# COMMONWEALTH OF PENNSYLVANIA

# HEALTH & HUMAN SERVICES IT DELIVERY CENTER

# INFORMATION TECHNOLOGY GUIDELINE

|  |  |
| --- | --- |
| Name of Guideline: | Number: |
| **Recovery Planning** | **GDL-IOS002** |
| Domain: | Category: |
| **Operations and Support** | **Recovery Planning** |
| Date Issued: **2/14/2020** | Issued by Direction Of:  **Howard J. Eckman** |
| Date Revised: **9/10/2020** | **Operations Optimization & Support Manager** |
|  | **Health & Human Services Delivery Center** |

**Abstract:**

In the event of a system failure resulting in a need to restore data to its enterprise systems, the Health & Human Services Information Technology Delivery Center (HHS IT DC)requires a recovery plan. The recovery plan for HHS IT DC entails the use of a disk backup system.

**General:**

The purpose of this document is to provide backup and recovery requirements and standards for enterprise systems.

**Guideline:**

**Backup and Restoration for HHS IT DC Enterprise Systems**

Backup/Recovery performance, availability, and operational automation requirements are:

* Raised-floor Unix and NT systems running business/mission critical applications.
* Raised-floor Unix and NT systems running very large databases (VLDBs) at HHS IT DC. These are Oracle, SQL, Unisys relational and hierarchal databases.
* Windows 2008, 2012, 2016 serves, Linux servers, Virtual servers
* Mobile or remote desktop systems.
* Shared disk storage systemor segmented-drive configurations.
* Dedicated network connections between the backup server and its clients.
* The product used for the backup process must provide adequate tracing and error messaging diagnostic functions. Error messages must provide details clearly.

Vendor plans for integrating new functions for non-disruptive backup and rapid application recovery into the backup/recovery processes must be evaluated. Area to evaluate include:

* Hardware and software-based point-in-time replication functions.
* Intelligent storage-server data-mover functions.
* DBMS and application backup *proxy copy* APIs.
* Block-level change-capture functions.

*Client-backup/recovery functionality:*Basic client-backup/recovery functions that should be implemented by any enterprise-class product include end-user and administrator-initiated requests of operational staff for:

* Backup and recovery.
* Point-in-time recovery, recovery to alternative directories and systems, and inclusion/exclusion filtering.
* Advanced functions include product support for automated *bare metal* recovery and direct client-read access to the server back store.

*Backup/recovery-process monitoring, reporting and supplemental automation:* Many organizations have a requirement for comprehensive reporting and analysis functions, including:

* Service-level reporting.
* Service-level management (external backup-process monitoring and recovery).
* Proactive service-level analysis (backup window trending and component analysis).
* Basic reporting and a command-level interface for external management.
* Automation functions that enable the integration of backup/recovery and storage resource-management products.

**Database Backup and Recovery Considerations**

The traditional backup methods are based upon a periodic, full, physical database backup in combination with the archival of intervening transaction logs. Database recovery involves a restoration of the full backup, followed by a reapplication of transaction logs.

**A best business practice for a general approach to a high performance VLDB backup is to maximize disk-read and tape-write data rates through multitasking, parallelism, and data-stream consolidation.**

Software components that require backup procedures:

* Server operating system.
* File system.
* Database storage-management interface and the storage-management software.
* When general-purpose file systems are used, throughput limits may be introduced. (Veritas software provides a file system that is optimized for use under databases).

**Backup/Recovery Types**

In general, all backups regardless of the platform on which they are housed and run contain a variety of data types. When developing backup strategies, the person(s) conducting the backup must decide on what information to copy. The basic backup types include, but are not limited to:

* Whole database
* Table space
* Data file
* Control file
* Archived redo log
* Parameter file
* Password file
* Full backup to disk of database, data storage systems, and server operation system.
* Backup to disk of selected files or software.
* Backup to disk of files and software that has changed since previous backup.
* Granular incremental backup to disk of databases and file system replicas that are pre-staged for recovery and versioned.

**HHS IT DC Operational Backup Standards**

* Weekly
  + Full backup to disk of database, file systems, and server operation system.
  + Backup to disk of selected files or software.
* Daily
  + Backup to diskof selected files or software.
  + Backup to disk of files and software that has changed since previous backup.
  + Granular incremental backup to disk of databases and file system replicas that are pre-staged for recovery and versioned.

**HHS IT DC Operational Recovery Standards**

* Operational staff can recover selected files, when requested, with scripts/runs.
* Operational staff must have database approval before any database recovery scripts/runs can be used to recover the database.
* Operational staff must have engineering approval before any database recovery scripts/runs is used to recover server system software.

**Disaster Recovery and Contingency Plans**

Loss of access to **HHS IT DC** is not at present covered by business continuity plans. Loss of services from a disaster are not presently covered.

**Refresh Schedule:**

All guidelines and referenced documentation identified in this document will be subject to review and possible revision annually or upon request by the HHS Information Technology Delivery Center Domain Leads.

**Standard Revision Log:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Change Date** | **Version** | **Change Description** | **Author and Organization** |
| 1/15/2020 | 1.0 | New Organization/Review Content | Paul Barkman HHS IT DC |
| 9/10/2020 | 1.1 | Signature removed, identity protection | P. Gillingham HHS DC TSO |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |