**G-Cube Business Continuity Manual**

**NOTICE**

The information contained in this document is not to be used for any purpose other than the purposes for which this document is furnished by G-Cube, nor is this document (in whole or in part) to be reproduced or disclosed to other G-Cube employees without a need to know, or to any third party or made public without the prior express written permission of G-Cube.

**Version Control: 2.1**

**Author**-SEPG

**Version**-Baselined

**Date Created**- 13 Apr 2011

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Version No. | Version Date | Types of Changes | Owner/  Author | Reviewer | Date of review | Approver | Approval Date |
| 1.0 | 1 Oct | Created | SEPG | Milind | 10-Sep | Milind | 1-Oct |
| 2.0 | 14 Jan | Review | SEPG | Milind | 14-Jan | Milind | 20-Jan-11 |
| 2.1 | 7 Apr | Review | SEPG | Milind | 13-Apr | Mlind | 13-Apr-11 |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

**Table of Contents**

1. Background-----------------------------------------------------------3

2. Scope----------------------------------------------------------------- 3

3. Objective--------------------------------------------------------------3

4. Assumptions---------------------------------------------------------- 3

5. Disaster Definition----------------------------------------------------3

6. Project responsibilities------------------------------------------------4

7. Instructions for using BCP--------------------------------------------4

8. High availability practices for G-Cube--------------------------------5

9. Local High Availability Approach--------------------------------------5

10. Multi Location High Availability Approach---------------------------6

11. Alternate work location & Standby sites----------------------------6

12. Emergency Management Procedures--------------------------------6

13. BCP review and maintenance---------------------------------------10

14. Emergency response checklist--------------------------------------10

15. BCP Committee responsibility---------------------------------------11

Note:

This document contains information that is vital to the proper functioning of G-Cube processes. This document in the future would be read and referred to by BCP Committee, ERT & Project Teams for ensuring recovery options and redundancy plans for the organization or projects.

Background

The purpose of this business continuity plan is to prepare G-Cube in the event of extended service outages caused by factors beyond our control (e.g., natural disasters, man-made events), and to restore services to the widest extent possible in a minimum time frame. All G-Cube sites are expected to implement preventive measures whenever possible to minimize operational disruptions and to recover as rapidly as possible when an incident occurs.

The plan identifies vulnerabilities and recommends necessary measures to prevent extended service outages. It is a plan that encompasses all G-Cube system sites and operations facilities.

## Scope

This is a business continuity manual, and not a daily problem resolution procedures document.

## Objectives

* Serves as a guide for the emergency response teams.
* Provides procedures and resources needed to assist in recovery.
* Identifies vendors and customers that must be notified in the event of a disaster.
* Assists in avoiding confusion experienced during a crisis by documenting, testing and reviewing recovery procedures.
* Identifies alternate sources for supplies, resources and locations.
* Documents storage, safeguarding and retrieval procedures for vital records.

## Assumptions

* Key people (team leaders or alternates) will be available following a disaster.
* A national disaster such as nuclear war is beyond the scope of this plan.
* This document and all vital records are stored / made available in a secure off-site location so that it not only survives the disaster but also accessible immediately following the disaster.
* Each support organization will have its own plan consisting of unique recovery procedures, critical resource information and procedures.

## Disaster definition

Any loss of utility service (power, water), connectivity (system sites), or catastrophic event (weather, natural disaster, vandalism) that causes an interruption in the service provided by G-Cube operations. The plan identifies vulnerabilities and recommends measures to prevent extended service outages.

## Project responsibilities

* Each team member will designate an alternate back up.
* All of the members should keep an updated calling list of their work team members’ work, home, and cell phone numbers both at home and at work.
* All team members should keep this plan for reference at home in case the disaster happens after normal work hours. All team members should familiarize themselves with the contents of this plan.
* Team member’s engaged in business critical processes must have project specific redundancy process. [laptop/cell phone/remote connectivity]

## Instructions for using the business continuity plan

### Invoking the plan

This plan becomes effective when a disaster occurs. Normal problem management procedures will initiate the plan, and remain in effect until operations are resumed at the original location or a replacement location and control is returned to the appropriate functional management.

