Information Technology Services
Disaster Recovery Plan
Policy 5056

A Provider of Mental Health, Addiction and Developmental Disability Services

FY 2017

Bryan Stephens, Interim Executive Director: ________________________________

Date: 10/17/16

Jamie Allison, Chief Quality Office: ________________________________

Date: ________________________________

Reviewed August 30, 2016
Introduction
This document is the Disaster Recovery Plan for the Cobb County Community Services Board and the Douglas County Community Services Board, hereafter referred to as the CSB, Information Technology (IT) Department. The information present in this plan guides CSB management and technical staff in the recovery of computing and network facilities operated or maintained by the Information Technology department in the event that a disaster destroys all or part of the facilities.

Description
The Recovery plan is composed of a number of sections that document resources and procedures to be used in the event that a disaster occurs at the Information Technology department, which is located in the Administrative Office at 3830 South Cobb Drive, Suite 300, Smyrna, GA. or any of the CSB facilities. Each supported computing platform has a section containing specific recovery procedures. There are also sections that document the personnel that will be needed to perform the recovery tasks and an organizational structure for the recovery process.

This plan will be updated on a regular basis as changes to the computing and networking systems are made.

The Disaster Recovery Plan
Section 1: General Information about the Plan
Section 2: Disaster Planning
Section 3: Backup Procedures
Section 4: Vendor Contact Information
Section 5: Disaster Recovery List
Section 6: Maintaining the Plan

Reviewed August 30, 2016
Section 1
General Information About The Plan

Primary FOCUS of the Plan
The primary focus of this document is to provide a plan to respond to a disaster that destroys or severely cripples the CSB's central computer systems operated by the IT department. The intent is to restore operations as quickly as possible with the latest and most up-to-date data available.

Primary OBJECTIVES of the Plan
This disaster recovery plan has the following primary objectives:
1. Present an orderly course of action for restoring critical computing capability for the CSB within 14 days of initiation of the plan.
2. Set criteria for making the decision to recover at a cold site or repair the affected site.
3. Describe an organizational structure for carrying out the plan.
4. Provide information concerning personnel that will be required to carry out the plan and the computing expertise required.
5. Identify the equipment, floor plan, procedures, and other items necessary for the recovery.

OVERVIEW of the Plan
This plan outlines the approach to recovery from a disaster that destroys or severely cripples the computing resources in the Administrative Office at 3830 South Cobb Drive or other CSB facilities. Several departments have their own plan if the computer network is down.

Personnel
Immediately following the disaster, a planned sequence of events begins. Key personnel are notified and recovery teams are grouped to implement the plan. Personnel currently employed are listed in the plan. However, the plan has been designed to be usable even if some or all of the personnel are unavailable.

Salvage Operations at Disaster Site
Early efforts will be targeted at protecting and preserving the computer equipment. In particular, any magnetic storage media (hard drives, magnetic tapes, diskettes) will be identified and either protected from the elements or removed to a clean, dry environment away from the disaster site.

Designated Recovery Site
At the same time, a survey of the disaster scene is done by appropriate personnel to estimate the amount of time required to put the facility (in this case, the building and utilities) back into working order. A decision is then made whether to use the Cobb Outpatient Site (referred throughout this policy as the “Cold Site”), a location some distance away from the scene of the disaster where computing and networking capabilities can be temporarily restored until the primary site is ready. Work begins almost immediately at repairing or rebuilding the primary site. This may take months, the details of which are beyond the scope of this document.

Reviewed August 30, 2016
Policy #5056 – Disaster Recovery Plan

Purchase New Equipment
The recovery process relies heavily upon vendors to quickly provide replacements for the resources that cannot be salvaged. The CSB will rely upon emergency procurement procedures approved by the CSB’s purchasing office to quickly place orders for equipment, supplies, software, and any other needs.

Begin Reassembly at Recovery Site
Salvaged and new components are reassembled at the recovery site according to the instructions contained in this plan. Since all plans of this type are subject to the inherent changes that occur in the computer industry, it may become necessary for recovery personnel to deviate from the plan. If vendors cannot provide a certain piece of equipment in a timely manner, it may be necessary for the recovery personnel to make last-minute substitutions.

After the equipment reassembly phase is complete, the work concentrates on the data recovery procedures.

Restore Data from Backups
Data recovery relies entirely upon the use of backups stored in locations off-site from the Administrative Office. Backups can take the form of CD ROMs, disk drives, and other storage media. Early data recovery efforts focus on restoring the operating system(s) for each computer system. Next, first line recovery of application and user data from the backup disk is done. Individual application owners may need to be involved at this point, so teams are assigned for each major application area to ensure that data is restored properly.

Restore Applications Data
It is at this point that the disaster recovery plans for users and departments (e.g., the application owners) must merge with the completion of the Information Technology Department plan. Since some time may have elapsed between the time that the off-site backups were made and the time of the disaster, application owners must have means for restoring each running application database to the point of the disaster. They must also take all new data collected since that point and input it into the application databases. Designated staff from each department will need to be involved in testing the restored data to ensure accuracy prior to going live.

NOTE: The main EMR System, CareLogic, is hosted and maintained by QualiFacts Inc., in Nashville, Tennessee.

Move Back to Restored Permanent Facility
If the recovery process has taken place at the Cold Site, physical restoration of the Administrative Office (or an alternate facility) will have begun. When that facility is ready for occupancy, the systems assembled at the Cold Site are to be moved back to their permanent home.
Section 2  
Disaster Planning

As important as having a disaster recovery plan, taking measures to prevent a disaster or to mitigate its effects beforehand is even more important. This portion of the plan reviews the various threats that can lead to a disaster and steps we should take to minimize our risk. The threats covered here are both natural and man-made.

- Fire
- Flood
- Tornadoes and High Winds
- Earthquake
- Computer Crime
- Sabotage

FIRE
Preventive Measures
Fire Alarms
The Administrative Office is equipped with ceiling-mounted smoke detectors throughout the building.

Fire Extinguishers
Hand-held fire extinguishers are mounted in visible locations throughout the building. Staff is trained in the use of fire extinguishers.

Training and Documentation
Instructions for dealing with fire are present in the Agency’s Emergency Plan and H.E.L.P. Book. Staff is required to undergo training on hire and annually on the proper actions to take in the event of a fire. Staff is required to demonstrate proficiency in periodic, unscheduled fire drills and received annual training on the use of Fire Extinguishers.

NOTE: Fire Alarms and Fire Extinguishers are inspected as outlined by agency policy.

FLOOD
Preventive Measures
Elevated server racks/shelves
Servers are kept on server racks/shelves that are elevated off the ground.

Tarps
Tarps are available to cover the servers to protect from water.

Wet-Dry Vacuums
Wet-Dry vacuums are available to remove standing water.

TORNADOS AND HIGH WINDS
Preventive Measures
Tarps
Tarps are available to cover the servers to protect from debris.
Policy #5056 – Disaster Recovery Plan

**EARTHQUAKE**

**Preventive Measures**

Tarps
   Tarps are available to cover the servers to protect from debris.

**COMPUTER CRIME**

**Preventive Measures**

Firewalls
   The agency firewall protects computers from unauthorized access and harmful downloads.

Strong Passwords
   The agency uses strong passwords to protect computers from unauthorized access.

Software Updates
   The agency applies software updates to keep software versions up to date.

Anti-virus
   The agency uses anti-virus software to protect computers from viruses/spyware.

Backups
   The agency keeps data backups that can be restored in case data is compromised.

**SABOTAGE**

**Preventive Measures**

Physical Security
   The door to the Server room is always locked and only authorized staff have keys.
Section 3
Backup Procedures

Every system the Information Technology Department operates is backed up regularly. The agency computer systems are backed up using full and differential methods. Full backups are completed once a month and are stored in a fireproof cabinet. Differential backups are stored on removable media which is rotated each day.

