Information Technology Statement of Intent

This document delineates our policies and procedures for technology disaster recovery, as well as our process-level plans for recovering critical technology platforms and the telecommunications infrastructure. This document summarizes our recommended procedures. In the event of an actual emergency situation, modifications to this document may be made to ensure physical safety of our people, our systems, and our data.

Our mission is to ensure information system uptime, data integrity and availability, and business continuity.

Policy Statement

.

- A formal risk assessment shall be undertaken to determine the requirements for the disaster recovery plan.
- The disaster recovery plan should cover all essential and critical infrastructure elements, systems and networks, in accordance with key business activities.
- The disaster recovery plan should be periodically tested in a simulated environment to ensure that it can be implemented in emergency situations and that the management and staff understand how it is to be executed.
- All staff must be made aware of the disaster recovery plan and their own respective roles.
- The disaster recovery plan is to be kept up to date to take into account changing circumstances.

Objectives

The principal objective of the disaster recovery program is to develop, test and document a well-structured and easily understood plan which will help the City recover as quickly and effectively as possible from an unforeseen disaster or emergency which interrupts information systems and business operations. Additional objectives include the following:

- The need to ensure that all employees fully understand their duties in implementing such a plan
- The need to ensure that operational policies are adhered to within all planned activities
- The need to ensure that proposed contingency arrangements are cost-effective
- The need to consider implications on other City sites
- Disaster recovery capabilities as applicable to key customers, vendors and others

The major goals of this plan are the following:

- To minimize interruptions to the normal operations.
- To limit the extent of disruption and damage.
- To minimize the economic impact of the interruption.
- To establish alternative means of operation in advance.
- To train personnel with emergency procedures.
- To provide for smooth and rapid restoration of service.
-

Key Personnel Contact Info

Name, Title	Contact Option	Contact Number
	Work	
	Alternate	
	Mobile	
	Home	
	Email Address	
	Alternate Email	
	Work	
	Alternate	
	Mobile	
	Home	
	Email Address	
	Alternate Email	
	Work	
	Alternate	
	Mobile	
	Home	
	Email Address	
	Alternate Email	
	Work	
	Alternate	
	Mobile	
	Home	
	Email Address	
	Alternate Email	
	Work	
	Alternate	
	Mobile	
	Home	
	Email Address	
	Alternate Email	

Name, Title	Contact Option	Contact Number
	Work	
	Alternate	
	Mobile	
	Home	
	Email Address	
	Alternate Email	

Preparing for Hurricanes

Interior Preparations:

- Verify that vital records are in a safe storage area. Files, records and storage cabinets might be wrapped in plastic for moisture protection. If necessary, temporarily relocate records to a safe storage facility off-site.

Disconnect all electrical appliances and equipment

Close and lock all windows. Draw the blinds or drapes

Gather all relevant network infrastructure documents, e.g., network diagrams, equipment configurations, databases

Take Inventory of IT Equipment

Complete an inventory of all computers, equipment, supplies and receipts/verification of ownership to show your insurance provider post-disaster

Moving to more affordable disaster recovery solutions

Obtaining an inventory of what is on the network, knowing spare parts to have available for potential hardware problems as well as localized events, knowing the criticality of each of the inventoried items to determine priority in the recovery stage, and capturing configuration data for every device are a few essential processes in rapid recovery

Diagram your current network and identify network devices

In case of an emergency things to look for:

- Origin of the emergency or disruption
- Potential for additional disruptions or damage
- Area affected by the emergency
- Status of physical infrastructure
- Inventory and functional status of the most important equipment
- Type of damage to equipment
- Items to be replaced
- Estimated time to restore normal services if disaster procedures were not in place

Activation Planning

- List of systems and services that need to be restored
- Their interdependencies and sequence of restoration
- Time estimations for each restoration (documented in the plan)
- Instructions for reporting failures to the team leads
- Plan for communication between teams

