# COMMONWEALTH OF PENNSYLVANIA

# HEALTH & HUMAN SERVICES DELIVERY CENTER

# INFORMATION TECHNOLOGY GUIDELINE

|  |  |
| --- | --- |
| Name of Guideline: | Number: |
| **Backup and Restoration**  **of Enterprise Systems** | **GDL-IOS001** |
| Domain: | Category: |
| **Operations** | **Recovery Planning / Backup and Restoration Procedures** |
| Date Issued: | Issued by Direction Of:  **Howard J. Eckman** |
| **2/14/2020** |  |
| Date Revised: | **Operations Optimization & Support Manager** |
| **9/10/2020** | **Health & Human Services Delivery Center** |

**Abstract:**

The Health & Human Services Delivery Center (HHS DC) is committed to providing the best security and business continuity for its enterprise server systems. HHS DC has established enterprise-wide teams and sub teams to identify the needs to implement a disaster recovery plan for its network server applications and data storage systems, that include, but are not limited too; Windows 2012, Windows 2016, and VMware.

**General:**

This team effort is being coordinated by the Technology Services Office of the HHS DC and includes members of the other offices and bureaus which include: Departments of Health (DOH), Human Services (DHS), Aging (PDA), Drug and Alcohol Programs (DDAP) and Military and Veterans Affairs (DMVA) business applications.

The purpose of this document is to detail the backup and restoration plan that identifies the requirements and guidelines to implement a comprehensive restoration of Health and Human Services enterprise server systems and mission critical applications.

Please refer to the Database Backups documentation on Data Domain for a more detailed explanation of Data Base centric processes, procedures, and best practices.

Intranet: <http://mydhs/cs/groups/webcontent/documents/document/p_032166.pdf>

Internet: <https://www.dhs.pa.gov/providers/Providers/Documents/Business%20and%20Tech%20Standards/Data%20Domain/p_032166-DatabaseBackups.pdf>

**Guideline:**

# Backup/Recovery Requirements

The backup/recovery performance, availability, and operational automation requirements are:

* Business and mission critical applications must be run on Windows systems and housed in enterprise-controlled environments.
* Large databases (VLDBs) must be run on Windows systems, or Linux and housed in enterprise-controlled environments. (Oracle and Microsoft SQL)
* Microsoft Windows file servers(most are being replaced by One Drive, SharePoint, and Shared disk storage systems.
* Mobile or remote desktop systems.
* The backup product must provide adequate diagnostic instrumentation in the form of trace facilities, and the detailed, comprehensible error messaging to provide clear detail.

# Needed Evaluation of Plans for New Functions

HHS needs to evaluate new technology for integrating enterprise systems with new functions that enable non-disruptive backup and rapid application recovery. These plans are:

* Hardware and software-based point-in-time replication functions
* Intelligent storage-server data-mover functions
* Database Management Systems (DBMS) and application backup “proxy copy” APIs
* Block-level change-capture functions

Client-backup/recovery Functionality

Basic client-backup/recovery functions include end-user and administrator-initiated requests of operational staff for:

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

Backup/Recovery-process Monitoring, Reporting, and Supplemental Automation

Many organizations have a requirement for supporting 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

Traditional backup methods are periodic, full, physical database backups in combination with the archival of intervening transaction logs. Please refer to Data Base Backups STD-DMS006 at Database Backups on the internet for a more detailed explanation of the current processes.

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)

Data Types

In general, all backups, regardless of the platform on which they are housed and run, contain a variety of types of data. When developing backup strategies, the person(s) conducting the backup must decide what information to copy.

Types of Backup/Recovery for Servers

* Best available recovery point of database, file systems, and server operation system to disk
* Backup of selected files or software to disk
* Backup of files and software that has changed since previous backup
* Granular incremental backup of databases and file system replicas that are prestaged for recovery and versioned to disk

Types of Backup/Recovery for Database

* Point in Time
* Full Cold Backup
* Logical Backups
* Schema/User level
* Incremental
* Ad hoc backups when requested or deemed necessary by DBA

Operational Backup Standards

Weekly Backups

* Full backup of database, file systems, and server operation system to disk (as application dependent)
* Backup of selected files or software to disk.

Daily Backups

* Backup of selected files or software to disk:
  + Backup of files and software that has changed since previous backup
  + Granular incremental backup of databases and file system replicas that are prestaged for recovery and versioned to disk

Operational Recovery Standards

Operational Recovery Standards follow:

* Operational staff can recover selected files, when requested, with scripts/runs
* Database administrator (DBA) will provide assistance in running database recovery scripts/runs to recover the database
* Operational staff must have approval of the appropriate section of the Technology Services Office before using any runs to recover server system software.

# Disaster Recovery and Contingency Plans

Business continuity plans do not cover loss of access to Enterprise business systems supported by HHS DC. Loss of services from a disaster is not 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 Delivery Center Domain Leads.

**Standard Revision Log:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Change Date** | **Version** | **Change Description** | **Author and Organization** |
| 1/15/2020 | 1.0 | New Organization/Content Review | Paul Barkman HHS IT DC |
| 9/10/2020 | 1.1 | Removal of Signature/Org Correction | Michael E. Sites HHS DC/TSO |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |