

Business and Service Continuity Plan



Teams, Contacts, Logistics, and Facilities

Methods & Procedures

(External Version: Certain proprietary information has been intentionally omitted or redacted)

1. OVERVIEW 4

2. EMERGENCY RESPONSE AND RESTORATION TEAMS..... 6

2.1. EXECUTIVE TEAM..... 7

2.2. EVENT CHAIRPERSONS 7

2.3. EMERGENCY TEAM CHART 8

2.4. EVENT SUPPORT TEAM..... 11

2.5. EMERGENCY RESPONSE/RESTORATION TEAM CENTER..... 11

2.5.1. OTHER EMERGENCY CENTER LOCATIONS..... 12

2.5.2. NETWORK OPERATIONS CENTERS 12

2.5.3. ALTERNATE LOCATION RESOURCES..... 12

2.6. ORGANIZATIONAL AND LOCATION PRIORITIES 13

3. DETAILED METHODS AND PROCEDURES 15

PROCEDURE CATALOG 15

GENERAL RESPONSE AND RESTORATION PROCEDURE 17

3.1.1. IMMEDIATE ACTION..... 17

3.1.2. ASSESSMENT 17

3.1.3. RESPONSE 19

3.1.4. RESTORATION 19

3.2. DISRUPTING EVENT PROCEDURES 21

3.2.1. SNOW STORM 22

3.2.2. COMMERCIAL POWER DOWN 23

3.2.3. HVAC DOWN 24

3.2.4. GAS LEAK..... 25

3.2.5. WATER LEAK 27

3.2.6. VOICE COMMUNICATIONS DOWN 28

3.2.7. MULTIPLE APPLICATIONS DOWN..... 29

3.2.8. COMPUTER HACKER 30

3.2.9. INTERNAL WALKOUT/STRIKE 31

3.2.10. EXTERNAL STRIKE/WALKOUT 32

3.2.11. BIOHAZARD 32

3.2.12. HOSTAGE/VIOLENCE IN BUILDING..... 33

3.2.13. TERRORISM AND WIDESPREAD ATTACK..... 35

3.3. PANDEMIC PLANNING..... 37

3.3.1. PLANNING AND RESPONSE GOALS..... 37

3.3.2. ASSUMPTIONS 37

3.3.3. ADVANCED PANDEMIC PREPAREDNESS RECOMMENDATIONS 37

3.4. PANDEMIC RESPONSE PROCEDURES..... 39

3.4.1. PANDEMIC RESPONSE 39

3.4.2. POST-PANDEMIC RESPONSE 39

3.5. SERVICE-PROVIDING NETWORK RESPONSE AND RESTORATION PROCEDURES 40

Business and Service Continuity - Crown Castle Fiber

TRANSFER NOC FUNCTION	40
3.5.1. OUTSIDE PLANT RECOVERY AND RESTORATION	41
3.5.2. OUTSIDE PLANT FAILURE	42
3.5.3. NETWORK NODE RECOVERY AND RESTORATION	42
3.5.4. NETWORK NODE FAILURE.....	44
3.5.5. NETWORK ELEMENT FAILURE	45
3.5.6. RELOAD NETWORK ELEMENT.....	45
3.5.7. REPLACE NETWORK ELEMENT	46
3.5.8. BYPASS NETWORK ELEMENT	47
3.5.9. NETWORK ELEMENT CONFIGURATION AND RESTORATION	48
3.6. BUSINESS PROCESS RECOVERY AND RESTORATION PROCEDURES	48
3.6.1. TEMPORARY WORK LOCATION	48
3.6.2. MEDIUM-TERM SITE RELOCATION.....	48
3.6.3. RECOVER TELECOMMUNICATIONS	49
3.6.4. RESTORE STAFFING LEVELS	50
<u>4. IT SYSTEMS BUSINESS CONTINUITY STRATEGY</u>	<u>51</u>
4.1. SYSTEM / APPLICATION MITIGATION AND RESPONSE STRATEGY TABLE	51
4.2. APPLICATION/SERVER FAILURE	53
4.3. DHCP FAILURE	55
4.4. DOMAIN CONTROLLER FAILURE	56
4.5. PERSONAL COMPUTER LOSS.....	57
4.6. INTERNAL LAN/WAN FAILURE	58
4.7. SYSTEM MONITORING	59
4.8. DATA BACKUP AND RETENTION.....	59
4.9. PASSWORD MANAGEMENT	60
4.10. SUPPORTING IT DOCUMENTATION	60
<u>5. APPENDIX</u>	<u>61</u>
5.1. ANCILLARY PROCEDURES	61
5.1.1. GENERAL FIRE / EVACUATION PROCEDURES	61
5.1.2. FIRE / EVACUATION LEADS	63
5.1.3. EMERGENCY PURCHASE AND CASH PROCEDURES	65
5.1.4. PANIC AVOIDANCE MEASURES.....	65
5.1.5. BUSINESS CONTINUITY PLAN (BCP) EMPLOYEE ALERT HOTLINE	65
5.1.6. NOC CRISIS BRIDGE.....	66
5.1.7. IT MANAGEMENT NOTIFICATION SYSTEM.....	66
5.1.8. TELECOMMUNICATIONS SERVICE PRIORITY (TSP)	66
5.2. FORMS	67
5.2.1. CRITICAL EVENT SUMMARY FORM.....	67
5.2.2. CRITICAL EVENT LOGGING FORM.....	68
5.2.3. DAMAGE ASSESSMENT FORM	69
5.2.4. PURCHASE ORDER FORM	70

1. Overview

This document outlines the foundations for the Business Continuity Plan for Crown Castle Fiber (“Crown Castle Fiber”). The data and procedures are to be utilized as a guide to manage business through potential disruptions in the event of a disaster affecting personnel and/or business offices, nodes, or other facilities.

The policies and recommendations herein are designed to allow continuation of business and minimize impact and risk while enabling Crown Castle Fiber personnel to perform necessary steps to efficiently recover and restore to normal operations.

Crown Castle Fiber Emergency Response and Restoration Teams are described, along with resource lists, equipment descriptions, emergency contacts, and supporting methods and procedures for restoration of networks and operations.

