Information Technology Policies and Procedures

Table of Contents

Topic	Page
1. Purpose and Scope	2
2. Help Desk	3
3. On-Call Policy	6
4. Storage and Backup Policy	7
5. The Magic System	8
6. IT Workflow Chart	10
7. Disaster Recovery Plan	11

Information Technology Policies and Procedures

Revised Date: May 1, 2010
Effective Date: May 1, 2010

Approved By: Christopher Campbell
IT Director

Purpose	This document contains the internal policies and procedures utilized by the KVC Health Systems Inc. Information Technology department.
Scope	These policies apply to the Information Technology department operations and guidelines as they pertain to supporting the overall mission of KVC Health Systems Inc and subsidiaries.

KVC Information Technology Mission Statement

The Information Technology department will provide the highest quality information services, in the most cost-effective manner, to support the mission of KVC in enriching and enhancing the lives of children and families.

To meet this mission we will:

- Provide fast & reliable access to all information systems
- Maintain all electronic systems used by KVC and subsidiaries.
- Coordinate with state and external partners to ensure technical compatibility
- Promote new uses of technology in an effort to enhance the productivity of KVC staff.
- Establish relations with vendors in order to obtain the lowest cost possible for our technology needs.
- Secure all data within KVC in accordance with all contracting organizations, government agencies and applicable laws.
- Support KVC staff in the use of technology systems in an effort to increase their productivity and functionality.
- Monitor all KVC electronic systems in an effort to ensure they are functioning at an optimum level.

Helpdesk Policy

- KVC employees can submit a request to the help desk via a web interface or by calling into the published help desk phone number.
- Information Technology requests include all hardware (Desktop/Laptop/Printer), all telecommunications (phone, fax, voicemail), all security (access permissions, passwords, account changes), and all off the shelf software (software not internally developed) requests.
- Each IT request is assigned a severity level from one to six, based on the following criteria:

  Severity Level 1 – Critical Impact (Service not available)
  - Service is unavailable or halted; or
  - Complete loss of service for all users or a single location; or
  - Loss of access to one or more global shared resources (server, application, phone system); or
  - Loss of communication with SRS

  AND
  - No ability to avoid or reduce the effect via a workaround

  Severity Level 2 – Major Impact (Severely Impaired)
  - Service is severely impaired or seriously degraded; or
  - Access to shared resources is functioning, but at a degraded level causing multiple users to lose the capability to be productive; or
  - Loss of access to one or more local shared resources (server, printer); or
  - Complete work stoppage for multiple users; or
  - Application critical to multiple users' primary function is unavailable; or
  - Admissions department unable to process SRS requests

  AND
  - There is no ability to avoid or reduce the effect via a workaround

  Severity Level 3 – Minor Impact (Single User Desktop/Critical Application)
  - Complete work stoppage for a single user; or
  - Single user unable to access application critical to user's primary job function; or
  - Single user unable to print to any printer; or
  - Multiple users unable to access KVC resources from home

  AND
  - There is no ability to avoid or reduce the effect via a workaround

Severity Level 4 – Low Impact (Single User Non-Critical Application)

- Single user unable to access critical application, workaround exists; or
- Single user unable to access application NOT critical to user's primary job function; or
- Single user unable to access application from home; or
- Single user unable to print to primary printer, secondary printer is available; or
- E-mail from outside accounts being blocked by spam filter

Severity Level 5 – No Immediate Impact

- Password resets
- Moves, adds, changes
- Software or hardware installations
- Access rights
- Exchange distribution list changes
- File restores

Severity Level 6

- Purchase Requests
- Cabling Requests

1.1.1. Service Level Standards

A Service Level Standard defines the level of service the IT department will provide to our users based on the severity of the request received.

Each priority level is assigned a Mean-Time-To-Resolution. The resolution time starts at the time a request is received. The goal of the IT department is to have the request completed and a confirmation from the user that the issue is resolved within the specified time limit.

