

---

<b>Document Type:</b> <sup>1</sup>	<input type="checkbox"/> Policy & Procedure	<input type="checkbox"/> Process Guideline	Adopted: 04/22/04
	<input checked="" type="checkbox"/> Plan	<input type="checkbox"/> System Description	Last Reviewed: 11/06/08
			Retired: _____

Revisions: 12/09/04; 10/19/06; 11/06/08

---

## I. DEFINITIONS:

- A. Disaster: The occurrence of any event that causes a significant disruption in IS capabilities.
- B. Hot site: An off-site commercial disaster recovery service that would allow GCBH information systems to continue in the event of a disaster. Includes all or most equipment needed including phones, furniture, and computers.
- C. Cold site: An off-site commercial disaster recovery service that would allow GCBH information systems to resume, but only provides office space and does not provide additional equipment.

## II. EXECUTIVE SUMMARY:

Greater Columbia Behavioral Health (GCBH) has adopted this Business Continuity and Disaster Recovery Plan (BCDR Plan) to comply with the Federal law requiring contingency plans to respond to emergencies; with the Health Insurance Portability and Accountability Act of 1996 (HIPAA); with the Balanced Budget Act of 1997 (BBA), with External Quality Review Organization (EQRO) requirements; and because it is our duty to protect the confidentiality and integrity of client information as required by other laws, professional ethics, and accreditation requirements. All GCBH Information Systems (IS) personnel must be familiar with the contents of this plan and follow its guidance, as appropriate, in a declared disaster. In addition, familiarity with the plan is an important part of every employee's responsibilities.

Organizations are becoming more dependent on the service and record-keeping of the data processing department. The overall objectives of the Business Continuity and Disaster Recovery Plan is to protect GCBH resources, to safeguard the organization's vital records of which the data center has become pivotal and to guarantee the continued availability of essential IS services.

This Plan is designed to minimize the effect a disaster will have upon on-going operations. Occurrences of a less severe nature are controlled at the appropriate management level as a part of the total Plan.

For the recovery process to be effective, the Plan is organized around the team concept. The Plan contains the phone numbers of the team members in non-

published Attachment A1 and represents a dynamic process that is kept up-to-date. As recommendations are completed or as new areas of concern are recognized, the Plan will be updated reflecting the current status.

### **III. PURPOSE AND SCOPE:**

This document represents the Business Continuity and Disaster Recovery Plan for the services provided by Information Technology Services at GCBH.

- A. Purpose: To establish and define the procedures that will insure the continued operation and/or orderly recovery of services provided by the IS Department in the event of loss due to disaster or destruction, within reasonable time and costs. This plan will not address routine maintenance issues such as temporary downing of equipment for repairs.
  
- B. Scope: This plan considers restoration of services within a limited scope of a disaster. The plan primarily addresses the full or partial loss of mission-critical components due to a loss of or inaccessibility to the primary site and loss of key staff. In the event of a major catastrophe, such as loss of major portions of the surrounding geographic area, this plan does not adequately address steps to deal with major displacement of personnel, equipment and vital agency services to restore services. However, it would be possible to follow the same framework in dealing with the disaster.

### **IV. ASSUMPTIONS:**

- A. The viability of the core agency applications and network are critical to the operation of the agency as defined in the attachments.
  
- B. Virtually all users frequently use hardware and software in performance of their job duties or as a part of the business and clinical processes.
  
- C. It is imperative that IS resources be protected and that a plan be implemented that minimizes inconvenience and provides accessibility to these services.
  
- D. No matter how many precautions are implemented and to what extent they are enforced, most people in the data processing field agree that there are no completely secure computers. The operations of a data center could be suddenly disrupted by events that there is little or no control over, involving people, mechanics, electronics, or natural disasters. It is important to realize what the exposure to the Agency and the loss of the data center would be, and that steps are taken to minimize the costs resulting from loss or damage to its resources and capabilities.

- E. The server room is the heart of our data center. Any threat in or near the server room can affect the critical flow of information from this nerve center. The location of the disaster could be more important than the amount of damage it causes. A small problem at a critical location could cripple the data center and require it to reestablish operations at a backup facility.