Section 4
Vendor Contact Information

1. Geneva software company, Inc. (Financial Server Software)
   Thomas W. Vincent (President)
   Geneva Software Company, Inc.
   45 Dolley Madison Road, Suite 402
   Greensboro, NC 27410
   336-275-8887

2. Dell (servers)
   Dell, Inc.
   7133 Koll Center Parkway
   Pleasanton, CA 94566
   510-426-6400 (voice)
   510-426-6486 (fax)
   1-800-223-OPEN (Customer Support)
   http://www.dell.com

3. HP (Financial Server Hardware)
   1-800-727-2472 (Tech Support)
   http://www.hp.com

4. VMware Server (Cadis Server)
   Xtend Consulting
   1100 North Cobb Parkway, Suite D
   Marietta, GA 30062
   Phone: 770-771-5067
   Fax: 770-771-5070
   http://www.extendconsult.com

5. WindStream (Internet and Phones)
   1-877-340-2555 (Tech Support)
   http://www.windstream.com

6. IBM (Cadis Server Hardware)
   1-800-426-7378 (Tech Support)
Section 5
Disaster Notification List

The disaster notification list for Information Technology Department is shown below. These people are to be notified as soon as possible when disaster threatens or occurs.

### Safety Personnel

<table>
<thead>
<tr>
<th>Services</th>
<th>On CSB Phones Dial</th>
<th>Outside Phones Dial</th>
</tr>
</thead>
<tbody>
<tr>
<td>Emergency Fire, Ambulance, Rescue, Police, and HAZMAT</td>
<td>9-911</td>
<td>911</td>
</tr>
<tr>
<td>Director of Operations</td>
<td>5019</td>
<td>770-429-5019</td>
</tr>
<tr>
<td>Executive Director</td>
<td>5002</td>
<td>770-429-5002</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Title</th>
<th>Office Phone</th>
<th>Cellular</th>
</tr>
</thead>
<tbody>
<tr>
<td>I.T. – Systems Administrator</td>
<td>770-429-5014</td>
<td>770-509-5818</td>
</tr>
<tr>
<td>I.T. – Business Analyst</td>
<td>770-429-5015</td>
<td>(678) 487-9904</td>
</tr>
</tbody>
</table>
Section 6
Maintaining the Plan

Having a disaster recovery plan is critical. But the plan will rapidly become obsolete if a workable procedure for maintaining the plan is not also developed and implemented. This document provides information and maintenance procedures necessary to keep it up to date.

Basic Maintenance
The plan will be routinely evaluated once each year. All portions of the plan will be reviewed by the Information Technology Department. In addition the plan will be tested on a regular basis and any faults will be corrected. The Information Technology Department has the responsibility of overseeing the individual documents and files and ensuring that they meet standards and consistent with the rest of the plan.

Change-Driven Maintenance
It is inevitable in the changing environment of the computer industry that this disaster recovery plan will become outdated and unusable unless kept up to date. Changes that will likely affect the plan fall into several categories:

1. Hardware changes
2. Software changes
3. Facility changes
4. Procedural changes
5. Personnel changes

As changes occur in any of the areas mentioned above, the Information Technology Department management will determine if changes to the plan are necessary. This decision will require that the managers be familiar with the plan in some detail. A document referencing common changes that will require plan maintenance will be made available and updated when required.

Changes that affect the platform recovery portions of the plan will be made by the staff in the affected area. After the changes have been made, IT Services will be advised that the updated documents are available. They will incorporate the changes into the body of the plan and distribute as required.

Changes Requiring Plan Maintenance
The following lists some of the types of changes that may require revisions to the disaster recovery plan. Any change that can potentially affect whether the plan can be used to successfully restore the operations of the department's computer and network systems should be reflected in the plan.

1. Hardware
   a. Additions, deletions, or upgrades to hardware platforms.
2. Software
   a. Additions, deletions, or upgrades to system software.
   b. Changes to system configuration.
   c. Changes to applications software affected by the plan.
Policy #5056 – Disaster Recovery Plan

3. Facilities
   a. Changes that affect the availability/usability of the Cold Site location.
   b. Changes that affect Cold Site choice such as enlargement, cooling, or electrical requirements etc.

4. Personnel
   a. Changes to personnel identified by name in the plan.
   b. Changes to organizational structure of the department.

5. Procedural
   a. Changes to off-site backup procedures, locations, etc.
   b. Changes to application backups.
   c. Changes to vendor lists maintained for acquisition and support purposes.