Specifically, this document covers significant disruptions to the Crown Castle Fiber entities described in the following table:

ENTITY	COMPONENT	DETAILS
Service-Providing Infrastructure	Physical OSP Infrastructure	<ul style="list-style-type: none"> Fiber Manholes Poles
	Core Node Locations	File Omitted
	Operations Support Infrastructure	<ul style="list-style-type: none"> Network Operations Centers (NOCs) at a) 80 Central St, Boxborough, MA, b) 201 Old Country Rd [REDACTED] Melville NY c) 300 Meridian Centre [REDACTED] 3605 NW 82nd Ave. Miami, FL 33166 [REDACTED] [REDACTED] Backup IT System Infrastructure at Production Data Communications Network & Out-
Business Infrastructure	Information Technology (IT) Infrastructure	<ul style="list-style-type: none"> Voice and data communications Core Business applications

Business and Service Continuity Crown Castle Fiber

Methods and Procedures

TEAMS, CONTACTS, LOGISTICS AND FACILITIES

	Business Locations	<ul style="list-style-type: none">☐ 80 Central St, Boxborough, MA☐ 55 Broad Street, Manhattan☐ 111 8th Avenue, Manhattan☐ 900 Corporate Dr, Newburgh, NY☐ 201 Old Country Rd Melville NY☐ 260 Franklin Street, Boston, MA☐ 505 Eighth Avenue, NYC, NY☐ 120 Lake Ave, Nesconset (LIFE)☐ 350 N. Orleans Suite 600 Chicago, IL☐ 196 Van Buren Drive Herndon, VA☐ 401 North Broad St Philadelphia, PA☐ 581 Main St, Woodbridge NJ☐ 196 Van Buren Street Herndon VA☐ 350 North Orleans Street Chicago IL☐ 300 Meridien Centre Blvd Rochester NY☐ 3605 NW 82nd Ave. Miami, FL 33166☐
		<ul style="list-style-type: none">☐

2. Emergency Response and Restoration Teams

Crown Castle Fiber's Emergency Response/Restoration Teams include both Information Technology and Network/Transport members supporting the East, South, Central and West regions. They support the Event Chairpersons and coordinate both response and restoration activities.

Response

Response Teams are responsible for executing the immediate response procedures of the Business Continuity Plan. Response Teams establish a Response Center, an assembly point, and base of operations for response and recovery efforts.

Restoration

Restoration Teams are responsible for long-term restoration activities and returning to "business as usual." Specifically, the Restoration Teams are responsible for:

- Damage assessment and evaluation
- Establishing the priorities and determining the restoration strategies
- Identifying and procuring resources for the restoration efforts
- Managing recovery time and recovery point objectives

Restoration Teams identify improvements in the disaster avoidance and recovery strategies, based on the recovery experiences. These improvements should be input into the Business and Service Continuity Plan update process to incorporate better understanding of recovery priorities, customer downtime tolerance, and cost.

Crown Castle Fiber personnel are combined into a single, cohesive Emergency Response/Restoration team including representation from the IT and Network-Transport organizations. Depending on the type of emergency, it is expected that the team will include one or more of the following teams:

The Response/Restoration Team draws on organizational and outside resources as needed, including.

- Operations
- IT & Support Systems
- Network & OSP Engineering
- Service Delivery (customer interface)
- Construction
- Sales

Business and Service Continuity Crown Castle Fiber

2.1. Executive Team

The Executive team has the responsibility of directing the activities of the internal organizations, as well as performing external-facing functions. The team provides the disaster declaration and overall direction during the disaster. In addition, the team acts as the spokesperson and press contact.

The Executive Team consists of the company leadership with the following functions:

PRIMARY INDIVIDUAL(S)	FUNCTIONS OF ROLE	BACKUP INDIVIDUAL(S) - IT	BACKUP INDIVIDUAL(S) – NETWORK/TRANSPORT
SVP	<ul style="list-style-type: none"> Declares disaster Responsible for response and recovery strategy decisions Provides liaison between Executive Team and Event Coordinator Backup for CEO functions 	VP of Customer Operations	Director, Network Assurance
VP, Finance	<ul style="list-style-type: none"> Ensures emergency financial management <ul style="list-style-type: none"> Purchases Payroll Provides liaison with insurance carriers 	Director, Assistant Controller	Manager, Treasury

2.2. Event Chairpersons

The Event Chairperson acts as overall coordinator and authority during all emergency response and restoration activities. The Event Chairperson has the authority to activate the Business and Service Continuity Plan, and to identify and assemble the appropriate Response and Restoration teams. The Event Chairperson also leads the assessment process.

The role of Event Chairperson is performed by:

IT PRIMARY & BACKUP INDIVIDUALS	NETWORK/TRANSPORT PRIMARY & BACKUP INDIVIDUALS	FUNCTIONS OF ROLE
VP, IS/IT Director, BSS Development Senior System Admin	VP, Customer Operations GM/VP, Operations, Director, Network Assurance	<ul style="list-style-type: none"> Leads the assessment process Activates the Business and Service Continuity Plan Acts as overall coordinator of activities during entire response and restoration Identifies and assembles the Response and Restoration Teams Backs up the Executive Team

2.3. Emergency Team Chart

IT Emergency Recovery and Restoration Team					
Team	Organization	Responsibilities		Team Leads and Backups	
		Recovery	Restoration	Primary	Secondary
Information Technology	IT Infrastructure and Application Support	Recover interim capabilities for: - IT Infrastructure - OSS/BSS Applications	Restore applications and IT infrastructure to business-as-usual	IT Systems Director CRM Director OSS Development Director	Senior Systems Admin Application Developer Application Developer

Chart continues onto next page

Network - Transport Emergency Recovery and Restoration Team

Org	Responsibilities		Team Leads and Backups			
	Recovery	Restoration	East	Central	South	West

Business and Service Continuity – Crown Castle Fiber

Methods and Procedures

TEAMS, CONTACTS, LOGISTICS AND FACILITIES

Field Ops	Recover interim capabilities for: - Service-providing networks and transport - Node and site services	Restore: - Long-term node and site services - Network capabilities to their normal operations	GM/VP Operations	GM/VP Operations	GM/VP Operations	GM/VP Operations
			Director Field Operations	Mgr, Field Operations	Mgr, Field Operations	Mgr, Field Operations
OSP			Manager Field Operations	Mgr, Field Operations	Field Operations Tech	Field Operations Tech
			GM/VP, Network Operations	GM/VP, Network Operations	SVP, Network Operations	GM/Director
			Dir, Engr. & Construction		Mgr, Fiber Engineering	Mgr, Fiber Eng & Construction

Business and Service Continuity – Crown Castle Fiber

Methods and Procedures

TEAMS, CONTACTS, LOGISTICS AND FACILITIES

			Fiber Engineer –	Mgr Fiber Construction –	Sr Mgr. Fiber Construction	Fiber Engineers	Fiber Eng & Construction
Network Engineering			P: VP, Engineering & Planning P: Sr. Dir, Network Engineering B: Sr. Dir. Network B: Dir. Network Planning				
Equipment Engineering & Facilities			VP Records & Deployment Facilities Manager				

Business and Service Continuity Plan - Crown Castle Fiber

2.4. Event Support Team

The Event Support Team supports the Response Centers during a crisis, surveys for missing or injured employees and notifies authorities and families. The Event Support Teams are also responsible for documenting all events and keeping track of personnel affected during the crisis. Working closely with the Executive Team, it provides the primary point of contact for public and press relations.