For general purposes of the Plan, hot and cold sites will not be used unless necessary. Also, where a disaster is critical or catastrophic, the Chief Information Officer may outsource as many disaster recovery functions as necessary. The GCBH Director will be apprised of such decisions in a timely fashion.

## **V. GOALS:**

- A. The goal is to restore service to critical components as quickly as possible, and the time frame is dependent upon the disaster or emergency situation.
- B. Users would need to plan to operate on their own during that outage and have a means of catching up with the information once the access is restored.
- C. Most other services to non-critical components should be restored as quickly as possible.

The "plan" as referenced in this document only represents the responsibilities assumed by Information Systems (IS) Department and does not constitute an entire emergency response plan for GCBH.

- D. A goal of this plan is to address mission critical computer infrastructure to the primary business location of GCBH in case of an emergency.

## **VI. REVIEW AND APPROVAL OF THE PLAN:**

The plan will be reviewed and/or revised annually. The plan will be considered in effect once approved by the GCBH Board of Directors (upon the recommendation of the IS Committee). The IS Department will be responsible for the review and testing of the plan as well as coordination with appropriate management as needed. Reviews of these tests will be provided to the GCBH IS Committee on an annual basis (or more frequently as appropriate).

GCBH central office staff will receive an annual review of the plan as part of their ongoing staff development. All new employees will receive a review of this plan (completed by the Chief Information Officer or designee) during their new hire orientation.

## **VII. IMPLEMENTATION OF THE PLAN & AUTHORITY:**

The decision to implement disaster recovery procedures is the responsibility of the Chief Information Officer, who at the time of activation of this Plan, becomes the Business Continuity and Disaster Recovery Coordinator, in coordination with the GCBH Director. In the case of a disaster, all or part of the disaster recovery team will assemble to assess the situation. In the case of a partial outage, the team coordinator (defined in [Section XI](#)) will work directly with the person responsible for the affected component or service and take the necessary steps to restore service according to the priorities as outlined in the plan. In the event of a major disaster such as extensive loss of hardware components or inaccessibility to facilities, the team may require access to other resources on a priority basis. Users will be notified of the disaster and given updates on the status of restoring services. All communications will flow through the IS Department or as assigned. *GCBH has a telephone directory/call tree and all employees have employee wallet cards with phone numbers.*

## **VIII. PLAN ATTACHMENTS:**

The following items are not distributed, but filed with the plan and a copy kept off-site in a safety deposit box at the Bank of America at 3420 West Kennewick Avenue, Kennewick, Washington.

- A. Information Service department organization chart
- B. Inventory listing of all hardware, software, network, telecommunications, and other fixed assets
- C. Vendor Maintenance Agreements and emergency contacts
- D. GCBH Network Diagram of Information Systems
- E. Process Manual for IS Department common tasks.

## **IX. THE PRIMARY NETWORK DISTRIBUTION CENTER RECOVERY PROCEDURE:**

The main premise of the plan is to address the operation of the critical computer infrastructure at GCBH, as defined in the non-published attachments A2 and A3. Critical components are located at the primary business location. Tape backups in the non-published attachment A4 and the plan attachments will be kept off-site.

The plan describes the composition of the Business Continuity and Disaster Recovery team and procedures to follow in the event of a disruption in service to a mission critical component. Since timely action is critical, backup personnel are identified if the designated team leaders cannot be reached. Depending on the

extent of the disaster, the team, as well as contracted IS personnel, may be involved in resolving the problem.

#### A. Basic Recovery Plan Requirements

1. Business Continuity and Disaster Recovery Team
2. Disaster recovery documentation
3. Backup computer facilities (hot site), if deemed necessary.

#### B. Off-site Storage of System Backup Tapes

In the event a disaster occurs in the current server room, having backup tapes stored off-site is critical. All incremental backups are stored in a fireproof container, with full backups stored in the bank's safety deposit box. The Chief Information Officer and PC & Network Technician are responsible for the proper rotation and maintaining and distributing all backup tapes. The Database Specialist will perform the full backup, when the Chief Information Officer and PC & Network Technician are unavailable. The Office Manager and/or PC & Network Technician will distribute the weekly full backup to the bank safety deposit box.