1.3 Backup Strategy

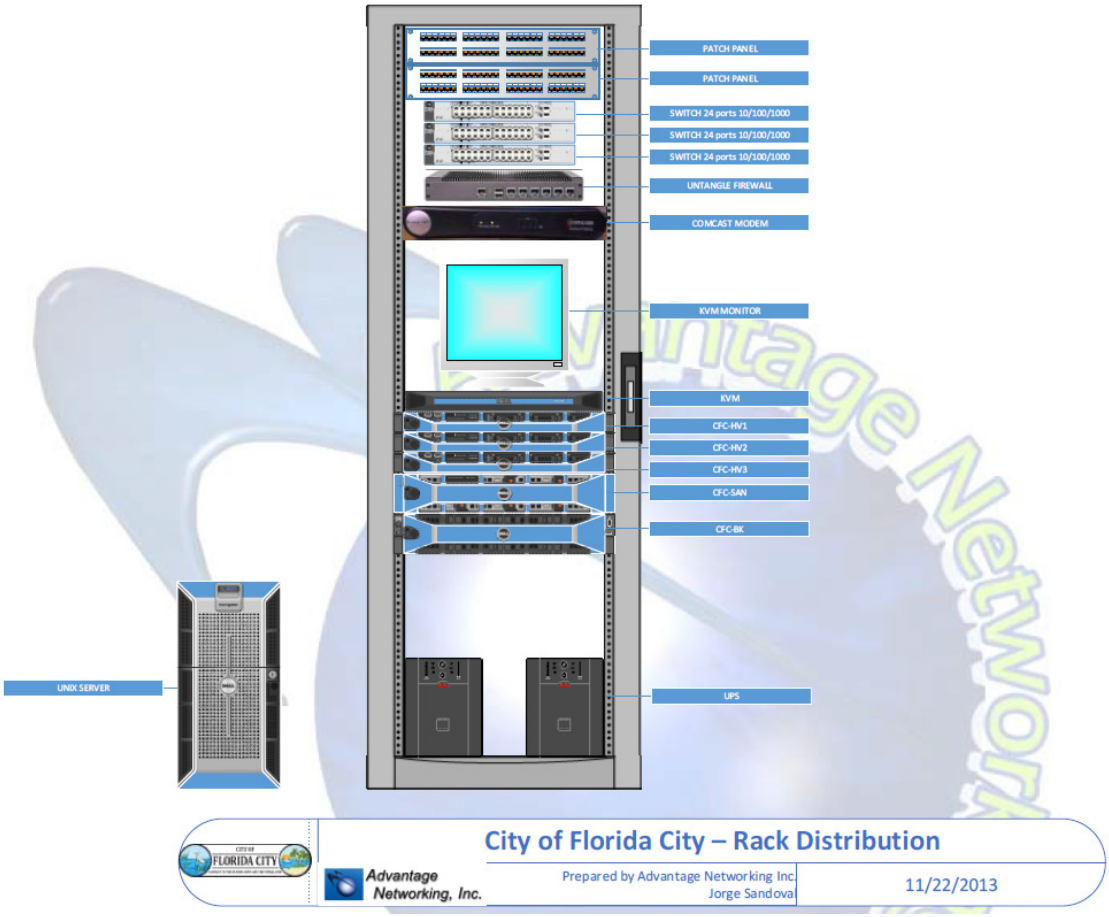
Key business processes and the agreed backup strategy for each are listed below. The strategy chosen is for a fully mirrored recovery site at the City's IT office. This strategy entails the maintenance of a fully mirrored duplicate site which will enable instantaneous switching between the live site (headquarters) and the backup site.

KEY BUSINESS PROCESS	BACKUP STRATEGY
IT Operations	Fully mirrored recovery site
Tech Support - Hardware	Fully mirrored recovery site
Tech Support - Software	Fully mirrored recovery site
Facilities Management	Fully mirrored recovery site
Email	Fully mirrored recovery site
Purchasing	Fully mirrored recovery site
Disaster Recovery	Fully mirrored recovery site
Finance	Fully mirrored recovery site
Contracts Admin	Fully mirrored recovery site
Warehouse & Inventory	Fully mirrored recovery site
Product Sales	Fully mirrored recovery site
Maintenance Sales	Fully mirrored recovery site
Human Resources	Off-site data storage facility
Testing Fully Mirrored Recovery site -	Fully mirrored recovery site
Workshop Fully Mirrored Recovery site -	Fully mirrored recovery site
Call Center	Fully mirrored recovery site
Web Site	Fully mirrored recovery site

Application	Data Communication Method to Disaster Recovery Site	Disaster Recovery Restore Method
Active Directory, DNS, DHCP	Backups stored at the Bunker	Restore from Backup
Active Directory, DNS	Backups stored at the Bunker	Restore from Backup
File Server	Backups stored at the Bunker	Restore from Backup
Hyper-V Hosts	Backups stored at the Bunker	Restore from Backup
Print Server, Print Manager Pus	Backups stored at the Bunker	Restore from Backup

Rack Distribution

How the servers are distributed into the Rack.