Roles and Responsibilities

Role	Responsibilities	Individual
Logistics/Administration	<ul style="list-style-type: none"> • Communicates work-at-home instructions • Coordinates insurance employee claims • Documentation of all activities • Off-site arrangements • Food/Supplies • Generators/Fuel • Petty cash 	Director, Sales Operations
Business Support	<ul style="list-style-type: none"> • Manages treatment and trauma support • Reservations • Grief counseling 	Business Support VP
Communications, Public Relations Coordinator	<ul style="list-style-type: none"> • Creates call in message for employees on the BCP Alert Hotline • Manages public release of information, including press releases & press conferences 	VP, Customer Operations VP – Marketing and Client Services

2.5. Emergency Response/Restoration Team Center

The Emergency Response/Restoration Center is where the Executive Team, Event Chairpersons, and Emergency Teams assemble and operate. The location of the Center is:

Primary	80 Central St, Boxborough, MA
---------	-------------------------------

Business and Service Continuity Plan – Crown Castle Fiber

Methods and Procedures

DETAILED METHODS AND PROCEDURES

Secondary	201 Old Country Rd, Melville NY
Tertiary	300 Meridien Centre Blvd, Rochester NY

Important note:

These locations are the “normal” operational Emergency Centers as designated at the time a disaster is declared. As stated earlier, if a member of the Executive Team is aware of a disaster and is unable to communicate for 4 hours, he or she should report to the nearest available Emergency Center.

2.5.1. Other Emergency Center locations

In the event that primary, secondary tertiary or quaternary locations are not available, a non-Crown Castle Fiber site with the following characteristics will need to be arranged:

- Space for 20 people or about 500 sq. ft.
- Desks available
- High speed Internet access available
- Telephone service with multiple handsets and a speakerphone available
- Television available
- Food services at or nearby
- Nearby transportation: roads or public transportation. If roads: parking nearby
- Nearby hotel or motels
- Toilet facilities at or nearby

2.5.2. Network Operations Centers

Crown Castle Fiber has two staffed NOC locations that have the ability to work in a similar manner. The locations are at 80 Central Street Boxborough, Massachusetts and 201 Old Country Rd Melville NY. If one of these locations is damaged or unable to provide NOC services, then the other locations can cover NOC functions until the damaged location is repaired. In the event that two NOC locations are simultaneously out of service, then Crown Castle Fiber NOC technicians can operate remotely until such time as a suitable location is designated.

2.5.3. Alternate Location Resources

The following table identifies resources that should be available to the Response and Restoration Centers and alternate NOC locations. These resources may have to be obtained at the time of an emergency as part of the Response Procedures.

TYPE	DETAIL
COMPUTER EQUIPMENT	6 Laptops are maintained for emergency use by Crown Castle Fiber IT Printer Copier Fax Video projector
POWER	Power plugs/strips Power backup
TELEPHONE	Telephone service with # handsets

Business and Service Continuity Plan – Crown Castle Fiber

Methods and Procedures

DETAILED METHODS AND PROCEDURES

	Speakerphone/conference unit Cell phone batteries/chargers
TELEVISION/RADIO	TV set w/UHF antenna Cable or satellite connection VCR/DVD AM/FM Radio
DATA COMMUNICATIONS	Data jacks Access to the Crown Castle Fiber Intranet & Crown Castle Fiber applications Internet access Email access
ADMINISTRATIVE	Whiteboard Flip chart Pens Pencils Paper pads
DOCUMENTATION	Business and Service Continuity Plan Company Directory
NOURISHMENT / SUNDRIES / CLOTHING	Basic food items (canned food) Manual can opener Water – 1 gal, per person, per day Paper plates / cups Utility knife First aid kit Flashlights / batteries Water-proof matches Sleeping bags

2.6. Organizational and Location Priorities

If a critical failure impacts multiple Crown Castle Fiber locations and multiple Crown Castle Fiber business processes, the priority for response and restoration priorities and interim recovery time/response objectives are as follows:

Response Time Objectives

RESPONSE PRIORITY	ORGANIZATION	RESPONSE TIME OBJECTIVE (INTERIM OPERATION)
Primary	Information Technology	<1 day
	Operations	<1 day
	NOC	1-2 hours
	Engineering	1-2 days
	Outside Plant/Construction	1-2 days
	Financial (POs)	3-4 days
	Outside Relations	3-4 days
Secondary	Business Support	1-2 days
	Legal	3-4 days

Business and Service Continuity Plan – Crown Castle Fiber

Methods and Procedures

DETAILED METHODS AND PROCEDURES

Tertiary	Sales Marketing Business Development	2 weeks 2 weeks 2 weeks
----------	--	-------------------------------

Business and Service Continuity Plan – Crown Castle Fiber

Methods and Procedures

DETAILED METHODS AND PROCEDURES

	Financial (other)	2 weeks
--	-------------------	---------

Business Process Location Response Priorities

PRIORITY	LOCATION
Primary	80 Central St, Boxborough, MA
Secondary	201 Old Country Rd Melville NY
Tertiary	300 Meridien Centre Blvd Rochester NY
Quaternary	3605 NW 82 nd Ave. Miami, FL 33166

3. Detailed Methods and Procedures

This section contains the detailed procedures for responding to disrupting events and impacts on the service-providing network. The section is organized as follows:


- [General Procedure](#) (Page 19)
The General Response and Restoration Procedure is used as the basis and template for the other procedures.

In some cases, the specific procedure to be followed for a disrupting event or a network impact is the General Response and Restoration Procedure. In such cases, the specific procedure links provided below link to the general procedure.

- [Disrupting Event Procedures](#) (Page 24)
Procedures for responding to specific disrupting events
- [Service-Providing Network Response and Restoration Procedures](#) (Page 50)
Procedures for recovery of service-providing network disasters or disasters affecting network operations and /or IT System Infrastructure
- [Business Process Recovery and Restoration Procedures](#) (Page 61)
Procedures for recovery of business locations, business processes, and Information Technology infrastructure

In some cases, procedures may invoke or reference other procedures. Cross-references are made using hyperlinks.





