


| | | | |
|--|-----------------------------------|--|---|
| Name of Policy: Information technology disaster recovery and back-up policy. | |  Original Effective date: July 28, 2008 | |
| Policy Number: 3364-65-04 | | | |
| Approving Officer: President | | | |
| Responsible Agent: Vice President of Information Technology | | | |
| Scope: all University campuses (for assets maintained by Information Technology) | | | |
| X | New policy proposal | <input type="checkbox"/> | Minor/technical revision of existing policy |
| <input type="checkbox"/> | Major revision of existing policy | <input type="checkbox"/> | Reaffirmation of existing policy |

(A) Policy statement

Information technology is committed to ensuring that information technology’s resources and information stores are appropriately backed-up to support recovery and business resumption efforts following accidental deletion, system corruption, and/or physical loss or damage.

(B) Purpose

To ensure that information technology’s procurement and development life-cycle incorporates disaster recovery and back-up methodologies that will enable recovery and subsequent business resumption following accidental deletion, system corruption, and/or physical loss or damage.

(C) Scope

Compliance with this policy is mandatory for procurement and development efforts for infrastructure and server-based systems/applications managed by information technology to include, but not limited to, data and telecom infrastructure, data center environmental, servers, and data storage solutions initiated following the policy’s effective date.

Existing systems and procurement/development efforts initiated prior to this policy’s effective date identified as having a criticality rating of high or medium will incorporate the concepts addressed in this policy as appropriate for the systems life-cycle status. As a minimum, disaster recovery and back-up service level agreements (SLA) will be developed for all high/medium criticality systems.

(D) University of Toledo policy and applicable guidance

- (a) CFR 164.308(a)(7) for HIPAA
- (b) Joint Commission standard IM.2.30 for continuity of information

(E) Procedure

Information technology directors and team leads will incorporate disaster recovery and back-up planning into their procurement and development efforts throughout the life-cycle of information technology applications, systems, and infrastructure. These efforts will be made to minimize the impacts to university functions due to accidental deletions, system corruption, and/or physical loss or damage.

Planning will minimally include:

- (a) Resource criticality
- (b) Data back-up requirements
- (c) Disaster recovery methodology

Standard policies for back-up, recovery, and retention are defined as follows. Any requirements for deviations from standard policies should be specifically identified and coordinated with the back-up administrator.

Backup policy:

All data will be backed up according to the university information technology standard backup policy unless otherwise requested. The data owner is responsible for establishing the criticality of the data. Any additional retention needs must include a business case statement as deviations from the standard incur additional costs to the university.

Standard server policy:

The standard server policy will create a full copy of the server minus any network mounted shares. This includes system state files such as the registry and active system related settings. Fourteen versions of a file will be kept on the backup system and the data retention will be set at fourteen days.

Recovery and retention:

Recovery times and points will depend on the amount of data involved and the state of the machine at the time of the request. Retention policies are flexible and can be configured to handle file revisioning. Back-up media will be stored in a secure controlled environment utilizing best practices for offsite data storage.

Note: While point in time recovery may be achievable for day-to-day data recovery purposes, the recovery point for data recovered following a disaster utilizing back-up media stored off-site will be based upon the latest data written to the off-site media. This would potentially result in the loss of up to forty-eight hours of data based on standard back-up policies.

Additional information: Windows shadow backup service is supported and if needed can be configured to facilitate the capture of “in-use” and “locked” files. Some file cannot be captured even with the shadow copy service (i.e. SQL databases) and will need to be saved during periods when the file is not locked or in use.

Responsibilities:

Overall responsibility for policy compliance resides with IT senior management; however, functional leads should initiate and maintain disaster recovery and back-up planning documentation specific to their areas of responsibility. For application driven systems, the system analyst maintains overall responsibility for documentation of the disaster recovery and back-up requirements using the Disaster Recovery and Back-Up Service Level (SLA) form.

The business continuity administrator will facilitate the disaster recovery planning process to ensure management objectives for system recovery are met in a fiscally responsible manner within information technology’s strategic plan and will maintain a repository of completed disaster recovery and back-up SLAs.