A log will be maintained of all backups and restores, including time and tape number. This log will be audited quarterly by the GCBH Auditor. Results of these audits will be reported to the Chief Information Officer and Director.

#### C. Backup Facility (hot site)

In the case of fire or natural disaster it may become necessary to move the server room to a backup location. The GCBH Director would have to approve the procurement of a hot site in the case of a catastrophic emergency, with subsequent approval by the GCBH Board of Directors.

#### D. Disaster Preparation

Being ready and planning ahead is the easiest way to be sure we can quickly and fully recover from a disaster. The Business Continuity and Disaster Recovery Plan testing and update are addressed in [Section XVI](#).

#### E. Emergency Response

These are the first actions taken in an emergency situation, designed to bring the computer systems back to operation, even if not at full capacity or in a degraded state.

#### F. Disaster Preparation

This section outlines the minimum steps needed to insure full recovery from a disaster.

1. The disaster plan must be kept current and all of the team members on the recovery team must be made aware of any changes.

2. The off-site storage area should be inspected periodically to insure that the correct backup tapes are in storage.
3. All fire fighting equipment in the computer rooms should be inspected annually and serviced as needed. Additionally, all staff is trained on the location and use of fire extinguishers.
4. The maintenance staff should have a phone number to contact the GCBH Director or designee in case of an emergency occurring during off-hours.
5. Procedures and lead times for replacement equipment and communications will be established.
6. In the event that there is warning of an impending disaster, i.e., potential flood situation, earthquake activity in the immediate area, fire or potential building damage, the following steps should be taken:
  - a. Notice should be given to as many BCDR Team members as possible.
  - b. The GCBH Director or designee should be briefed and a decision should be made whether to shut down the systems. The recovery team should convene and review whatever actions may be necessary.

#### G. Emergency Response

This section details the basic actions that need to be taken in the event of a disaster situation.

1. The IS Department and the BCDR Team should be notified and assembled as soon as reasonable under the circumstances.
2. Team members should assess damages.
3. Team members should advise the GCBH Director as to the extent of damage and recovery procedures necessary.
4. Pertinent vendors should be contacted and negotiations should be made for the delivery of equipment, and delivery time should be noted.
5. All affected department heads should be notified of any decisions and given an estimated time to the return to either full or degraded service.
6. Each member of the BCDR Team should supervise his or her own area of expertise.
7. All computer facilities should be secured.

#### H. Recovery Procedures

Recovery from a complete failure to a degraded mode of service may be necessary. In this case it may be possible to bring up individual departments on a priority basis.

The decision to operate in a degraded mode and the order in which departments are to be brought back into service should be made by the Chief Information Officer and the GCBH Director in consultation with team members.

If it is decided to transfer a server room to a hot site:

1. It is assumed that the basic emergency procedures have been followed as detailed above.
2. An inventory of the status of existing equipment and files should be accessed.
3. The move should be coordinated by the Chief Information Officer and recovery team members.
4. Vendors should be contacted to initiate delivery of replacement equipment to the hot site. At this time, an estimated time of delivery should be noted.
5. If needed, a new off-site backup storage facility should be located and used immediately.
6. All facility systems should be verified operational at this time.
7. Systems should be tested and loaded as soon as vendors give the release to test.
8. Communications, networking, operations, and applications software staff should be prepared to install and/or setup their individual function in the appropriate order.
9. GCBH management and personnel should be made aware of progress and/or setbacks on a regular basis.

Existing safety, emergency procedures, and security at the hot site should be examined for their adequacy as a computer room by the GCBH Risk Manager with consultation from the IS Department.

#### I. Recovery Timetable

The following timetable does not take into account the amount of time required to input data held on hardcopy during the recovery period, or re-inputting data which may have been lost during recovery, and depending on the situation, may be more or less time than indicated. In addition the attachments to the non-published version of the plan will be used to expedite this process.

##### 1. DAY 1

Convene the Disaster Recovery Team and assess damages, contact vendors, contracted personnel, and if needed, review and utilize hot site options.