Procedure Catalog

Category	Procedure
General	General Response and Restoration (Page 19)
Disrupting Events	 <p>Natural Disasters</p> <ul style="list-style-type: none"> A. Snow Storm (Snow Emergency) (Page 25) B. Earthquake – Follow General Response and Restoration (Page 19) C. Flood – Follow General Response and Restoration (Page 19) D. Hurricane – Follow General Response and Restoration (Page 19) E. Tornado – Follow General Response and Restoration (Page 19)
	 <p>Building Infrastructure</p> <ul style="list-style-type: none"> A. Commercial Power Down (Page 26) B. HVAC Down. (Page 29) C. Fire in Structure – Follow General Response and Restoration (Page 19) D. Explosion in Structure – Follow General Response and Restoration (Page 19) E. Gas Leak (Page 31) F. Water Leak (Page 32)

Business and Service Continuity Plan – Crown Castle Fiber

Methods and Procedures

DETAILED METHODS AND PROCEDURES

		<p>System Failures</p> <ul style="list-style-type: none"> A. Voice Communications Down (Page 34) B. Multiple Applications Down (Page 35)
	 	<p>Human/Organizational Problems</p> <ul style="list-style-type: none"> A. Bomb Threat (Page 36) B. Computer Hacker (Page 36) C. Internal Walkout/Strike (Page 38) D. External Walkout/Strike (Page 39) E. Biohazard (Page 40) F. Hostage/Violence in the Building (Page 42) G. Civil Unrest and Localized Riots – Follow General Response and Restoration (Page 19) H. Terrorism and Widespread Attack (Page 43) I. Pandemic (Page 46)
<p style="text-align: center;">Network Recovery & Restoration</p>		<ul style="list-style-type: none"> A. Transfer NOC Function (Page 50) B. Outside Plant Recovery (Page 51) C. Network Node Recovery (Page 53) D. Network Element Recovery (Page 56) E. IT System Infrastructure Recovery (Page 65) F. Network Element Configuration and Restoration (Page 60)

General Response and Restoration Procedure

3.1.1. Immediate Action

- [Evacuate location \(Page 80\)](#) or seek shelter and safety in building
- Notify authorities
- Account for all personnel
- Take steps to [avoid panic](#) (Page 83)
- Identify injuries and provide immediate treatment, if trained personnel available locally
- Initiate normal escalation process
- Notify Event Chairperson
- [Activate NOC Crisis Bridge](#) (Page 84)
- [Transfer NOC Function](#) (if NOC location affected) (Page 50)

3.1.2. Assessment

- Obtain damage reports and building assessment from building management, if applicable
- Determine if disaster should be declared and BCP procedures implemented
- If so, [Initiate notification and callout](#) (Page 9)
- Activate [Emergency Response and Restoration Center](#) locations
- Coordinate and assign initial responsibilities to [Response and Recovery Team](#) (Page 13) members
- Perform assessment of impact to Crown Castle Fiber (use [Damage Assessment Form](#) (Page 89))
 - Widespread, multiple location impact
 - Locations inaccessible
 - Personnel unavailable
 - Equipment and site damaged
 - Network Impact
 - Customer service directly affected
 - Customer service at risk
 - Causes
 - Node failure
 - Network element failure(s)
 - Fiber cut
 - Manhole issues
- Location specific impact
 - 80 Central St, Boxborough, MA
 - NOC Impact
 - Location inaccessible
 - Personnel unavailable
 - Equipment damage
 - OSS failure
 - 201 Old Country Rd Melville NY
 - NOC Impact
 - Location inaccessible

Business and Service Continuity Plan – Crown Castle Fiber

- Personnel unavailable
- Equipment damage
- OSS failure
- 900 Corporate Dr, Newburgh, NY
 - NOC Impact
 - Location inaccessible
 - Personnel unavailable
 - Equipment damage
 - OSS failure
- 300 Meridien Centre Blvd Rochester NY
 - Location inaccessible
 - Personnel unavailable
 - Equipment and site damaged
 - Node site failure (Corporate IT)
- [REDACTED]
 - Location inaccessible
 - Personnel unavailable
 - Equipment and site damaged
 - Node site failure
- [REDACTED]
 - Location inaccessible
 - Personnel unavailable
 - Equipment and site damaged
 - Backup OSS site failure
- 300 Meridien Centre Blvd Rochester NY
 - Location inaccessible
 - Personnel unavailable
 - Equipment and site damaged
- [REDACTED]
 - Location inaccessible
 - Personnel unavailable
 - Equipment and site damaged
- [REDACTED]
 - Location inaccessible
 - Personnel unavailable
 - Equipment and site damaged
- Secure location(s) with barriers, security tape, and guard, if needed. Protect from weather conditions and exposure.
- Videotape, record and/or photograph location and damage for insurance purposes
- Retrieve critical IT items, if undamaged
 - [REDACTED]: Laptop and PCs, Application Servers, and backup tapes
- Turn off power to powered devices
- Determine response and restoration priorities and Recovery Time Objectives
 - For network failures, use established Crown Castle Fiber customer priorities to ensure all Service Level Agreements (SLAs) and [Telecommunications Service Priority \(TSPs\) \(Page 86\)](#) are met.
 - For business process failures, consult [Priorities and Time Objectives \(Page 15\)](#)

3.1.3. Response

- Establish a coverage schedule for the Executive and Response Teams, 24x7 if necessary
- If NOC impacted, [Transfer NOC Function](#) (Page 50)
 - If OSS impacted, initiate OSS recovery procedure provided in the *OSS and BSS Response* section
- If Network impacted, follow appropriate recovery procedure:
 - [OSP Issues](#) (Page 52)
 - Repair fiber cut
 - Bypass fiber cut
 - Reroute fiber
 - [Node Issues](#) (page 50)
 - Repair Node
 - Rebuild Node
 - Bypass Node
 - Deploy Temporary Node
 - Reroute Customers

If work locations (80 Central St , 300 Meridien Centre Blvd Rochester NY, 900 Corporate Dr, , 201 Old Country Rd Melville NY 3605 NW 82nd Ave. Miami, FL 33166

- impacted for less than two weeks, activate [Temporary Work Location](#) (Page 62) procedure
- If work locations impacted for more than two weeks, activate [Medium-Term Site Relocation Procedure \(Page 62\)](#)
- If [REDACTED] backup servers impacted
 - Select secondary site to install temporary servers
 - Activate [IT Response Strategies](#) (p. 63) procedure
- Activate [Emergency Purchase and Cash Advance Procedure \(Page 83\)](#)
- Notify vendors and activate any expedited supply procedures
- Obtain temporary personnel, as needed
- Keep employees informed of status
 - Update corporate message on [BCP Employee Alert Hotline](#) (Page 83)
 - Text Message Broadcast - [IT Management Notification System](#) (Page 84)
- Notify customers as necessary
- Notify press, if appropriate
- Notify insurance carriers
- If network failure affecting New York City service, regional service or requiring outside assistance, notify the Commissioner of the New York City Department of Information Technology and Telecommunications (DoITT) at (212) 788-6600.
 - If required, notification may trigger assistance from other carriers under the Mutual Aid and Restoration Consortium (MARC), every NYC telecommunications carrier is a member.