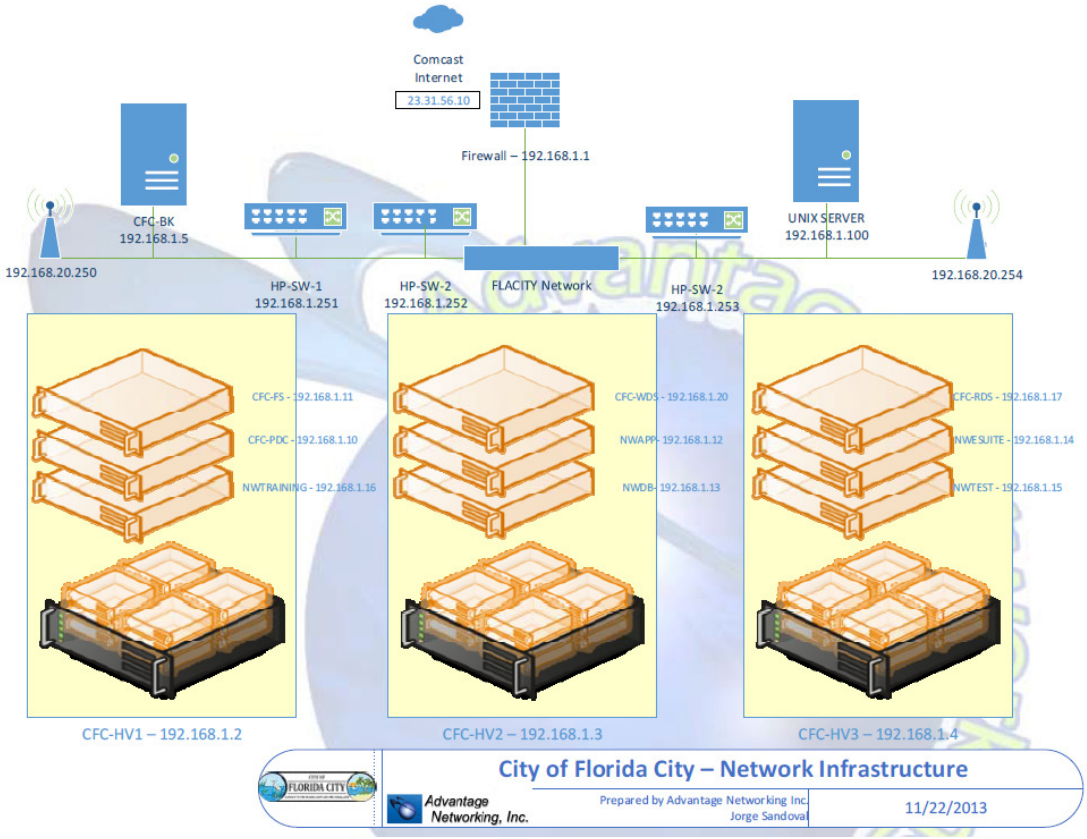


M:\AdvantageNetworking\City_of_Florida_City__IT_Information_Final_Document_V1.pdf

