Data Backup

ROWAN UNIVERSITY POLICY

Title: *Data Backup Policy*
Subject: *Information Security*
Policy No: *ISO:2016:04*
Applies: *University-Wide*
Issuing Authority: Senior *Vice President for Information Resources and Chief Information Officer*
Responsible Officer: *Director of Information Security*
Date Adopted: *04/01/2016*
Last Revision: *07/03/2018*
Last Review: *07/03/2018*

I. PURPOSE

The purpose of this policy is to outline the requirements for performing periodic backups of University systems, applications, and data to ensure they are adequately preserved and protected in the event of accidental deletion, data corruption, system failure, or disaster.

II. ACCOUNTABILITY

Under the direction of the President, the Chief Information Officer and the University's Director of Information Security shall implement and ensure compliance with this policy. The Vice Presidents, Deans, and other members of management will implement this policy.

III. APPLICABILITY

This policy applies to any Rowan University faculty member, staff member, student, temporary employee, contractor, outside vendor, or visitor to campus ("User") who process and/or store University data.

IV. DEFINITIONS

1. *Availability*– the expectation that information is accessible by Rowan when needed.
2. *Confidentiality*– the expectation that only authorized individuals, processes, and systems will have access to Rowan's information.
3. *Integrity*– the expectation that Rowan's information will be protected from improper, unauthorized, destructive, or accidental changes.
4. *Rowan Community*– faculty, staff, non-employees, students, attending physicians, contractors, covered entities, agents, and any other third parties of Rowan.

V. REFERENCES

1. Acceptable Use Policy
2. Data Backup and Retention Procedures

VI. POLICY

1. One of the most critical functions an IT organization can undertake is ensuring a structured and highly formalized data backup policy and procedures are in place. Backups are a must for any organization, especially considering today's growing regulatory compliance landscape and the ever-increasing cyber

security threats for which businesses face on a daily basis. A well thought out, efficient, and reliable backup and recovery strategy is essential for ensuring the confidentiality, integrity, and availability (CIA) of critical data.

2. The University requires that all University data is backed up according to the following best practices:
    a. All University systems, applications and data must be backed up on a technically practicable schedule suitable to the criticality, integrity, and availability requirements, as defined by the data owner.
    b. Retention period of backups should be proportionate to the criticality, integrity, and availability needs of the data. At a minimum, backup copies must be retained for 30 days, when appropriate.
    c. Records must be kept detailing the backup environment (what data is backed up and where it is backed up).
    d. Backup schedules must be maintained and periodically reviewed (See Appendix A).
    e. Backups of confidential or sensitive information will be encrypted to the standards set forth in the university Encryption Policy.
    f. All University data should have at least one fully recoverable backup version stored in a secure, geographically diverse location from the primary location of the data.
    g. Recovery procedures for the restoration of data must be kept up to date.
    h. Backup and recovery documentation must be maintained and periodically reviewed and updated to account for new technology, business changes, and migration of applications to alternative platforms.
    i. Backup media must be clearly labeled.
3. Federal and state regulations pertaining to the long-term retention of information (e.g., financial records) will be met using separate archive policy and procedures, as determined by the Business Owner of the information. Long-term archive requirements are beyond the scope of this policy.
4. Non-Compliance and Sanctions
    a. 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.

By Direction of the CIO:

Mira Lalovic-Hand,
SVP and Chief Information Officer