3.1.4. Restoration

- Verify from building management whether building is safe for occupancy
- Inventory damage for insurance and replacement
 - Work with insurance companies and equipment vendors to determine if any equipment is salvageable
- Coordinate location clean up

Business and Service Continuity Plan – Crown Castle Fiber

Methods and Procedures

DETAILED METHODS AND PROCEDURES

- Replace office furniture
- [Restore Telecommunications \(Page 63\)](#)
- [Restore IT Systems Infrastructure](#) (Page 65)
- Re-supply location(s) with office supplies and equipment
- Notify employees when safe to return to building
 - Update BCP [Alert Hotline \(Page 83\)](#)
- Arrange for appropriate post trauma counseling, as necessary
- Restore normal functions of location
- Secure insurance claim payment(s)
- Perform post-mortem

3.2. Disrupting Event Procedures

Natural Disasters
A. Snow Storm (Snow Emergency) (Page 25)
B. Earthquake – Follow General Response and Restoration (Page 19)
C. Flood – Follow General Response and Restoration (Page 19)
D. Hurricane – Follow General Response and Restoration (Page 19)
E. Tornado – Follow General Response and Restoration (Page 19)
Building Infrastructure Failures
A. Commercial Power Down (Page 26)
B. HVAC Down (29)
C. Fire in Structure – Follow General Response and Restoration (Page 19)
D. Explosion in Structure – Follow General Response and Restoration (Page 19)
E. Gas Leak (Page 31)
F. Water Leak (Page 32)
System Failures
A. Voice Communications Down (Page 34)
B. Multiple Applications Down (Page 35)
Human/Organizational Problems
A. Bomb Threat (Page 36)
B. Computer Hacker (Page 36)
C. Internal Walkout/Strike (Page 38)
D. External Walkout/Strike (Page 39)
E. Biohazard (Page 40)
F. Hostage/Violence in the Building (Page 42)
G. Civil Unrest and Localized Riots – Follow General Response and Restoration (Page 19)
H. Terrorism and Widespread Attack (Page 43)
I. Pandemic (Page 49)

3.2.1. Snow Storm Response and Restoration Procedure

I. Immediate Action

- Initiate normal escalation process
- Notify Event Chairperson
- [Activate NOC Crisis Bridge\(Page 84\)](#)

II. Assessment

- Confirm severity of storm
- Determine whether significant accumulation (> 2 ft.) has occurred or is pending
- Determine whether building or office closure will occur
- Perform assessment of business impact
 - Network services support at risk
 - Location(s) inaccessible
 - Personnel unavailable
 - Normal business functions at risk
 - Location(s) inaccessible
 - Personnel unavailable

III. Response

- If NOC facility impacted, [Transfer NOC Function\(Page 50\)](#) (to alternate facility if more accessible)
- Notify employees of closure
 - Voice Mail/Email
- Update information on [Employee Alert Hotline](#) (Page 83)
- Reserve local hotel space for critical employees
- For NOC, create NOC coverage schedule
 - At NOC location – use people stranded by storm; provide rotation
- For all work locations
 - Activate [Temporary Work Location\(Page 62\)](#) procedure

IV. Restoration

- Coordinate accessibility with building and/or city officials
- Notify employees when to return to building

3.2.2. Commercial Power Down Response and Restoration Procedure



I. Immediate Action

- Initiate normal escalation process
- Notify Event Chairperson
- [Transfer NOC Function \(Page 50\)](#) (if NOC location affected)
- [Activate NOC Crisis Bridge \(Page 84\)](#)

II. Assessment

- Confirm outage with the power company
- Calculate backup capacity available at location (number of hours)
- Estimate duration of the outage
- Reserve availability of additional backup capacity
 - Additional batteries
 - Mobile generator
- Determine if disaster should be declared and BCP procedures implemented
- [Initiate notification and callout \(Page 9\)](#)
- Activate [Emergency Response and Restoration Center \(Page 13\)](#) locations
- Coordinate and assign initial responsibilities to [Response and Recovery Team \(Page 7\)](#) members
- Perform assessment of immediate or potential impact (use [Damage Assessment Form \(Page 89\)](#))
 - Widespread impact/multiple location failure
 - NOC Impact
 - Location inaccessibility
 - Personnel availability
 - IT Infrastructure Impact
 - Network Impact
 - Node failure
 - Network element failure(s)
 - Location specific failure
 - 80 Central St, Boxborough, MA
 - [REDACTED]
 - 55 Broad St., NYC
 - 900 Corporate Dr, Newburgh, NY
 - 201 Old Country Rd Melville NY
 - [REDACTED]

II. Response

- If NOC impacted, [Transfer NOC Function \(Page 50\)](#)
 - If IT Infrastructure is impacted, initiate [IT System Infrastructure recovery \(Page 65\)](#) procedures
- If network impacted:
 - Install additional batteries or activate backup generator, as needed
 - Turn off non-critical equipment
 - Follow appropriate response procedure:
 - [Node Issues \(Page 53\)](#)
 - Bypass node

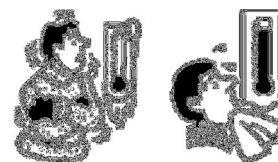
- Deploy temporary node
- Reroute customers
- If backup power is drained, turn equipment off.
- Contact Service Delivery Director to notify customers as a courtesy
- If work locations impacted
 - Power down non-critical equipment to reduce drain on battery backups. The following equipment should remain on battery backup
 - LAN Switches
 - File Servers
 - Domain Controller
 - Bring in additional batteries as a precaution.
 - If batteries drained, turn equipment off.
- Activate [Temporary Work Location\(Page 62\)](#) procedure
- Relocate non-critical servers to a backup location
- Keep employees informed of status, [BCP Employee Alert Hotline\(Page 83\)](#)