### Disaster declaration

BCP Committee & ERT is responsible for declaring a disaster and activating the various recovery teams as outlined in this plan.

In a major disaster situation affecting multiple business units, the decision to declare a disaster will be determined by G-Cube senior management. ERT will respond based on the directives specified by BCP Committee.

### Notification

Regardless of the disaster circumstances, or the identity of the person(s) first made aware of the disaster, the ERT must be activated immediately in the following cases:

* Two or more business critical systems are down concurrently for two or more hours
* Any problem at any system or network facility that would cause the above conditions to be present or there is certain indication that the condition is about to occur.

### 

### External communications

Corporate public relations personnel are designated as the principal contacts with the media (radio, television, and print), regulatory agency, government agencies, and other external organizations following a formal disaster declaration.

### High Availability Practices for G-Cube

High availability solutions can be categorized as **local high availability solution** that provide high availability at a single location, and multi location high availability solutions which are geographically distributed deployments and provide **protections from disasters** resulting in site/city outage.

**Local High Availability Approach**

Data backup policy

Full and incremental backups preserve corporate information assets and should be performed on a regular basis for audit logs and files that are irreplaceable, have a high replacement cost, or are considered critical. Backup media should be stored in a secure, geographically separate location from the original and isolated from environmental hazards.

Department-specific data and document retention policies specify what records must be retained and for how long. All organizations are accountable for carrying out the provisions of the instruction for records in their organization.

IT follows these standards for its data backup and archiving:

Tape retention policy

Backup media is stored at locations that are secure, if needed; isolated from environmental hazards, and geographically separate from the location housing the system.

Billing tapes

1. Tapes/Media greater than three years old are destroyed every six months.
2. Tapes/Media less than three years old must be stored locally off-site.
3. The IT dept. is responsible for the transition cycle of tapes/media.

System image tapes (specific project level requirements can take a precedence)

* A copy of the most current image files must be made at least once per week.
* This backup must be stored offsite.

1. The system supervisor is responsible for this activity.

Off-site storage procedures (if needed)

* Tapes and disks, and other suitable media are stored in environmentally secure facilities.
* Tape or disk rotation occurs on a regular schedule coordinated with the storage vendor.
* Access to backup databases and other data is tested annually.

**Disaster Recovery Approach / Multi Location High Availability Approach**

In this approach we set up two homogeneous sites; one active and one passive. Each site is a self contained system. The active site is called production site, and passive site is called standby site. During normal operation the production site serves the request, in the event of a disruption or site failover, the stand by site takes over the production role and all requests are routed to the standby server.

To maintain the standby site for failover, the standby site must contain homogenous installations and applications. Data and configurations must be synchronized constantly from the production site to the standby site. In addition a heart beat mechanism is setup between these two sites: “Production Site” and “Standby Site”. This mechanism can be established through cluster. Cluster agents can detect a failover situation, shut down the active instance completely and bring up the passive instance (standby site) and the application services can resume processing.

G-Cube is in the process of undergoing reciprocal arrangements with external organizations for a mutually beneficial agreement wherein both will deploy standby passive servers of business critical applications for each other. Operations can help take the advantage in a situation where in the engagement is highly prioritized. G-cube is also in the process of identifying suitable contingency sites. Its an ongoing process and the details will be communicated.

Projects needing redundancy process or continuity actions which require standby site/alternate work locations need to contact SEPG at sepg@gc-solutions.net.

### Emergency management procedures

The following procedures are to be followed by system operations personnel and other designated G-Cube personnel in the event of an emergency. Where uncertainty exists, the more reactive action should be followed to provide maximum protection and personnel safety.

These procedures are furnished to G-Cube management for reference. Several pages have been included to supply emergency contacts.

In the event of any situation where access to a building housing a system is denied, personnel should report to alternate locations. Working from home can be approved by the supervisor either over phone or mail. Primary and secondary locations are listed below.