Network Diagram

The following diagram shows the network connectivity inside the Boca building

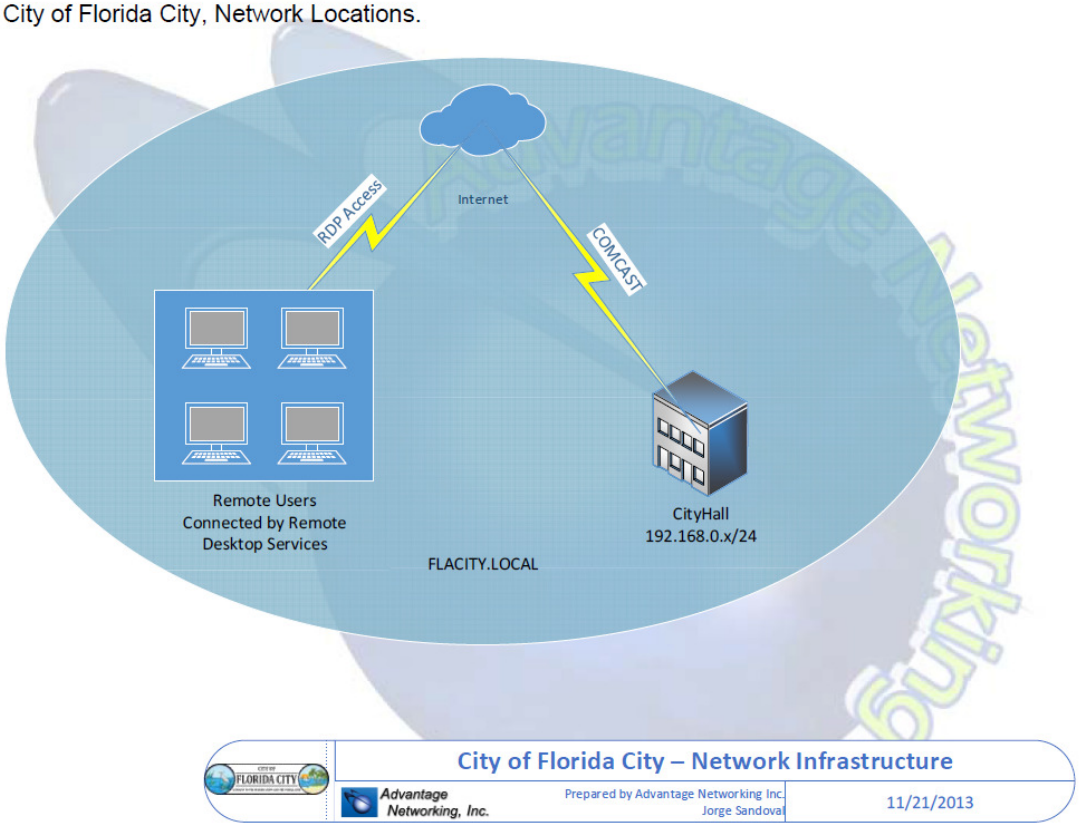
LAN Distribution



Network Topology

Sites

City of Florida City, Network Locations.



Network Sites

Risk Management

There are many potential disruptive threats which can occur at any time and affect the normal business process. We have considered a wide range of potential threats and the results of our deliberations are included in this section. Each potential environmental disaster or emergency situation has been examined. The focus here is on the level of business disruption which could arise from each type of disaster.

Potential disasters have been assessed as follows:

Potential Disaster	Probability Rating	Impact Rating	Brief Description Of Potential Consequences & Remedial Actions
Flood	3	4	All critical equipment is located on 1st Floor
Fire	3	4	FM200 suppression system installed in main computer centers. Fire and smoke detectors on all floors.

Tornado	5		
Electrical storms	5		
Act of terrorism	5		
Act of sabotage	5		
Electrical power failure	3	4	Redundant UPS array together with auto standby generator that is tested weekly & remotely monitored 24/7. UPSs also remotely monitored.
Loss of communications network services	4	4	Two diversely routed T1 trunks into building. WAN redundancy, voice network resilience

Probability: 1=Very High, 5=Very Low Impact: 1=Total destruction, 5=Minor annoyance

Plan Triggering Events

Key trigger issues at headquarters that would lead to activation of the DRP(Disaster Recovery Plan) are:

- Total loss of all communications
- Total loss of power
- Flooding of the premises
- Loss of the building

Recovery Procedures

The disaster recovery plan should provide detailed procedures to restore the system or system components. Procedures for IT service damage should address specific actions such as:

- Get authorization to access damaged premises or geographic area
- Notify users associated with the system
- Obtain required office supplies and work space
- Obtain and install required hardware components
- Obtain and load backup media
- Restore critical operating systems and application software
- Restore system data
- Test system functionality including security controls
- Connect system to network or other external systems