##### 2. DAY 2-5

Restore programs and data, test integrity of programs and data. Begin restoring communications and networking capabilities.

##### 3. Day 6

Restore partial operation to priority departments.

##### 4. Day 7-9

Determine priority of data processing.

## 5. Day 9-15

Take delivery and setup new equipment. Restore full communications and networking capabilities. Work with departments to verify data and operation of applications.

## **X. PHYSICAL FACILITIES:**

Address: 101 N. Edison St., Kennewick, Washington, the existing information technology center, will be the primary location for housing the critical infrastructure equipment. This site contains the most up-to-date equipment:

- A. Fire protection
- B. A commercial uninterruptible power system
- C. Close access to a main telecommunications hub
- D. Limited secured access
- E. On-site staff

Storage Site: The safety deposit box site where full data backups are housed is at Bank of America, 3420 West Kennewick Avenue, Kennewick, Washington with limited access to authorized persons, and is equipped with a fireproof vault to house the data backup tapes and the non-published version of the Plan's attachments.

## **XI. CRITICAL COMPONENTS:**

These components provide critical services to GCBH that need to be restored as soon as possible from the point of the declared disaster. The resources that make up these components have been distributed to separate locations outside the main computer room to reduce the possibility of complete failure. As a part of the actual Plan, a diagram a complete inventory of the equipment, the insurance information and the maintenance list is attached to the Plan in non-published attachments A2, A5, A6, and A7. Each critical component and its location is listed on the network configuration chart which is kept with the BCDR Plan off-site. The critical components are identified below:

- A. GCBHS1 MAIN SERVER/DATA CENTER
- B. GCBHS2 Web Server
- C. GCBHS3 Exchange Server (e-mail)
- D. SQL Server
- E. Network Switch
- F. CISCO Router/Firewall
- G. LAN (Local Area Network)
- H. Cisco VOIP Phone Unity & Call Manager Servers

## **XII. BUSINESS CONTINUITY AND DISASTER RECOVERY TEAM:**

- A. Team Headquarters: If the primary site is usable, the team will assemble in an available conference room. In the event the building or room is unavailable, the team will meet at an alternate site assigned by the Chief Information Officer.
- B. Duties and Responsibilities: The Business Continuity and Disaster Recovery Team members and responsibilities follow the organization structure of Information Systems. The Business Continuity and Disaster Recovery Team has been established and organized to determine the magnitude of destruction and assess the damage to the computer facility, to control and coordinate recovery/backup actions, and to make recommendations to the GCBH Director. The team consists of a cross section of staff responsible for one or more of the following functions:
1. Recovery administration
  2. Insurance notification
  3. Supplies
  4. Organization
  5. Systems software
  6. Applications software
  7. Hardware
  8. Communications
- C. Disaster Recovery Coordinator - The Chief Information Officer will serve in this capacity. The responsibilities are:
1. Determine the extent and seriousness of the disaster.
  2. Invoke the Business Continuity and Disaster Recovery Plan (in conjunction with the GCBH Director when feasible).
  3. Coordinate the disaster recovery activities.
  4. Inform GCBH senior management of recovery activities and information.
  5. Determine the extent of equipment disability.
  6. Ascertain disability of software and training program materials.
  7. Coordinate acquisition of replacement materials and products.
  8. Notify End User Support personnel of required activities, locations and schedules.
  9. Oversee and coordinate all interim activities.
  10. Define criteria for establishing a temporary backup facility.

11. Schedule and direct the return to normal operations.
12. Oversee and coordinate all interim systems and programming functions and systems recovery.
13. Schedule and direct return to normal operations.
14. Review production cycles and prioritize applications with users.
15. Identify required involvement of application and user personnel.
16. Coordinate required activities for applications staff and users as necessary.
17. Assist with negotiations with vendors and managers of alternate site facilities.
18. Notify operations personnel of required activities, locations and schedules.
19. Oversee and coordinate all interim operations functions and equipment recovery.
20. Secure backup material from off-site storage and coordinate delivery to appropriate sites.
21. Schedule and direct return to normal processing operations.