Severity Level	**1**	**2**	**3**	**4**	**5**	**6**
Resolution Time (MTTR)	<4 clock hours	<8 clock hours	<24 business hours	<40 business hours	<56 business hours	<112 business hours
ESCALATION						
Escalation to Management occurs:	Immediately	<30 min	After resolution time expired	After resolution time expired	Not Escalated	Not Escalated

• Priorities 1, 2, 3 & 4s are Incidents (degradation in service) while Priority 5 & 6 are Service Requests (requests not related to service degradation)

•MTTR (Mean Time to Resolution) = Ticket Open to Ticket Resolution (note: all objectives above are from the time the ticket is initially opened)

- Once the severity level is assigned, the request is forwarded to the appropriate technician based on the originating office of the request and the user is notified that the request has been assigned.
- In order to track the performance of the IT helpdesk and ensure that requests are being completed on time, the following weekly reports are used:
    - Help Desk Call Report – details the number of calls received during the week, how many were answered, and how many went to voicemail.
    - First Call Report – details how many incoming support phone calls were able to be solved at the time of call.
    - Current Request Count – shows the total number of requests currently in the IT queue, the distribution among all technicians, and the number of requests currently overdue.
    - Overdue Requests Report – shows the details of any overdue requests for discussion and potential escalation.
- Once the request is completed, the request is closed and the user is notified via e-mail.

On-Call Policy

- Network Technician staff are required to be on-call for one week, on a rotational basis with other Network Technician staff.
- The weekly on-call period is from 2:00PM Wednesday to 1:59PM the following Wednesday.
- The on-call technician will be assigned a pager which must be carried at all times.
- Payment for on-call duties exceeding the normal 40 hour work week are paid at the standard overtime rate.
- It is the responsibility of the on-call technician to record any time spent responding to pages. All reported time should be rounded up to the nearest quarter-hour.
- On-call technicians have 30 minutes to respond to any page received.
- During each technician's assigned week, the assigned technician is responsible, and will be held accountable, for the timely resolution of all after-hours issues.
- Automated notifications from monitoring systems will be e-mailed to the on-call pager. Each technician is responsible for investigating these notifications during their on-call period.
- The on-call schedule will be posted in Outlook.
- Changes to the schedule require prior approval from the IT Director.
- When requesting a change, it is the responsibility of the scheduled on-call technician to secure a replacement for the entire week they are scheduled. If a replacement cannot be found the original scheduled technician must work the on-call. The switch request form must be submitted a minimum of 48 hours prior to start of the on-call period (Monday by 2:00PM) to be accepted. Any submissions after this time, except for a family emergency, will not be allowed.

Storage and Backup Policy

I. Storage

- KVC Health Systems Inc. utilizes an EMC Celerra Network Server as the primary storage server
- The storage server specifications are:
    - Two terabytes of storage drive space
    - Two data movers for speed and redundancy
    - Four gigabit ethernet interfaces which are channeled together in two channel groups for increased redundancy

II. Backup

- All KVC Health Systems Inc. servers are backed up to tape media on a nightly basis
- Tapes are stored in a fireproof safe in the KVC Health Systems Inc. Corporate Office in Olathe, KS
- Once per week, media containing a full backup of all servers is transported off-site and stored at the KVC Behavioral Healthcare office in Kansas City, KS
- Once per month, media containing a full backup is taken out of rotation and placed in long-term storage.

