Policy Title: Information Technology Services – Data Backup and Restoration Policy

Policy Number:

Established: December 2017

Approved by:

Last Approval Date:

Revision Date:

Position Responsible for Maintaining and Administering the Policy: Executive Director, Information Technology Services

Contact: Ryan Kenney, Executive Director, IT Services, (519) 253-3000 ext. 2740

Table of Contents

Policy Statement

Data backup and restoration activities are intended to provide redundancy and recovery capabilities that may result from system failures, catastrophic occurrences, or human error. This Policy outlines the terms under which data is backed up and restored within Information Technology (IT) Services.

Purpose

The purpose of this Policy is to define the standards for data backup and restoration performed within IT Services.

Scope

This Policy applies to all University faculties, departments and associated stakeholders for whom IT Services performs backups of data. More specifically, these backups may include, but not be limited to files, folders, disks, and email.

Please note that backups do not include individual desktop workstations (i.e. personal, local drives) and clients with these specific requirements should seek potential alternate solutions (i.e. network) to satisfy these needs.

.Responsibilities:

1. IT Services has the responsibility to:
    - Provide specified services and advice to clients
2. Client area receiving the specified service has the responsibility to:
    - Clearly specify the requirements of the service request
    - Acknowledge that any fees for service (as may be applicable) will be incurred
    - Verify the service has been received
    - Provide funding to cover the cost of the service as agreed
3. IT Steering Committee has the responsibility to:
    - Regularly review this Policy
    - Provide feedback and guidance on this Policy
    - Approve amendments to this Policy

Exceptions to Policy
The Executive Director, IT Services may determine that certain situations or circumstances require exceptions to this Policy in order to best serve the interests of the University. Such decisions should be communicated in writing to the Executive Director, IT Services and should include the exact nature of the exception and, if appropriate, the time period during which the exception should be granted.

Cross-References

None

Definitions

None

Procedures

When a client area request these services, IT Services will be responsible (where applicable) to:

- Utilize an industry standard storage management product to automate the data backup process. This process will be comprised of a central server, running at an agreed upon interval as determined by IT Services to provide incremental backups (i.e. weekly, monthly, annual and / or term) as may be required
- In the event of a catastrophic occurrence (e.g. fire, earthquake, etc.), prioritize the restoration based on:
    - Nature and extent of the situation
    - Relative importance of the individual system and / or data to support the continued operations of the University

Conditions
- Files stored on a network server must be on the server for a duration sufficiently long enough to reach a scheduled backup cycle in order to be recoverable. Files that are accidentally deleted, corrupted, or overwritten on network drives that have not made it into the backup cycle, may not be available for recovery
- Efforts to complete data recovery will be performed by IT Services as quickly as is possible. Instant data recovery will not be available.
- Individual file restoration will be a "best effort" service and may take a period of several hours to several days to complete
- Issues resulting from catastrophic occurrence or other impacting events (e.g. power surge, etc.) that are beyond the control of IT Services staff may impact ability to backup and restore data

Review Process for Policy

This Policy will be reviewed every five (5) years. There may be certain circumstances that may cause for the review of the Policy prior to that date: changes in legislation that affect the Policy; a specific incident triggers a review of the Policy; there is a request made by Senior Management or the Board of Governors to review the Policy.

Process for Communicating Policy

The policy will be posted on the University of Windsor's IT Services website, within two weeks of the approval of the Policy. Separate notifications may also be sent via e-mail or other means to Departments directly affected by the Policy, or in some cases, the broader campus community if deemed applicable.

Contact Information
Inquiries regarding the policy should be directed to Executive Director, IT Services or appropriate individual in the Department where the policy was developed, as per the contact information at the introduction of the Policy.