Administrative Data Backup and Restoration Policy

1.0 Overview

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 vital 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.

The purpose of this policy is to ensure that necessary records and documents are adequately protected and maintained and to outline Information Technology's backup, restoration and retention policy for the server and administrative data systems in use at WPI.

2.0 Policy

- The University requires that all administrative data on IT managed servers is backed up according to the following best practices:
    - All University systems, applications, and administrative data must be backed up on a technically practicable schedule suitable to the criticality, integrity, and availability requirements, as defined by the data owner.
    - 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.
    - Records must be kept detailing the backup environment (what data is backed up and where it is backed up).
    - Backup schedules must be maintained and periodically reviewed (See Appendix A).
    - Backups of confidential or sensitive information will be encrypted.

- Recovery procedures for the restoration of administrative data must be kept up to date.
- In order to validate backup files and procedures, a restore from backup must be performed at least twice a year.
- 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.
- Backup media must be clearly labeled.

- Statutory regulations pertaining to the long-term retention of information (e.g., financial records, PII or other confidential data) 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. Please refer to Data Classification Policy and Data Retention and Destruction Policy for specific departmental data requirements.
- This policy will defer to administrative data retention and destruction schedules outlined in the Data Retention and Destruction Policy. This Backup Policy will not extend any data retention beyond what is defined by the data owners.

3.0 Enforcement

Any person that violates any of the measures found in this policy will be subject to disciplinary action, which may include termination or dismissal from WPI, or other appropriate disciplinary action.

4.0 Approval and Revisions

Policy Category: Institutional Risk & Compliance

Policy Approved By: Approved by WPI's Information Security, Risk and Compliance Committee on 2/15/19.

Policy Reviewed Annually By: Director, Systems Operations

Related University Policies:

Confidentiality Policy

Data Classification and Usage Policy

Records Retention and Destruction Policy

Last Modified:

2/12/2019

Appendix A - Data Retention Schedule

Functional Area	Record Class	Record Types	Retention	Backup	Archive to Cloud
Administrative Data	Departmental Shares	Standard forms, templates, letters, procedural documents	*Permanent unless deleted by user	30 days	Up to 15 months
	Home Directories	Personal Word Documents, Excel Files, Visio Diagrams, Personal work	*Permanent unless deleted by user	30 days	Up to 15 months

*(Recommended to remain on the main storage arrays. Should not be deleted.)