Information Technology Policies and Procedures

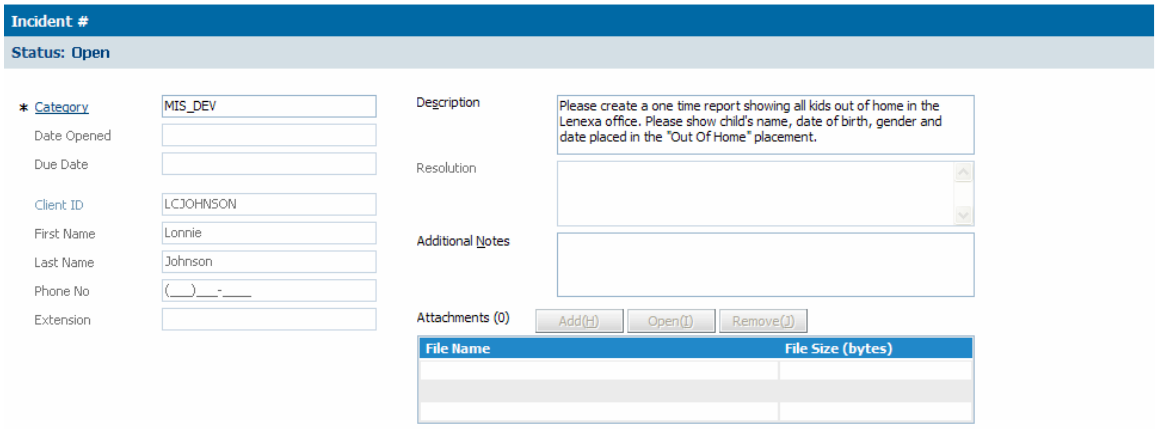
The MAGIC SYSTEM

Magic is a third party software system that KVC Health Systems Inc. uses to initiate, track and communicate about any issue, enhancement or concern with respect to hardware, software, data or any other technology need.

Employees use this system to notify us if something is broken, to identify a need to enhance an existing item, or create something new. It has proven to be invaluable in the on-going improvement of our software systems and applications. Every employee has a chance to voice an idea about how we can make the system more user-friendly, efficient and shape it in a way that we can get optimal use of the on data on our kids and homes.

The Information Technology department utilizes the Magic System exclusively to track and report on all open requests and projects.

A typical request would start with an employee filling out this form which is the first step of the Magic system.



Once that is filled out it automatically gets routed to our help desk staff for assignment.

An employee may go to the magic system at any time to see the status of their request. A list of open issues is displayed as such.

My Incidents - Open Showing 1 - 7 of 7

View: My Incidents | Open

Filter by: Incident # | OK | Clear

Incident #	Status	Open Date & Time	Client ID	Incident Description	Incident Resolution	Category Description
24212	OPEN	06/04/08 10:43:11 AM	LCJOHNSON	SIP - Create Regional Trainins, MA ...		MIS Project
35486	OPEN	05/06/09 8:54:11 AM	LCJOHNS ...	Add functionality from 18971 in the Document Manager to ...		MIS Project
35520	OPEN	05/07/09 10:49:31 AM	LCJOHNS ...	Convert Case Logs to a web based program.		MIS Project
42057	OPEN	12/16/09 9:33:20 AM	LCJOHNS ...	Please install dotnet 3.5 framework on the citrix servers. A ...		Software Setup
42204	OPEN	12/22/09 1:41:51 PM	LCJOHNS ...	Per conversation with Liz Croney, create a system that will ...		MIS Project
42987	OPEN	01/25/10 1:22:23 PM	LCJOHNS ...	Edit connection strings in all .net applications for mirrored se ...		SQL Database Enhance ...
43316	OPEN	02/04/10 7:47:22 AM	LCJOHNS ...	DataAdmin: There is a bug when Lonnie Johnson is assigne ...		MIS Tools

At this point an employee may select any of the items to get a more detailed view.

Incident # 42057

Status: Open

* Category	SOFTWARE SETUP
Date Opened	12/16/09 9:33:20 AM
Due Date	03/10/10 1:08:48 PM
Client ID	LCJOHNSON
First Name	Lonnie
Last Name	Johnson
Phone No	(___)___-____
Extension	

Description: Please install dotnet 3.5 framework on the citrix servers. As we move from MS Access development we will go to vb winforms for small to medium rapid application development. Our most recent

Resolution:

Additional Notes:

Attachments (0) Add(H) Open(I) Remove(J)