Reconstitution Phase

In the reconstitution phase, operations are transferred back to the original facility once it is free from the disaster aftereffects, and execution-phase activities are subsequently shut down. If the original system or facility is unrecoverable, this phase also involves rebuilding. Hence the reconstitution phase may last for a few days to few weeks or even months, depending on the severity of destruction and the site's fitness for restoration. As soon as the facility, whether repaired or replaced, is able to support its normal operations, the services may be moved back. The execution team should continue to be engaged until the restoration and testing are complete.
The following major activities occur in this phase:

- Continuously monitor the site or facility's fitness for reoccupation
- Verify that the site is free from aftereffects of the disaster and that there are no further threats
- Ensure that all needed infrastructure services, such as power, water, telecommunications, security, environmental controls, office equipment, and supplies, are operational

- Install system hardware, software, and firmware
- Establish connectivity between internal and external systems
- Test system operations to ensure full functionality
- Secure, remove, and relocate all sensitive materials at the contingency site
- Arrange for operations staff to return to the original facility

The Disaster Recovery Plan Document

The outcome of the disaster recovery planning process is the disaster recovery plan document. During an emergency, this document will be the primary source of information for disaster recovery procedures.

Document Contents

The disaster recovery plan document is the only reliable source of information for the disaster recovery during an emergency. It should be very easily readable, with simple and detailed instructions. Following are some of the contents that need to be in this document.

- **Document Information:** The document should include information such as the authors/owners with their contact details, revision history and other document details (name, location, version), references, and the audience of the document. In the document revision history, it is good to have a brief description of the changes made in each version. A table of contents is a must for quick reference, and it is highly recommended that the sections be numbered to the lowest possible level for easy reference purpose. It is also good to give an appropriate confidential status for the document as it contains sensitive information.
- **Purpose:** The purpose of the document must be clearly stated in the introduction, defining the objectives the plan intends to achieve.
- **Scope:** The scope of the plan defines the circumstances under which the plan is invoked and the length of time the procedures defined in the document are in effect. The different failure conditions that lead to invoking the plan should be clearly listed. For example, a system being down for couple of hours may not result in invoking the plan, but a daylong outage may suffice. Similarly, the conditions at the failed system/facility that warrant the reconstitution phase should also be clearly stated.
- **Assumptions:** Any conditions the plan assumes to be present for success should be clearly stated. This may involve listing the dependencies of the plan as well. For example, a certain number of trained personnel may be assumed to be available at the disaster recovery facility. Wherever possible, these dependencies must be accompanied with the appropriate contact details.
- **Exclusions:** Any related disaster activities that the plan does not cover should be stated and any known references mentioned here. For example, the plan may exclude the dependent power restoration plan, referring instead to the appropriate document and the department contact details. Such information will be useful during the disaster recovery.
- **System Description:** The description of the disaster recovery system should be simple to understand with appropriate figures, workflow charts, and so on. If necessary the descriptions may reference appendices that give more detail. The functions that need to be revived need to be clearly mentioned.
- **Roles and Responsibilities:** The roles of the managerial and technical staff and their responsibilities during the activation, execution, and reconstitution phases should be clearly listed. An organization structure diagram showing the reporting relationships is beneficial. Key roles should have primary and alternate personnel assigned.
- **Contact Details:** Full contact information should be included for all the managerial and technical staff involved in the planning, activation, execution, and reconstitution phases. Contact details both during normal situations and emergency situations should be mentioned. This information is recommended to be added as an appendix to the disaster recovery plan document.
- **Activation Procedures:** The procedures for notification, damage assessment, and activation planning should be outlined. Any topic that needs to be covered in great detail may be added as an appendix.
- **Execution Procedures:** The recovery procedure for each of the components the plan covers should be explained step by step in detail. When there are parallel threads of tasks, it is beneficial to have a flow chart diagram to visualize the dependencies of the tasks. The success and failure criteria of each procedure also should be mentioned as well as instructions on further actions in case of both success and failure.
- **Reconstitution Procedures:** Similar procedures for the reconstitution of the components should be explained in detail. The success and failure criteria and instructions for further actions in case of success and failure should be given.

• **Periodic Updates:** Technologies, systems, and facilities that the plan covers may change over time. It is important that the disaster recovery plan document reflect the current information about the components it covers. For this purpose, the Disaster Recovery Committee should ensure that the document is audited periodically (say once every quarter) against the present components in the organization. Another way to achieve this is to ensure that the committee is notified of any change that happens to any system/component in the organization so that the committee may update the document accordingly