INFORMATION BACK-UP POLICY

OPS.075

Approved By:	**Chief Operating Officer**	Effective Date:	**02/28/10**
Distribution:	**Executive Team, Information Technology; Facilities; Site Administrators; Site Specialists**	Revision Date(s):	**N/A**
		Last Revised:	**N/A**
		Retired Date:	**N/A**

PURPOSE

An information back-up policy is similar to an insurance policy: it provides the last line of defense against data loss and is sometimes the only way to recover from a hardware failure, natural disaster, data corruption or a security incident. A back-up policy is related closely to a disaster recovery policy, but since it protects against events that are relatively likely to occur, in addition to those more rare incidents, in practice it will be used more frequently than a contingency planning document. ODCHC's back-up policy is among its most important policies. The purpose of this policy is to provide a consistent framework to apply to the process of protecting and assuring back-up of essential ODCHC data. The policy provides specific information to ensure back-ups are available and useful when needed; whether to simply recover a specific file or implement a larger-scale recovery effort. This policy applies to all data stored on ODCHC corporate systems and covers the type of data to be backed-up, frequency of back-ups, storage of back-ups, retention of back-ups and restoration procedures.

POLICY

It is the policy of ODCHC to identify, back-up (copy), secure and protect, and retain that data stored on ODCHC computer and electronic systems deemed critical to the organization.

PROTOCOL

1. **Definitions**: The following definitions apply to the terms used throughout this policy:
   - 1A. **Back-Up**: To copy data to a second location solely for the purpose of the safe-keeping of such data.
   - 1B. **Back-Up Media**: Any storage devices that are used to maintain data for back-up purposes. Back-Up media include magnetic tapes, CDs, DVDs or hard drives.
   - 1C. **Full-Back-Up**: A back-up that makes a complete copy of the target data.
   - 1D. **Incremental Back-Up**: A back-up that only backs-up files that have changed in a designated time period, typically since the last back-up was run.
   - 1E. **Restoration** (also called "recovery"): The process of restoring the data from its back-up state to its normal state so that it can be used and accessed in a regular manner.

2. **Identification of Critical Data**

   The ODCHC Compliance Officer and Executive Team identify that data considered most critical to its operations in keeping with local, state and federal guidelines and regulations (see OPS.018 Records Retention). Such data is given the highest priority during the back-up process. Other data not considered most critical will be protected and preserved in keeping with this policy but may not receive the highest priority during the back-up process. The back-up process balances the importance of the data to be backed-up with the burden such back-ups place on the users, network resources and the designated back-up administrator. Data to be backed-up will include:
   - 2A. All data determined to be critical to ODCHC operations and employee job performance;
   - 2B. All information stored on the ODCHC file server(s) and email server(s). It is the individual user's responsibility to ensure that any individual data considered to be of importance is moved to files related to servers subject to high priority back-up.
   - 2C. All information stored on network servers, which may include web servers, database servers, domain controllers, firewalls and remote access servers.

3. **Frequency**

   Back-up frequency is critical to successful data recovery and system integrity. ODCHC has determined that incremental back-up will occur daily and full system back-up will occur one each week.

4. **Off-Site Rotation**

   Geographic separation of the back-up media must be maintained, to the extent possible and reasonable, in order to protect such from fire, flood or other regional or large-scale catastrophes. Offsite storage must be balanced with the time required to recover the data in keeping with ODCHC's up-time requirements. ODCHC has determined that back-up media must be rotated off-site at least per day.

Approved By:	**Chief Operating Officer**	Effective Date:	**02/28/10**
Distribution:	**Executive Team, Information Technology; Facilities; Site Administrators; Site Specialists**	Revision Date(s):	**N/A**
		Last Revised:	**N/A**
		Retired Date:	**N/A**

5. Back-Up Storage

Storage of back-up media must recognize the importance, confidential nature and time-sensitivity of the data being stored. ODCHC has determined the following guidelines for back-up storage:

5A. When stored on-site, back-up media must be stored in fireproof containers in an access-controlled area.

5B. When shipped off-site, a hardened facility (i.e., commercial back-up service) that uses accepted methods of environmental controls, including fire suppression, must be used to secure the integrity of the back-up media. If a back-up service is used, rigorous security procedures must be developed and maintained, which will include, at a minimum, credential-verification and signature of the back-up service courier.

5C. Online back-up services are allowable if the service meets the criteria specified herein. Confidential data must be encrypted using industry-standard algorithms to protect against data loss.

6. Back-Up Retention

When determining the time required for back-up retention, ODCHC will review what number of stored copies of back-up data is sufficient to effectively mitigate risk while preserving required data. Back-up retention will be in keeping with other ODCHC records retention policies, specifically OPS.018 Records Retention. ODCHC has determined that incremental back-ups must be saved for at least one month and full-quarterly back-up will be saved indefinitely.

7. Restoration Procedures and Documentation

Data restoration procedures will be tested and documented. Documentation will include designation of responsible personnel and roles, how restoration is performed, under what circumstances restoration will be performed, and how long it should take to restore what types of data. The Information Technologies Director will maintain restoration documentation. Testing of the restoration procedures will be performed at least twice a year and when any change to software or equipment is made which may impact the back-up and/or restoration system.

8. Expiration of Back-Up Media

Certain types of back-up media, such as magnetic tape, have limited functional lifespans. After a certain amount of time in service the medica can no longer be considered dependable. When back-up media is put into service, the date of first use will be recorded on the media and in such other place(s) as deemed appropriate by the Information Technologies Director. The date of expiration, as suggested by the manufacturers' recommendations, will also be recorded on the media and in such other place(s) as deemed appropriate by the Information Technologies Director. The media must be retired from service on or before the recorded expiration date.

9. Applicability of Other Policies

This policy is part of ODCHC's comprehensive set of security and records retention policies. Other policies may apply to the topics covered here, particularly OPS.018, and such applicable policies should be reviewed as needed. Unless otherwise determined by the ODCHC Executive Team, the most conservative and/or restrictive policy will apply when policies are deemed to be in conflict.

10. Enforcement

This policy will be enforced by the ODCHC Information Technologies Director in concert with the ODCHC Facilities Manager, Chief Operating Officer and Executive Team as appropriate. Violations may result in disciplinary action, which can include suspension, restriction of access or more severe penalties up to and including termination of employment. When illegal activities or theft of ODCHC physical or intellectual property are suspected, ODCHC may report such activities to the applicable authorities.

Approved:

Cheyenne Spetzler

Cheyenne Spetzler
Chief Operations Officer