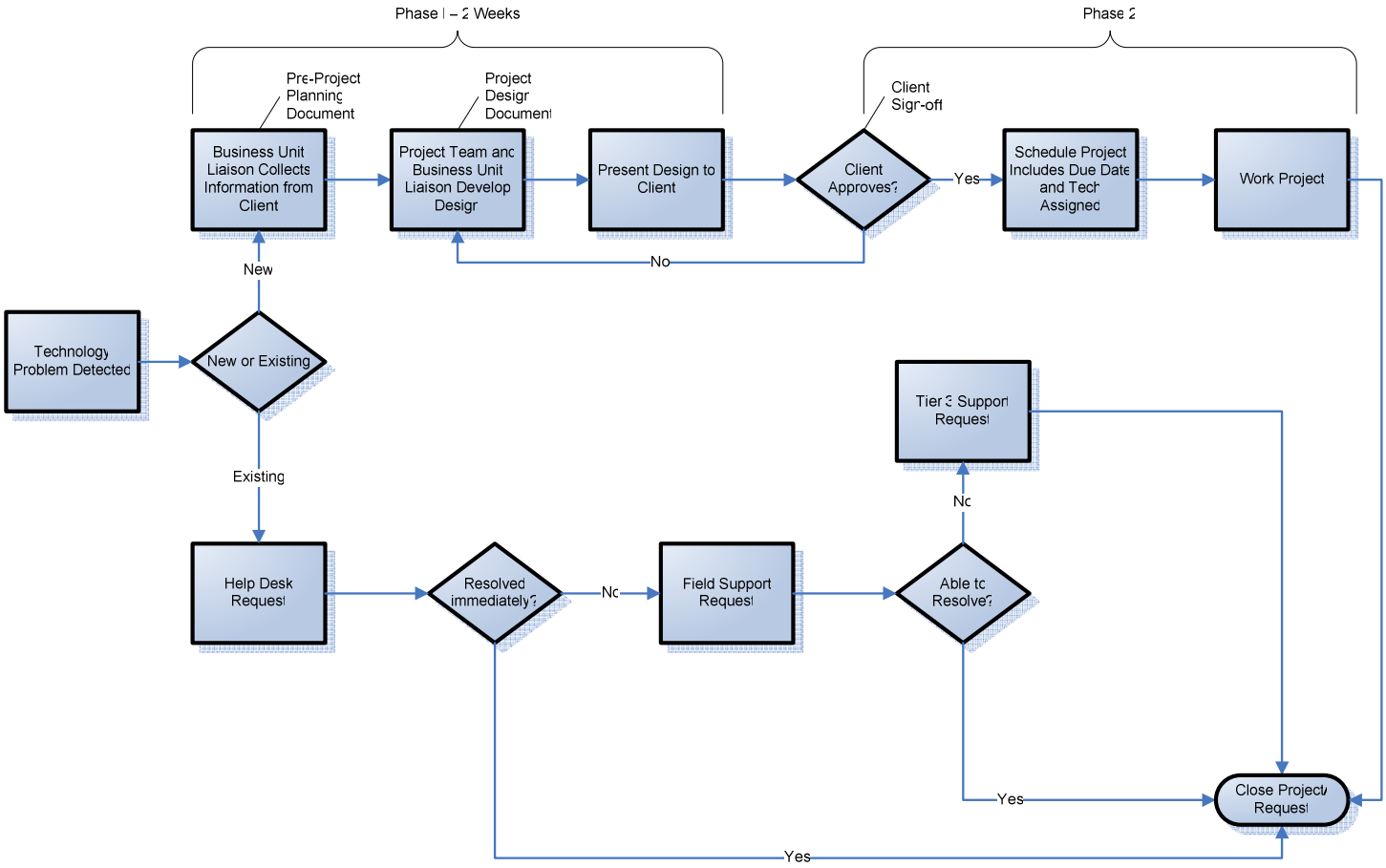
File Name	File Size (bytes)

Once a request has been completed the employee is notified via email with the results.

Information Technology Policies and Procedures

Below is a chart showing how a request travels through the different points of the department by way of the magic system.