D. Systems Programming and Operations Recovery Team Coordinator - The PC & Network Technician will serve in this capacity. The responsibilities are:

1. Assume the responsibilities of the Business Continuity and Disaster Recovery Coordinator in the event he/she is disabled or not available.
2. Inform the Business Continuity and Disaster Recovery Coordinator of recovery activities and information.
3. Negotiate with vendors and managers of backup facilities.
4. Coordinate scheduling for programming and computer time.
5. Coordinate activities of the systems recovery and operations under the supervision of the Business Continuity and Disaster Recovery Coordinator.
6. Record all disaster recovery activities.
7. Provide support for Business Continuity and Disaster Recovery Coordinator and assist in a disaster recovery functions as needed.

E. Data Systems Team Coordinator - The Database Maintenance Specialist will serve in this capacity. The responsibilities are:

1. Assume the responsibilities of the Systems Programming and Operations Recovery Team Coordinator in the event he/she is disabled or not available.

2. Assess the state and condition of the GCBH data systems and ability to collect data from GCBH providers, and the ability of GCBH to transmit data to the MHD.
3. Inform the Business Continuity and Disaster Recovery Coordinator of recovery activities and information.
4. Work to resume data systems functionality and integrity as soon as possible.

F. Other individuals as determined necessary by the Business Continuity and Disaster Recovery Coordinator and/or GCBH Director.

### **XIII. EQUIPMENT MAINTENANCE AND REPLACEMENT**

- A. GCBH maintains an IS equipment inventory list, which along with the GCBH insurance policy, vendor and key contacts, and the Business Continuity and Disaster Recovery Plan are kept in the safety deposit box at the Bank of America. All Management staff, including Fiscal, are part of the BCDR Team.
- B. In the event of breakage, damage or loss of equipment, various approaches are taken to restore the service provided by the component. Decisions about the approach are dependent upon the critical nature of the equipment, cost and number of units in service. In some cases, the equipment is protected against loss with full replacement protection under a service or insurance policy. In other cases, spare components may be kept on hand and swapped in the event of a failure. Most critical components are placed under vendor maintenance service agreements for normal service requirements. Refer to appendix for list of major components and the method used to maintain and/or replace them. Copies of all vendor agreements will need to be kept with the actual Plan at the primary and backup site location.
- C. The following describe the major services provided by external vendors:
  1. Vendor Maintenance - For protection against outages due to normal wear and tear, outside vendors are contracted to perform maintenance services. This is usually the manufacturer of the equipment, but not necessarily in all circumstances.
    - a. Normal contracted maintenance conditions include:
      - i. Call window - 8 a.m. - 5 p.m. (Monday through Friday)
      - ii. Parts - furnished.
      - iii. Labor - furnished.
      - iv. Response time - within four (4) hours of notification
      - v. Type of maintenance included:
        - o Preventive

- Continued remedial - (Customer approved/action plan after 4 hours)
  - Remote diagnostics
  - Installation of engineering modifications
2. Equipment Replacement - In some cases, services are used for full product repair and/or replacement for damage caused by accidents or incidents not covered under service agreements. These plans expand service to cover fire, water damage, natural disasters, power failure, sprinkler leakage, theft, etc. It provides reimbursement for the cost of transportation, removal of damaged equipment, installation of replacement equipment, replacement of fire protection chemicals, restoration of damaged system software, and restoration of customer data from backup disks/tapes.
  3. These services are only available on items under full maintenance coverage and chargeable at a percentage of the annual fee for that component or through special agreements as attachments to vendor contracts.
  4. For critical and non-critical items, the extra cost of replacement services and insurance would have to come from existing agency resources. Decisions of whether to cover items would also take into consideration the state of technology, the cost of replacement and evaluating the risk of loss versus the on-going annual premium cost. These decisions will be revisited each year during the review process.