IV. Restoration

- Verify commercial power is restored with the power company
- Power up equipment and check functionality
- Once all network functions are confirmed up, restore phones and NOC functionality back to primary NOC and confirm they are working correctly
- Restore other phones and communications reroutes
- Notify employees that locations are back in service
- For service affecting failures, notify customers of service recovery
- Perform Internal Post Mortem
 - Schedule a Major Outage Critique with team
 - Deliver Internal Outage Report within 72 hours
- Perform External Post Mortem with utility(s)
- For service affecting failure, deliver Outage Report to Customers within 96 hours
- Secure Service Credits from Utility

3.2.3. HVAC Down

Response and Restoration Procedure



I. Immediate Action

- Initiate normal escalation process
- Notify Event Chairperson
- [Transfer NOC Function](#) (Page 50)(if NOC location affected)
- [Activate NOC Crisis Bridge](#) (Page 84)
- Identify if this site is at a [Crown Castle Fiber Core Equipment Site](#) (Page 5)

II. Assessment

- Determine whether extreme weather conditions are occurring
- Determine whether building closure required
- Calculate backup cooling capacity (number of hours)
- Estimate duration of the outage
- Estimate equipment power dissipation at location and expected temperature rise.
- Reserve availability of mobile cooling unit for additional backup

Business and Service Continuity Plan – Crown Castle Fiber

Methods and Procedures

DETAILED METHODS AND PROCEDURES

- Determine if disaster should be declared and BCP procedures implemented
- [Initiate notification and callout](#) (Page 9)
- Coordinate personnel to implement recovery and/or restoration procedures
- Perform assessment of immediate or potential impact to Crown Castle Fiber
 - NOC Impact
 - Location inaccessibility
 - Personnel availability
 - IT Infrastructure Impact
 - Network Impact
 - Node failure
 - Network element failure(s)
 - Location specific failure at one of Crown Castle Fiber's [Business Locations \(Page 6\)](#)

III. Response

- If NOC impacted, [Transfer NOC Function](#) (Page 50)
 - If OSS impacted, initiate [IT Infrastructure Restoration Process](#) (Page 66)
- Obtain and activate mobile cooling unit, if available
- If emergency cooling not available
 - If Network impacted or at risk, follow appropriate recovery procedure:
 - [Node Issues \(Page 55\)](#)
 - Bypass node
 - Deploy temporary node
 - Reroute customers
- If temperature is rising to or expected to exceed 100° F (38° C), power down electronic equipment sequentially and observe effect on temperature. Power down the least critical systems first.
- At 80 Central St. Boxboro, 111 8th Avenue, and 900 Corporate Dr, Newburgh, NY locations, power down equipment ONLY after NOC functions have transferred to another NOC location, or to Virtual NOC operations.
- Coordinate repair with Building Management
- Activate [Temporary Work Location \(Page 62\)](#) procedure

IV. Restoration

- Verify HVAC is restored and acceptable temperature is reached
- Power up equipment and check functionality
- Once all network functions are confirmed up, transfer phones and NOC functionality back to primary NOC and confirm they are working correctly
- Notify Crown Castle Fiber personnel and customers that NOC and/or node are back in service
- Notify employees of when to return to building
- Perform Internal post mortem
 - Schedule a major outage critique with team
 - Deliver internal outage report within 72 hours
- Perform external post mortem with provider(s)
- Deliver outage report to customers within 96 hours

3.2.4. Gas Leak

Response and Restoration Procedure



I. Immediate Action

- [Evacuate location](#) (Page 80)
- Notify authorities
- Account for all personnel
- Identify injuries and provide immediate treatment, if trained personnel available
- Initiate normal escalation process
- Notify Event Chairperson
- [Transfer NOC Function](#) (if NOC location affected) (Page 50)
- [Activate NOC Crisis Bridge](#) (Page 84)

II. Assessment

- Obtain building assessment from building management
- Determine if disaster should be declared and BCP procedures implemented
- [Initiate notification and callout \(Page 9\)](#)
- Coordinate personnel to implement recovery and/or restoration procedures
- Perform assessment of impact to Crown Castle Fiber
 - NOC Impact
 - Location inaccessibility
 - Personnel availability
 - IT Infrastructure Impact
 - Network Impact
 - Node failure
 - Network element failure(s)
 - Location impact at [Key Business Locations \(Page 6\)](#)

III. Response

- If NOC facility, [Transfer NOC Function](#) (Page 50) to alternate facility
 - If OSS impacted, initiate OSS recovery procedure according to the IT Systems Continuity Strategy section
- If Network impacted, follow appropriate recovery procedure:
 - [Node Issues](#) (Page 53)
 - Bypass Node
 - Deploy Temporary Node
 - Reroute Customers
- Activate [Temporary Work Location](#) (Page 62) procedure
- Notify vendors and activate any expedited supply procedures
- Keep employees informed of status, BCP Employee Alert Hotline
- Notify, if necessary
 - Customers
 - Press
 - Insurance Carriers
 - Commissioner of the New York City Department of Information Technology and Telecommunications (DoITT) at (212) 788-6600.
 - If required, notification may trigger assistance from other carriers under the Mutual Aid and Restoration Consortium (MARC)

IV. Restoration

- Reoccupy premises once the local utility and Fire Dept have cleared the building
- Verify all network elements and systems are working and synchronized

- Notify employees when safe to return to building
- Restore functions of location, e.g., NOC and/or Network Node
- Perform post-mortem on incident

3.2.5. Water Leak Response and Restoration Procedure



I. Immediate Action

- [Evacuate location](#) (Page 80) (if necessary)
- Initiate normal escalation process
- Notify Event Chairperson
- [Transfer NOC Function](#) (Page 50) (if NOC location affected)
- [Activate NOC Crisis Bridge](#) (Page 84)

II. Assessment

- Obtain damage reports and building assessment from building management, if applicable
- Determine if disaster should be declared and BCP procedures implemented
- [Initiate notification and callout](#) (Page 9)
- Coordinate personnel to implement recovery and/or restoration procedures
- Perform assessment of impact to Crown Castle Fiber
 - NOC Impact
 - Location inaccessible
 - Equipment damage
 - IT Infrastructure Impact
 - Network Impact
 - Node failure
 - Network element failure(s)
 - Location impact at [Key Business Locations \(Page 6\)](#)
- Videotape and/or photograph site for record

III. Response

- If NOC impacted, [Transfer NOC Function](#) (Page 50)
 - If IT Infrastructure is impacted, initiate IT Systems Infrastructure recovery procedure
- If Network impacted, follow appropriate recovery procedure:
 - [Node Issues](#) (Page 53)
 - Repair node
 - Rebuild node
 - Bypass node
 - Deploy temporary node
 - Reroute customers
- If IT infrastructure is impacted, [Initiate IT Systems Continuity Strategy](#) (Page 66)
- Activate [Temporary Work Location \(Page 62\)](#) procedure

IV. Restoration

- Verify building safety
- Reoccupy premises once the local utility and Fire Department have cleared the building.