IT Workflow Diagram



KVC Health Systems Inc.
Disaster Recovery Plan

1. INTRODUCTION

1.1 PURPOSE

This IT Infrastructure Disaster Recovery Plan establishes procedures to recover the IT Infrastructure following a disruption. The following objectives have been established for this plan:

- Maximize the effectiveness of contingency operations through an established plan that consists of the following phases:
  - **Notification/Activation phase** to detect and assess damage and to activate the plan
  - **Recovery phase** to restore temporary IT operations and recover damage done to the original system
  - **Reconstitution phase** to restore IT system processing capabilities to normal operations.
- Identify the activities, resources, and procedures needed to carry out IT Infrastructure processing requirements during prolonged interruptions to normal operations.
- Assign responsibilities to designated KVC Health Systems Inc. personnel and provide guidance for recovering IT Infrastructure during prolonged periods of interruption to normal operations.
- Ensure coordination with other KVC Health Systems Inc. staff who will participate in the contingency planning strategies. Ensure coordination with external points of contact and vendors who will participate in the contingency planning strategies.

1.2 APPLICABILITY

The IT Infrastructure Disaster Recovery Plan applies to the functions, operations, and resources necessary to restore and resume KVC Health Systems's IT Infrastructure operations as it is installed at primary location in Olathe, KS. The IT Infrastructure Disaster Recovery Plan applies to KVC Health Systems Inc. and all other persons associated with IT Infrastructure as identified under Section 2.3, Responsibilities.

1.3 SCOPE

1.3.1 Planning Principles

Various scenarios were considered to form a basis for the plan, and multiple assumptions were made. The applicability of the plan is predicated on two key principles:

- The KVC Health Systems Inc. facility in Olathe, KS, is inaccessible; therefore, KVC Health Systems Inc. is unable to perform IT Infrastructure processing for the company.

- A valid contract exists with the alternate site that designates that site in Overland Park, KS, as the KVC Health Systems alternate operating facility.

  – KVC Health Systems Inc. will use the alternate site building and IT resources to recover IT Infrastructure functionality during an emergency situation that prevents access to the original facility.

  – The designated computer system at the alternate site has been configured to begin processing IT Infrastructure information.

  – The alternate site will be used to continue IT Infrastructure recovery and processing throughout the period of disruption, until the return to normal operations.

1.3.2 Assumptions

Based on these principles, the following assumptions were used when developing the IT Disaster Recovery Plan:

- The IT Infrastructure is inoperable at the primary location and cannot be recovered within 48 hours.
- Key IT Infrastructure personnel have been identified and trained in their emergency response and recovery roles; they are available to activate the IT Infrastructure Disaster Recovery Plan.
- Preventive controls (e.g., generators, environmental controls, waterproof tarps, sprinkler systems, fire extinguishers, and fire department assistance) are fully operational at the time of the disaster.
- Computer center equipment, including components supporting IT Infrastructure, are connected to an uninterruptible power supply (UPS) that provides 45 minutes to 1 hour of electricity during a power failure.
- IT Infrastructure hardware and software at the KVC Health Systems Inc. original site are unavailable for at least 48 hours.
- Current backups of the application software and data are intact and available at the offsite storage facility.
- The equipment, connections, and capabilities required to operate IT Infrastructure are available at the alternate site in Overland Park, KS and/or service agreements are maintained with IT Infrastructure hardware, software, and communications providers to support the emergency system recovery.

1.4 REFERENCES/REQUIREMENTS

This IT Infrastructure Disaster Recovery Plan complies with the KVC Health Systems Inc. IT contingency planning policy as follows:

> The organization shall develop a contingency planning capability to meet the needs of critical supporting operations in the event of a disruption extending beyond 72 hours. The procedures for execution of such a capability shall be documented in a formal contingency plan and shall be reviewed at least annually and updated as necessary. Personnel responsible for target systems shall be trained to execute contingency procedures. The plan, recovery capabilities, and personnel shall be tested to identify weaknesses of the capability at least annually.