#### **XIV. BACKUP PROCEDURES:**

- A. The main application server(s) are backed up to tape on a daily basis using the Backup Exec utility. This backup is called an incremental backup. It is done Monday through Friday nights, to copy all files that have been updated since the last full BACKUP was performed.
- B. On Wednesday night, a full BACKUP of the entire system is taken. Once weekly, a full backup tape is sent to the off-site, fireproof vault, where they are stored.
- C. In tape storage, there are designated tapes that are used in a round-robin fashion for the incremental backups. Backup tapes are maintained back to 2000 and kept at GCBH. The rotation schedule and log for the safety deposit box is as follows:
  - The full monthly tapes go back six (6) months; and
  - The full weekly tapes (1-10) are rotated as needed.

## **XV. IMPLEMENTATION OF THE PLAN:**

### **A. Circumstances to Declare a Disaster**

1. Any event that significantly disrupts critical services or is likely to significantly disrupt critical services or cause personal injury will require that a disaster be declared by the Chief Information Officer and the GCBH Director and the plan followed.
2. In the event there is a limited outage due to loss of a critical component that doesn't cause widespread loss of service or is temporary, an abbreviated plan of action will be followed. Management and the BCDR Team are responsible for determining when a limited disaster exists and will decide what measures to take to correct the problem. In some cases, this may be a service call to the vendor responsible for maintenance.
3. All events will be documented and discussed as part of the review process to determine whether changes to the plan are necessary to reduce the risk of future failures. This review should be done by the Chief Information Officer and the IS Committee in conjunction with the Risk Manager.

### **B. Major Event Significantly Disrupting Services**

1. Emergency Procedures When the Primary Site is Unoccupied - In the event it is necessary to provide notification of a disaster or emergency during a period when the building is unoccupied, it is expected that a senior management team member will be on call and will initiate the notification procedures outlined above until one team member is contacted. The team member notified by the senior management representative on call will complete the notification process.
2. Operations section team members will report to the primary site, completing the damage assessment evaluation prior to reporting to the team headquarters. The damage assessment team members will be admitted to the building after presenting their GCBH I.D. cards to the senior management representative on call at the site.
3. Emergency Procedures When Building Is Occupied - In the event it is necessary to provide notification of a disaster or emergency during a period when the building is occupied, it is expected that the Operations Coordinator (discussed in [section XII](#)), will initiate the notification procedures. This assumes that the primary site server room or the adjacent space is involved with the disaster. Otherwise, the Chief Information Officer or designee will initiate the notification procedures.
  - a. The following activities may be directed as the situation may require:

- i. An announcement to evacuate the building. The Public Address system and/or messengers will be sent for this purpose. A copy of the building evacuation chart is attached.
- ii. Designate individuals to secure the area by activating lockup.
- iii. Initiate shutdown procedures for equipment, electrical service, or air conditioning.
- iv. Direct damage limiting measures to be taken.
- v. Determine need for and secure emergency support services to insure personnel safety and building security.

C. Provisions for Backup of Key Personnel

1. Documentation of duties - Written instructions for IS common tasks and system setup is maintained by IS staff and a copy of these instructions are kept in the safety deposit box. These instructions are updated as needed.
2. Cross-training – When possible, IS staff are cross-trained on critical processes so that more than one person is able to perform that function.
3. Contract personnel – It may be determined necessary by the GCBH Director and/or Chief Information Officer that a temporary staff is needed to perform the duties of the key personnel as a stopgap until the key staff is either able to return to GCBH or be permanently replaced. If this implemented, the GCBH Director and/or Chief Information Officer will follow the guidelines as documented in the GCBH Purchasing Policy (FM8807).

D. Procedures to Utilize Alternate Site

In the event of a major disaster that destroys or leaves the primary site unusable for a prolonged period of time, the Chief Information Officer in coordination with the GCBH Director may authorize and designate a secondary site to be used to restore service. Although mission critical services will be restored as soon as possible, non-critical services may take longer depending upon need. An inventory of items deemed critical and non-critical is attached to the Plan.

E. Procedures to Restore Service for Critical Components

The infrastructure is designed to provide reasonable resumption of mission-critical services as soon as possible from the point of the declared disaster. The procedures for notification of the disaster and duties of the disaster recovery team are found in this document. This approach for the restoration of service to the critical components will be assigned by the Chief Information Officer.