- Obtain assistance of cleanup vendor or janitorial service
- Contact the insurance carriers
- Assess overall damage to area.
- Assess losses of equipment (printers, photocopiers, cubicles, windows, doors, etc.).
- Assess losses on all network and computer equipment (laptops, desktops and lab equipment).
 - Work with insurance companies and equipment vendors to determine if any equipment is salvageable
- Verify all systems working and synchronized
- Notify employees when safe to return to building
- Restore functions of location, e.g., NOC and/or NetworkNode
- Secure Insurance Claim Payments

3.2.6. Voice Communications Down Response and Restoration Procedure



I. Immediate Action

- Initiate normal escalation process (via email, as required)
- Notify Event Chairperson (via email, as required)

II. Assessment

- Determine cause of failure
- Determine expected duration of outage

III. Response

- Initiate incoming line forwarding service as required (see [IS-003 Corporate Toll Free Number Move Process document](#) (Page 85))
- Activate alternate communications methods – email, instant messaging, Internet voice, collaboration software, radio devices/ walkie-talkies, mobile phones (if available)
- Contact voice service vendors

IV. Restoration

- Follow normal [IT Systems Continuity Strategy \(Page 65\)](#) procedures
- Verify voice network is operational
 - Initiate LD, Local, In Building Calls
- Discontinue incoming line forwarding service as required (see [IS-003 Corporate Toll Free Number Move Process document](#))
- Send an event notification to employees to notify problem is corrected
- Notify any customer or vendors of restoration
- Perform Internal post mortem
 - Schedule a major outage critique with team

- Deliver internal outage report within 72 hours
- Perform external post-mortem with provider(s)
- Deliver outage report to customers within 96 hours
- Secure service credits from service providers, if appropriate

3.2.7. Multiple Applications Down Response and Restoration Procedure

Please refer to the [IT Trouble Management procedures](#) (Page 67)



Bomb Threat Response and Restoration Procedure

I. Immediate Action

- ☐ While caller is on the telephone log specifics of threat
 - Time call was received
 - Time call was terminated
 - Exact words of caller, as possible
 - Time the bomb is threatened to explode
 - Any special instructions by the caller
- ☐ Call 911
- ☐ [Evacuate location](#) or follow instructions of authorities
- ☐ Account for all personnel
- ☐ Initiate normal escalation process
- ☐ Notify Event Chairperson
- ☐ [Transfer NOC Function](#) (if NOC location affected)
- ☐ [Activate NOC Crisis Bridge](#) Notify Building Manager



II. Assessment

- ☐ Determine if disaster should be declared and BCP procedures implemented
- ☐ [Initiate notification and callout](#) (Page 80)
- ☐ Coordinate personnel to implement recovery and/or restoration procedures
- ☐ Perform assessment of impact
 - Location inaccessible
 - Personnel unavailability
- ☐ Determine duration of outage

III. Response

- ☐ If NOC impacted, [Transfer NOC Function](#) (Page 50)
- ☐ Activate [Temporary Work Location](#) (Page 62) procedure
- ☐ Keep employees informed of status, [BCP Employee Alert Hotline](#) (Page 62)
- ☐ Notify customers as necessary
- ☐ Notify press, if appropriate

IV. Restoration

- ☐ Return to building only upon instruction from authorities that it is safe
- ☐ Restore functions of location, e.g., NOC and/or Network Node

- ☒ Inform all employees, customers, and public as necessary
- ☒ Arrange for appropriate post trauma counseling as necessary
- ☒ Perform internal post mortem with business continuity and safety team
- ☒ Perform external post mortem with authorities

3.2.8. Computer Hacker Response and Restoration Procedure



I. Immediate Action

- Use normal escalation process
- Identify & Confirm Attack
 - Types of attacks:
 - Denial of Service (DoS),
 - Information theft,
 - Defacement,
 - File damage or theft
- Sever all connections outside of the internal network
- Notify Event Chairperson
- [Activate NOC Crisis Bridge \(Page 84\)](#)
- Notify Police or FBI of intrusion

II. Assessment

- Determine if disaster should be declared and BCP procedures implemented
- [Initiate notification and callout \(Page 66\)](#)
- Coordinate personnel to implement recovery and/or restoration procedures
- Obtain services of security consulting vendor, if necessary
- Perform assessment of impact
 - NOC Impact
 - OSS failure
 - Network Impact
 - Network element failure(s)
 - IT Infrastructure impact
 - Applications
 - Servers
 - IT services

III. Response

- Tighten server security (limit ports, limit access to files)
- Isolate attacked system(s) for digital forensics
- Secure snapshot of system log(s) (Audit Trail)
- If applications impacted, initiate Application Recovery provided in [IT Systems Continuity Strategy \(Page 65\)](#) section
- If Network impacted, follow appropriate recovery procedure:
 - [Network Element Issues \(Page 56\)](#)
 - Replace element
 - Rebuild element
 - Bypass element
 - Reroute customers

IV. Restoration

- Verify that the incident is resolved and security is reinstated.
- Reload all applications
- Sanitize the affected system(s) and restore them to a known good state or
- Rebuild the machine from initial installation via an installation procedure and restore the machine via tape backup etc.
- Perform internal post-mortem
 - Schedule a major outage critique with team
 - Deliver internal outage report within 72 hours
- Update all security features on Operating Systems and Applications
- Perform external post mortem with customer(s)
- Deliver outage report to customers within 96 hours
- Identify individual(s) responsible for damages (Internal vs. External)
 - Internal – terminate employment and press charges
 - External – press charges

3.2.9. Internal Walkout/Strike Response and Restoration Procedure



I. Immediate Action

- Identify affected personnel and locations
- Initiate normal escalation process
- Notify Event Chairperson
- [Activate NOC Crisis Bridge \(Page 84\)](#)
- Notify authorities

II. Assessment

- Determine scope of the potential interruption on services
- Determine whether to initiate the BCP
- [Initiate notification and callout](#) (Page 66)
- Perform assessment of impact
 - Location inaccessible
 - Personnel unavailability
- Determine coverage needs

III. Response

- Identify and assign available resources to handle the disrupted tasks and responsibilities
- Hire temporary personnel and/or assign others to critical functions, as needed
- If NOC affected,
 - [Transfer NOC Function \(Page 50\)](#) (if necessary)
 - Create NOC coverage schedule
- Activate [Temporary Work Location \(Page 62\)](#) procedure
- Change all system passwords and card access
- Disable remote access for all individuals involved in walkout