2. CONCEPT OF OPERATIONS

2.1 SYSTEM DESCRIPTION AND ARCHITECTURE

The IT Infrastructure of KVC Health Systems Inc. consists of five critical parts, listed in order of importance.

- The SQL database server is required to access data about the children in our care.
- The phone system, including two Cisco servers is required to support admissions and the case workers.
- The Exchange E-mail server is required to continue communication with state organizations.
- A valid internet connection is required to support incoming/outgoing e-mail.
- Citrix server farm is required to support field workers.

2.2 LINE OF SUCCESSION

KVC Health Systems Inc sets forth an order of succession, in coordination with the order set forth by the department to ensure that decision-making authority for the IT Infrastructure Disaster Recovery Plan is uninterrupted. The Senior VP – Administrative Services, KVC Health Systems Inc. is responsible for ensuring the safety of personnel and the execution of procedures documented within this IT Infrastructure Disaster Recovery Plan. If the Senior VP – Administrative Services, KVC Health Systems Inc. is unable to function as the overall authority or chooses to delegate this responsibility to a successor, the CFO shall function as that authority.

2.3 RESPONSIBILITIES

The following teams have been developed and trained to respond to a contingency event affecting the IT system.

The Disaster Recovery Plan establishes several teams assigned to participate in recovering IT Infrastructure operations. The Recovery Team is responsible for recovery of the IT Infrastructure computer environment and all applications. Members of the team name include personnel who are also responsible for the daily operations and maintenance of IT Infrastructure. The team leader title directs the Recovery Team.

Recovery Team A consists of: Christopher Campbell(Leader), Anthony Gussio, Chad Haines.
Recovery Team B consists of: Jeremiah Schultz(Leader), Lonnie Johnson, and Michael Brown

3. NOTIFICATION AND ACTIVATION PHASE

This phase addresses the initial actions taken to detect and assess damage inflicted by a disruption to IT Infrastructure. Based on the assessment of the event, the plan may be activated by the Contingency Planning Coordinator.

In an emergency, KVC Health Systems' top priority is to preserve the health and safety of its staff and clients before proceeding to the Notification and Activation procedures.

Contact information for key personnel is located in Appendix A. The notification sequence is listed below:

- The first responder is to notify the Contingency Planning Coordinator. All known information must be relayed to the Contingency Planning Coordinator.
- The Contingency Planning Coordinator is to instruct the Recovery Team Leaders to begin assessment procedures.
- The Recovery Team Leader is to notify team members and direct them to complete the assessment procedures outlined below to determine the extent of damage and estimated recovery time.

Damage Assessment Procedures:
(Detailed procedures should be outlined to include activities to determine the cause of the disruption; potential for additional disruption or damage; affected physical area and status of physical infrastructure; status of IT equipment functionality and inventory, including items that will need to be replaced; and estimated time to repair services to normal operations.)

- When damage assessment has been completed, the Damage Assessment Team Leader is to notify the Contingency Planning Coordinator of the results.
- The Contingency Planning Coordinator is to evaluate the results and determine whether the contingency plan is to be activated and if relocation is required.
- Based on assessment results, the Contingency Planning Coordinator is to notify assessment results to civil emergency personnel (e.g., police, fire) as appropriate.

The Contingency Plan is to be activated if one or more of the following criteria are met:

1. IT Infrastructure will be unavailable for more than 48 hours
2. Facility is damaged and will be unavailable for more than 24 hours
3. Other criteria, as appropriate.

- If the plan is to be activated, the Contingency Planning Coordinator is to notify all Team Leaders and inform them of the details of the event and if relocation is required.
- Upon notification from the Contingency Planning Coordinator, Team Leaders are to notify their respective teams. Team members are to be informed of all applicable information and prepared to respond and relocate if necessary.
- The Contingency Planning Coordinator is to notify the off-site storage facility that a contingency event has been declared and to ship the necessary materials (as determined by damage assessment) to the alternate site.