## F. System Access

It will probably not be sufficient to allow everyone to conduct business without some discussion of altered IS response times and capacities. This may lead to limiting the number of users, but it will certainly be sufficient to conduct critical business and clinical operations. This may also be an issue related to network access. In the event that controlled access is necessary, a combination of restricting the number of users or by time blocks will be used. For example, administrative use may be restricted to morning hours and clinical use in afternoon hours. For administrative users, the operations section will work with the heads of the user areas to identify key personnel to grant immediate access. At that point, reference would be made to the user area disaster recovery plans.

## G. Processing Priorities

1. In the event that the disaster creates a critical shortage of resources that doesn't permit all users to access the systems simultaneously, restrictions on access will be initiated and the production schedules altered to process in mission critical order.
2. Establishing application priorities and schedule planning are limited to short term recovery, which is the period until regular operations are back to normal. It is expected that normal scheduling will be resumed as the alternate and secondary sites are available.
3. The priority requirements and schedule will be developed and approved as directed by the Business Continuity and Disaster Recovery Coordinator. This is done after consultation with the major user areas. Timing of the interruption during the production cycle may affect priority requirements and scheduling.

General priorities of systems and functions are considered to be: 1) payroll, 2) financial systems, 3) Consumer Information System, 4) electronic mail and web access, 5) the phone system; and 6) clinical record processes (including intake and progress notes).

## H. Meeting Space

Primary and alternate meeting sites for the Business Continuity and Disaster Recovery Team personnel have already been addressed under Business Continuity and Disaster Recovery Team Headquarters. In the event a disaster occurs, relocation of personnel may be necessary until suitable space can be secured. The senior management team is responsible for space scheduling. Information concerning available sites and locations, as well as assistance in

the acquisition of needed floor space will be provided by the senior management team member on call.

I. Operational Procedures

1. A copy of the vendor supplied operation manual is kept in the server room. Manuals for each auxiliary device are stored with the device.
2. Task scheduling will be prioritized according to the severity and extent of the disaster.
3. All documentation for core business and clinical systems on the main application servers are maintained on-line. This provides automatic backup under standardized procedures with off-site storage.

J. History Outline

The Business Continuity and Disaster Recovery Team is responsible for establishing and maintaining a record of all disaster recovery activities. This history will be a record of events for subsequent reviews and debriefings with governmental agencies, insurance companies, vendors, and suppliers, et al.

The history outline shall include:

1. Chronological log of disaster events
2. Chronological log of recovery steps
3. Analysis of cause of disaster
4. Man hours and estimated costs of recovery tasks
5. Statement of the impact of service interruptions
6. Evaluation of the effectiveness of activities
7. Recommendations to minimize impact of future disaster

This information will be reviewed with the IS Committee and recommendations transmitted to the GCBH Board of Directors by the Chief Information Officer and GCBH Director.

**XVI. DISTRIBUTION AND REVISIONS:**

The Business Continuity and Disaster Recovery Plan will be distributed to the following individuals:

- A. Members of the Business Continuity and Disaster Recovery Team and their designated backups
- B. GCBH Director
- C. Board of Directors
- D. GCBH Employees

One copy of the plan will also be stored in the Disaster Recovery Coordinator's Office as well as a copy being stored with the backup files and documentation at the off-site vault location with a third copy of the plan being maintained by the Office Manager.

The Business Continuity and Disaster Recovery Team will review the plan as needed. Normal updates such as names, telephone numbers, equipment changes, and office relocation will be made routinely and distributed to all holders of the plan. Other revisions to the plan that change procedures and other major aspects will be submitted through the GCBH IS Committee and then to the Board of Directors for review and approval. These changes will be distributed upon approval.

**XVII. TESTING OF THE PLAN:**

The backups are tested at least once annually. This means that a test restore is done using either a full backup or a full backup in combination with an incremental backup at least once per year. All backups and restores (test or "live") are documented in a log and audited by the GCBH Auditor quarterly.

Disaster recovery drills are done once per year by the BCDR Team. Practice disaster scenarios are thought up and the BCDR Team walks through potential resolutions to the disaster.

Approved:

Date:

/S/ William Wilson  
William Wilson, DrPH  
Director

11/06/08