**Alternate locations and standby sites**

G-Cube is in the process of undergoing reciprocal arrangements with different organizations for arranging standby sites and alternative workplaces as a part of business continuity strategy. The address and terms of service / contract will be made available to the functions from BCP committee through SEPG. Projects needing redundancy process or continuity actions which require standby site/alternate work locations need to contact SEPG at sepg@gc-solutions.net.

**In the event of a natural disaster**

In the event of a major catastrophe affecting G-Cube facility, immediately notify the **Debasis Pati BCP Committee Contact: 9811686063/ Barsha Chakraborty 9811687845**

|  |  |  |
| --- | --- | --- |
|  | **STEP** | **ACTION OWNER PM** |
|  | **1** | Notify ERT of pending event, if time permits. |
|  | **2** | If the impending natural disaster can be tracked, begin preparation of site within 48 hours as follows:   1. Deploy portable generators with fuel within 100 miles. 2. Deploy support personnel, tower crews, and engineering within 100 miles. 3. Deploy tractor trailers with replacement work space, antennas, power, computers and phones. 4. Facilities department on standby for replacement shelters 5. Basic necessities are acquired by support personnel when deployed:  * Cash for one week * Food and water for one week * Gasoline and other fuels * Supplies, including chainsaws, batteries, rope, flashlights, medical supplies, etc. |
|  | **3** | In case of impending possible disaster situation:   * Create an image of the system and files * Back up critical system elements * Verify backup generator fuel status and operation * Create backups of e-mail, file servers, etc. * Fuel vehicles and emergency trailers * Notify senior management |

**In the event of fire**

If fire or smoke is present in the facility, evaluate the situation, determine the severity, categorize the fire as major or minor and take the appropriate action as defined in this section. Call 0120-2402161, 4000200 as soon as possible if the situation warrants it.

* Personnel are to attempt to extinguish minor fires (e.g., single hardware component or paper fires) using hand-held fire extinguishers located throughout the facility. Any other fire or smoke situation will be handled by qualified building personnel until the local fire department arrives.
* In the event of a major fire, 0120-2402161, 4000200 and immediately evacuate the area.
* In the event of any emergency situation, system security, site security and personal safety are the major concerns. If possible, the operations supervisor should remain present at the facility until the fire department has arrived.
* In the event of a major catastrophe affecting the facility, immediately notify all members of BCP committee.

[It is BCP teams’ responsibility to facilitate the training of associates in fire fighting & conduct mock drills as per building evacuation plan.]

**BCP Committee Contacts:** Manish Gupta 9717698051, Barsha Chakraborty 9711985871, Ankur Kashyap 9717765849, Debasis Pati 9811686063, Anuradha Jain 9899777509

|  |  |  |  |
| --- | --- | --- | --- |
|  | **STEP** | **ACTION OWNER PM** | |
|  | **1** | Dial 0120-2402161 to contact the admin department. | |
|  | **2** | Immediately notify all other personnel in the facility of the situation and evacuate the area. | |
|  | **3** | Alert BCP committee personnel on the contact numbers given.  Provide them with your name, extension where you can be reached, building and room number, and the nature of the emergency. Follow all instructions given. | |
|  | **4** | Alert the ERT.  *Note:* During non-staffed hours, security personnel will notify the Senior Executive responsible for the location directly. |
|  | **5** | Notify Building Security.  Local security personnel will establish security at the location and not allow access to the site unless notified by the Senior Executive or his/her designated representative. |
|  | **6** | Contact appropriate vendor personnel to aid in the decision regarding the protection of equipment if time and circumstance permit. |
|  | **7** | All personnel evacuating the facilities will meet at their assigned supervisor/or person commanding outside location (assembly point) and follow instructions given by the designated authority. **Under no circumstances may any personnel leave without the consent of supervision.** |

### In the event of a network services provider outage

In the event of a network service provider outage to any location, the guidelines and procedures in this section are to be followed. Outage for more than one hour will make it a BCP situation. Immediately notify **Debasis Pati BCP Committee Contact: 9811686063/ Barsha Chakraborty 9811687845 / Ankur Kashyap 9717765849.**

|  |  |  |
| --- | --- | --- |
|  | **STEP** | **ACTION OWNER PM** |
|  | **1** | Notify senior management of outage.  Determine cause of outage and timeframe for its recovery. |
|  | **2** | If outage will be greater than one hour, route all calls via alternate services.  If it is a major outage and all carriers are down and downtime will be greater than 12 hours, deploy satellite phones, if available. |