- The Contingency Planning Coordinator is to notify the Alternate site that a contingency event has been declared and to prepare the facility for the Organization's arrival.
- The Contingency Planning Coordinator is to notify remaining personnel (via notification procedures) on the general status of the incident.

4. RECOVERY OPERATIONS

This section provides procedures for recovering the application at the alternate site, whereas other efforts are directed to repair damage to the original system and capabilities.
The following procedures are for recovering the IT Infrastructure at the alternate site. Procedures are outlined per team required. Each procedure should be executed in the sequence it is presented to maintain efficient operations.

Recovery Goal. Prepare recovery server

- Recovery Team A
  - Install hardware necessary for recovering data at off-site facility, including server and tape drive.
  - Install software necessary for recovering data on server at off-site facility

Recovery Goal. Restore phone service

- Recovery Team A
  - Reconfigure Cisco Call Manager at off-site facility
  - Instruct communication provider to re-route incoming phone communications to a phone circuit at off-site facility.
  - Program phones necessary for admissions phone communications

Recovery Goal. Restore SQL database

- Recovery Team B
  - Install hardware necessary for recovering data on server
  - Install SQL Server software on hardware
  - Recover SQL Databases via recovery server
  - Re-route communications to new SQL server for all remote sites.

Recovery Goal. Restore Exchange E-mail Server

- Recovery Team A
  - Install hardware necessary for recovering data on server
  - Install Exchange E-mail software on hardware
  - Recover Exchange E-mail Databases via recovery server
  - Re-route communications to new Exchange server for all remote sites.

Recovery Goal. Restore Internet Communications

- Recovery Team B
  - Install hardware necessary for internet communications
  - Instruct communications provider to bring up backup internet service

- Re-route KVC internet traffic to new internet connection

Recovery Goal. Restore Citrix Server

- Recovery Team A
  - Install hardware necessary for recovering data on server
  - Install Citrix software on hardware
  - Re-route communications to new Citrix server for all remote sites.

5. RETURN TO NORMAL OPERATIONS

This section discusses activities necessary for restoring IT Infrastructure operations at the KVC Health Systems original or new site. When the computer center at the original or new site has been restored, IT Infrastructure operations at the alternate site must be transitioned back. The goal is to provide a seamless transition of operations from the alternate site to the computer center.

Original or New Site Restoration

Procedures should be outlined, per necessary team, to restore or replace the original site so that normal operations may be transferred. IT equipment and telecommunications connections should be tested.

5.1 CONCURRENT PROCESSING

Procedures should be outlined, per necessary team, to operate the system in coordination with the system at the original or new site. These procedures should include testing the original or new system until it is functioning properly and the contingency system is shut down gracefully.

Restoration Goal. Restore power to data center

- Recovery Team A
  - Ensure that stable power is provided to building

Restoration Goal. Power-on network and server equipment

- Recovery Team A
  - Power on equipment in following order:
    1. Cisco network infrastructure
    2. Microsoft Active Directory Servers
    3. EMC Storage Server
    4. Exchange E-mail Server
    5. Microsoft SQL Server
    6. Citrix Server Farm

Restoration Goal. Test application availability

- Recovery Team B
  - Test ASD applications and database access

Restoration Goal. Restore Phone Systems

- Recovery Team A
  - Coordinate with telephone provider to restore call routing to primary location.

6. PLAN APPENDICES

The appendices included should be based on system and plan requirements.

A. Personnel Contact List

Information Technology Policies and Procedures

Appendix A: Personnel Contact List

Name	Role	Phone
Renny Arensberg	Contingency Planning Coordinator	913-710-5153
Christopher Campbell	Recovery Team A Leader	913-660-8648
Chad Haines	Recovery Team A Member	913-322-4939
Anthony Gussio	Recovery Team A Member	913-568-6471
Jeremiah Schultz	Recovery Team B Leader	913-530-6984
Lonnie Johnson	Recovery Team B Member	913-744-5407
Michael Brown	Recovery Team B Member	816-769-4693