The back-up administrator will facilitate the back-up of data and servers per coordinated disaster recovery and back-up SLAs and maintain the ability to implement restoration procedures, locally and off-site, following accidental deletion, system corruption, and/or physical loss or damage. Back-up strategies provide for off-site storage and will be accomplished in accordance with management objectives, best practices, and current data retention standards.

Required documentation:

Compliance with this policy will be documented through use of the disaster recovery and back-up service level agreement (SLA) form located in Appendix A to this policy.

Information technology life-cycle:

During the information technology life-cycle, depicted in figure 1, there are multiple phases that require attention as to how disaster recovery and associated back-ups will be accomplished.

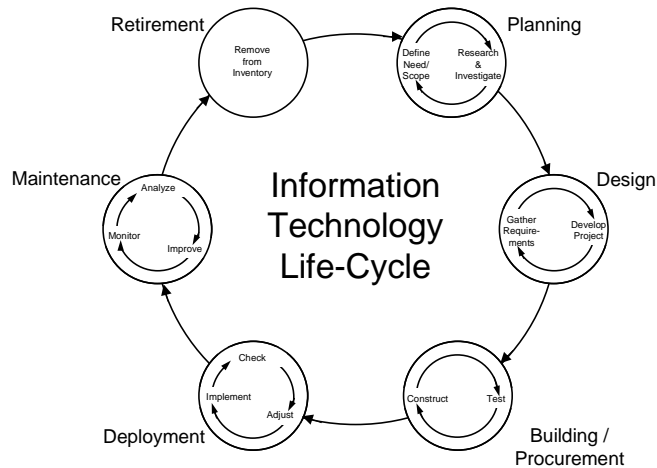


Figure 1: Information Technology Life-Cycle

Planning / Design:

Disaster recovery and back-up methodologies need to be initially considered during the planning and design phases of any information technology project. During these phases the criticality of the system should be identified so that appropriate disaster recovery methodologies can be explored and pursued during the procurement process.

Building / Procurement:

Disaster recovery and back-up requirements must be considered during the building and procurement phase as these needs may drive technical and financial considerations in order to meet recovery time objectives (RTO) and recovery point objectives (RPO) necessitated by the end-user community.

Deployment:

Upon deployment it is imperative that disaster recovery and back-up methodologies be defined and implemented.

Maintenance:

During the maintenance phase, the disaster recovery and back-up SLA must be updated to keep pace with changes made to deployed systems. Currency of this documentation will ensure common understanding among all involved and that associated strategies remain current.

Retirement:

The business continuity administrator and the back-up administrator should be notified when any system is retired and will no longer require disaster recovery and back-up support. The termination of any disaster recovery and/or back-up plans will ensure that limited University of Toledo resources are not expended when no longer necessary.

(F) Definitions:

Criticality rating – a method of identifying system importance for recovery purposes. Generally ratings will be based on the recovery time objective (RTO), but may be inflated due to additional factors. As a general guide:

- High; RTO < 48 hours
- Medium; RTO < 7 days, but > 48 hours
- Low; RTO > 7 days

Dependencies – any key relationships to other applications or equipment that would impact the utility of the application if they are not functional.

Disaster recovery methodology – there are multiple methodologies that can be employed for disaster recovery planning including, but not limited to:

- Rapid purchase
This methodology is most applicable for commodity items that can be rapidly procured from multiple vendor sources and locally installed/recovered within University of Toledo facilities or other identified computer centers within the identified recovery time objective (RTO). When this methodology is utilized, at least two (2) vendors will be identified and a rapid purchase agreement is highly recommended.

An additional option is to contract for the storage of unpowered systems to be stored on, or near, university property that can quickly be utilized if needed. Contracts of this type would entail full purchase price cost when the equipment is used but greatly decreases procurement time.