### In the event equivalent to a flood or damage due to water deluge

In the event of a flood or broken water pipe / equipment within any computing facilities, the guidelines and procedures in this section are to be followed after assessing the extent of potential damage it can cause.

|  |  |  |
| --- | --- | --- |
|  | **STEP** | **ACTION** |
|  | **1** | Assess the situation and determine if outside assistance is needed; if this is the case, dial 0120-2402161 immediately. |
|  | **2** | Immediately notify all other personnel in the facility of the situation and be prepared to cease operations accordingly. |
|  | **3** | Immediately notify all other personnel in the facility of the situation and be prepared to cease operations accordingly. |
|  | **4** | Water detected below the raised floor may have different causes:   * If water is slowly dripping from an air conditioning unit and not endangering equipment, contact repair personnel immediately. * If water is of a major quantity and flooding beneath the floor (water main break), immediately implement power-down procedures. While power-down procedures are in progress, evacuate the area and follow management’s (floor commander’s) instructions. |

## BCP review and maintenance

This plan must be reviewed quarterly and exercised on half early basis. The test may be in the form of a table top or walk-through or simulation testing. Additionally, with the dynamic environment present within organization, it is important to review the listing of personnel and phone numbers contained within the plan regularly.

The hard-copy version of the plan will be stored in a common location where it can be viewed by site personnel, associates and the ERT. This document will be subjected to change management/version control.

**Emergency Response Checklist**

|  |  |
| --- | --- |
| * Start a log of actions taken: |  |
|  |  |
| * Liaise with Emergency Services: |  |
|  |  |
| * Identify any damage: |  |
|  |  |
| * Identify Functions disrupted: |  |
|  |  |
| * Convene your Response / Recovery Team: |  |
|  |  |
| * Provide information to staff: |  |
|  |  |
| * Decide on course of action: |  |
|  |  |
| * Communicate decisions to staff and business partners: |  |
|  |  |
| * Provide public information to maintain reputation and business: |  |
|  |  |
| * Arrange a Debrief: |  |
|  |  |
| * Review Business Continuity Plan: |  |

**Emergency Response Team**

The Emergency Response Team comprises of the System Team, the Network Recovery Team, and the Offsite Storage Teams.

**System Team**: This team will be responsible for the following activities in the event of a disaster. [SPOC - Ankur Kashyap]

1. Reinstalling operating systems, and applications like outlook, exchange server in the event of system crash or physical loss of server
2. Applying the patches and other configuration settings to restore the system to its previous state.
3. Restoring the application data from the latest backed up data set
4. Putting the system in production mode again
5. Monitoring the system performance & trouble shooting
6. Setting up the hardware equipment like servers.

**Network Recovery Team**: This team will be responsible for routing of the data through redundant communication links, in case there is a

network failure. This team is also responsible for setting up of hardware equipment like hubs, routers and cables. [SPOC – Rahul Saini]

**Offsite Storage Team:** This team will be responsible for obtaining, packaging and shipping backup media/tapes and other system related

documents and records to any designated recovery site. [SPOC - Ankur Kashyap]

**BCP Committee responsibilities**

* Review, testing, maintenance and control of BCP document.
* Arranging contingency sites / alternate work locations for business continuity.
* Exercise contracts/SLA/OLA with internal/external support groups/vendors.
* Designing response strategy & ensuring associates are equipped with necessary knowledge and skill to deal with the disaster situations.
* Make arrangements/agreements in advance with local banks, credit card companies, hotels, office suppliers, food suppliers, transport and others for emergency support.
* Process Improvement, Process Definition and Communication about the QMS update related to BCP
* Work closely with corporate communication for developing employee engagement needed for implementing BCP effectively.
* Facilitate meeting the IT Service Continuity requirements at a project level,

Feedback on Business Continuity Manual

# Please send the improvement feedbacks at sepg@gc-solutions.net.