENT 2

NON-COMPLIANCE AND SANCTIONS

Violations of this policy may subject the violator to disciplinary actions, up to or including termination of employment or dismissal from a school, and may subject the violator to penalties stipulated in applicable state and federal statutes. Sanctions shall be applied consistently to all violators regardless of job titles or level in the organization.