1. PURPOSE

The purpose of this procedure is to define the process for backup and restoration of electronic data managed by CareTech, Inc. ("CTI").

2. SCOPE

This procedure applies to all data stored electronically on servers managed by CTI's Information Technology department ("CTI IT"). Servers managed by CTI IT may reside internally or externally.

Electronic data that are stored in company-issued personal computers, notebooks, laptops, mobile devices or any other storage device are not within the scope of this procedure.

3. RESPONSIBILITIES

3.1. Manager of IT Operations

The Manager – IT Operations is responsible for ensuring that Backup Tests are scheduled and performed at least quarterly. In the event that these tests uncover backup and/or recovery problems, the Manager of IT Operations is responsible for escalating the problem to the Senior Manager, IT Operations, ensuring that a root cause analysis is performed and confirming that the problem(s) are corrected.

3.2. System Administrators

System Administrators are responsible for maintaining the backup application and procedures for the application, rotating the backup tapes according to the schedule, and verifying the status of the previous night's backup jobs.

4. DEFINITIONS

4.1. Backup

Backups are Files, equipment, data and procedures ("Data") available for use in the event of a failure or loss, if the originals are destroyed or out of service.

4.2. Full Backup

A Full Backup includes all the Data that are specified in the backup selections list for the policy, regardless of when they were last modified or backed up.

4.3. Cumulative Backup

A Cumulative Backup all the Data that have been modified since that last Full Backup.

4.4. Restore

The process of reinstating data that have been lost.

5. PROCEDURE

5.1. Data to Be Backed Up

All Data that are considered essential to business operations or CTI's reputation with customers or partners is considered "Critical Data" and must be protected from loss (accidental or intended). These include:

- Data that, if list, would prevent CTI from conducting normal business operations now or in the future.

- Data that has been entrusted to CTI, either by customers or partners.
- Data that, if lost, could subject CTI to legal or contractual penalties.
- Data that, if lost, could adversely affect CTI's reputation.

5.2. General Procedure

Backups of Critical Data shall be conducted regularly according to an established Backup Schedule. A record of all backup activities shall be maintained in a Backup Log as defined in Section 7 Appendix – Backup Log.

Backup Logs must be reviewed daily by the Manager of IT Operations

5.3. Backup Schedule

5.3.1. CUMULATIVE backups are performed every night, Monday through Thursday.

5.3.2. FULL backups are performed every Friday night.

5.3.3. MONTH-END backups are performed on the first Friday evening of every month.

5.3.4. YEAR-END backups are performed on the first Friday of the new fiscal year.

5.4. System Backup Policy

In addition to business data, CTI IT will perform regular backups and restoration tests of all IT environments managed by CTI IT. Data to be backed up includes:

- System state data of all Microsoft and Linux servers to save all system-specific settings and information.
- All local drives on the Microsoft and Linux servers.
- All Database Servers.

5.5. Backup Media Storage

Backup Media must be stored in a location separate from the server room. The location must be secure from intrusion and include fire and water damage prevention mechanisms.

5.6. Backup Media Retention

5.6.1. Daily CUMULATIVE backup tapes are reused after one (1) full week has passed since the original backup.

5.6.2. Weekend FULL backup tapes are reused after one (1) full month has passed since the original backup.

5.6.3. Month End FULL backup tapes are reused after one (1) full year has passed since the original backup.

5.6.4. Year End FULL backup tapes are not reused.

5.7. Media Inventory

An inventory of all Backup Media must be performed semi-annually (every six months). The inventory must be completed no later than 4 weeks after the due date.

The results of third-party audits may be used in place of an internal inventory.

The results of these inventories must be reviewed and approved by the Manager of IT Operations.

5.8. Restore Testing Procedure

Backup tests are to be performed quarterly for each backup system. A restoration test must consist of a minimum of either 25 files or 100 Megs of data. Restoration test documentation is to be kept by IT and available for review.

5.9. Restore Procedures

Restores are performed on a per request basis. Documentation of the request and confirmation of the restore is maintained within IT.

6. APPROVALS

Functional Area	Printed Name	Signature	Date
CIO	Cathy Cooper	Signature on file	12 NOV 2012

7. APPENDICIES – BACKUP LOG

- **Instructions**
  - Date – Enter the date for running the backup. Format MM/DD/YYYY
  - Start Time – Enter the time when the backup started
  - End Time – Enter the time when the backup ended
  - System – Enter the name of the System being backed up
  - Schedule – Enter one of the following:
    - C – Cumulative Backup
    - F – Full Backup
    - M – Month-end Backup
    - Y – End-of-Year Backup
  - Backup ID – Record the Backup ID in the following format:
    - DDMMYYRRNNTT Where
      - DDMMYY – day, month and year for the backup
      - RR – run number (this number can only be greater than 01 if the backup had to be repeated)
      - NN – media number
      - TT – total number of media required to complete the backup

    Example: Backup ID = 100512010203. This Backup ID corresponds to a backup performed on May 10, 1012. It was run only once and this is the second medium of a total of three
  - Media – Enter one of the following:
    - T – Tape
    - D - Disk
  - Test Date – Enter the date when the Restoration test was completed if applicable
  - Comments – Enter any comments regarding the backup run.
  - Performed By – Enter the initials of the System Administrator(s) that ran the backup/restore
  - Reviewed By – Enter the initials of the Manager of IT Operations that reviewed the Backup Log

CareTech, Inc.
Backup Log

Date	Time		System	Schedule	Backup ID	Media	Test Date	Comments	Performed by	Reviewed by
	Start	End								