- University maintained back-up systems
This methodology relies upon the use of university maintained systems that can be utilized in a disaster recovery situation. Potential solutions include:
 - The use of currently installed equipment used for lower priority systems (e.g. test servers).
 - The use of virtualization fail-over methods on existing equipment
 - The use of dedicated back-up systems. Note: This option entails increased costs and overhead and may be applicable only for the most critical systems.

Note: The use of university maintained equipment to meet disaster recovery needs entails using equipment geographically dislocated from the primary location (e.g. Dowling Hall and the University Computer Center).

- Off-site contracts

Likely, the most costly of the disaster recovery methodologies is an off-site contract with a facility providing hot-site capability. The use of this option should only be explored for high criticality systems when other options have been exhausted.

Minimum recovery hardware – the hardware required to operate the intended system during the recovery period at an acceptable performance level. Note: During recovery some degradation of performance can be expected as this may be a temporary solution.

Off-site facility – based on the recognized threats to The University of Toledo computing environments, use of alternate campus (e.g. main campus and health science campus) facilities to meet off-site disaster recovery requirements may not be an acceptable risk identified by management.

Recovery point objective - a point in time to which data must be restored in order to be acceptable to the owner(s) of the processes supported by that data. (e.g. How recent must back-ups be?)

Recovery time objective - the boundary of time and service level within which a business process must be accomplished to avoid unacceptable consequences associated with a break in continuity. (e.g. How quickly do we need to have the application back up and running?)

| | |
|--|--|
| <p>Approved by:</p> <p><u>/s/ laj</u> Lloyd A. Jacobs, M.D. President</p> <p><u>August 12, 2008</u> Date</p> <p>Review/Revision Completed by: <i>Director, IT Administration</i> <i>Director, IT Operations/Infrastructure</i> <i>Director, Clinical Informatics</i></p> | <p>Policies Superseded by This Policy:</p> <ul style="list-style-type: none">• <i>024 Backup Policy (former Health Science Campus Policy, revision date 05/ 2005)</i> <p>Initial effective date: July 28, 2008 Review/Revision Date: Next review date: July 28, 2011</p> |
|--|--|

Disaster Recovery and Back-Up Service Level Agreement (SLA)

Application and Server Information

| | | | |
|------------------------|--|---------------------------|--|
| Server Name: | | Application Name: | |
| IT Analyst: | | Dept./Stakeholder: | |
| Phone: | | Phone: | |
| Hardware: | | Operating Sys: | |
| Application(s): | | | |

Disaster Recovery Information

| | |
|--|--------------------------------|
| Criticality Rating: | _____ High _____ Med _____ Low |
| Recovery Time Objective (RTO): | _____ Days _____ Hours |
| Recovery Point Objective (RPO): | _____ Hours |
| Dependencies: | |
| Minimum Recovery Hardware: | |
| DR Methodology: | |
| Vendors for DR: | |

Backup Information

| | | | |
|------------------------|-----------------------------|-------------------------------------|-----------------|
| Backup Type: | Backup Day and Time: | | |
| ___ No Backup Required | Please indicate reason: | | |
| ___ Nightly | Requested Time: | | Scheduled Time: |
| ___ Weekly | Time: _____ | Day: ___S___M___T___W___Th___F___Sa | |
| ___ Monthly | Time: _____ | Day of Month: _____ | |

Retention Needs – list any files or directories that have retention needs beyond the standard server retention

| File/Directory Specification: | Management Class |
|--------------------------------------|-------------------------|
| | |
| | |
| | |

| | |
|-----------------------|--|
| Business Case: | |
|-----------------------|--|

Exclusions – enter any files or directories that can be explicitly excluded from backups (ie log directories)

| File/Directory Specification: |
|--------------------------------------|
| |
| |
| |
| |

Acceptance

| | | | |
|---|--------------|---------------|--------------|
| Dept./Stakeholder Contact: | Sign: | Print: | Date: |
| IT Systems Analyst Team Lead: | Sign: | Print: | Date: |
| Business Continuity Administrator: | Sign: | Print: | Date: |
| Backup Administrator: | Sign: | Print: | Date: |
| Comments: | | | |