IV. Restoration

- Restore service and operations
- Notify customer and public of full service restoration
- Perform internal post mortem

3.2.10. External Strike/Walkout
Response and Restoration Procedure



I. Immediate Action

- Initiate normal escalation process
- Notify Event Chairperson
- [Activate NOC Crisis Bridge](#) (Page 84)

II. Assessment

- Determine duration and scope of potential interruption
 - If strike is of public employees, such as transportation, obtain information from news on city, state and federal plans
 - If strike is of vendors, obtain information on vendor strike plans
- Determine whether to initial the BCP
- Perform assessment of business impact
 - Network services support at risk
 - Location(s) inaccessible
 - Personnel unavailable
 - Normal business functions at risk
 - Location(s) inaccessible
 - Personnel unavailable

III. Response

- Establish call-in number with voice message on status
- Identify critical employees needed on-site
- Reserve local hotel space for critical employees with restricted travel
- If NOC affected,
 - [Transfer NOC Function \(Page 50\)](#) if secondary site more suitable or accessible
 - At normal NOC location – use people stranded by storm; provide rotation
 - At backup NOC location – use backup NOC personnel available locally
- Activate [Temporary Work Location](#) (Page 62) procedure, if required
- Locate alternative vendors for needed services and/or equipment
- Activate appropriate procedure for lost services, such as [Voice Communications Down](#) (Page 34)

IV. Restoration

- Coordinate accessibility with building and/or City officials
- Notify employees when to return to building

3.2.11. Biohazard
Response and Restoration Procedure



I. Immediate Action

- [Evacuate location \(Page 80\)](#) or seek shelter and safety in building
- Account for all personnel
- Identify injuries and, if trained personnel available locally, provide immediate treatment
- Initiate normal escalation process
- Notify Event Chairperson
- [Transfer NOC Function](#) (Page 50)(if NOC location affected)
- [Activate NOC Crisis Bridge](#) (Page 84)
- Notify City, State and Federal authorities if necessary
- Notify Building Manager

II. Assessment

- Determine if disaster should be declared and BCP procedures implemented
- [Initiate notification and callout](#) (Page 66)
- Coordinate personnel to implement recovery and/or restoration procedures
- Perform assessment of impact
 - Location inaccessible
 - Personnel unavailability

III. Response

- If NOC impacted, [Transfer NOC Function](#) (Page 50)
- Activate [Temporary Work Location](#) (Page 62)
- Keep employees informed of status, [BCP Employee Alert Hotline](#) (Page 83)
- Notify customers as necessary
- Notify press, if appropriate
- Notify insurance companies

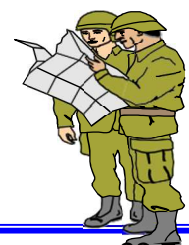
IV. Restoration

- Return to building only upon instruction from authorities that it is safe
- Restore service and operations
- Inform employees, customers, and public as necessary
- Arrange for appropriate post trauma counseling as necessary
- Perform internal post mortem with business continuity and safety team
- Perform external post mortem with authorities

3.2.12. Hostage/Violence in Building
Response and Restoration Procedure

I. Immediate Action

- Follow instructions of hostage taker or law enforcement representatives
- If possible:
 - Call 911



- [Evacuate location](#) (Page 80)
- Account for all personnel
- Identify injuries and provide immediate treatment, if trained personnel available locally
- Initiate normal escalation process
- Notify Event Chairperson
- [Transfer NOC Function](#) (Page 50) (if NOC location affected)
- [Activate NOC Crisis Bridge](#)(Page 84)

II. Assessment

- Determine if disaster should be declared and BCP procedures implemented
- [Initiate notification and callout](#) (Page 66)
- Coordinate personnel to implement recovery and/or restoration procedures
- Perform assessment of impact
 - Location and NOC Impact
 - Location inaccessibility
 - Personnel unavailability
 - Equipment damage
 - OSS failure
 - Network Impact
 - Node failure
 - Network element failure(s)
 - Fiber cut
 - Manhole issues

III. Response

- If NOC impacted, [Transfer NOC Function](#) (Page 50)
 - If OSS impacted, initiate OSS recovery procedure provided in [IT Systems Continuity Strategy](#) (Page 65) section
- If Network impacted, follow appropriate response:
 - [OSP Issues](#) (Page 52)
 - Repair fiber cut
 - Bypass fiber cut
 - Reroute fiber
 - [Node Issues](#) (Page 55)
 - Repair node
 - Rebuild node
 - Bypass node
 - Deploy temporary node
 - Reroute customers
- If business locations impacted, activate [Temporary Work Location](#)(Page 62) procedure
- Activate [Emergency Purchase Order and cash advance](#)(Page 83) procedures
- Notify vendors and activate any expedited supply procedures
- Keep employees informed of status, [BCP Employee Alert Hotline](#)(Page 83)
- Notify customers as necessary
- Notify press, if appropriate
- Notify insurance companies

IV. Restoration

- Return to building only upon instruction from authorities that it is safe
- Restore service and operations

- Inform and communicate to all Crown Castle Fiber employees, customers, and public as necessary
- Arrange for appropriate post trauma counseling as necessary
- Perform internal post mortem with business continuity and safety team
- Perform external post mortem with authorities

3.2.13. Terrorism and Widespread Attack Response and Restoration Procedure

I. Immediate Action

- ☐ Follow instructions of law enforcement representatives or emergency management personnel
- ☐ [Evacuate location \(Page 80\)](#) if possible
- ☐ Account for all personnel
- ☐ Identify injuries and, if trained personnel available locally, provide immediate treatment
- ☐ Initiate normal escalation process
- ☐ Notify Event Chairperson

II. Assessment

- ☐ Determine if disaster should be declared and BCP procedures implemented
- ☐ [Activate NOC Crisis Bridge \(Page 84\)](#)
- ☐ Identify Emergency Response Centers in an accessible area outside of affected region
- ☐ [Initiate notification and callout \(Page 66\)](#)
- ☐ Coordinate personnel to implement recovery and/or restoration procedures
- ☐ Perform preliminary assessment of impact
 - NOC impact
 - Network impact
 - Location impact
- ☐ Request additional information from the DoITT (NYC) at (212) 788-6600.

III. Response

- ☐ Dispatch teams to the temporary Emergency Response Centers to survey the location and determine the requirements for functional operation
- ☐ Activate [Emergency Purchase Order and cash advance \(Page 83\)](#) procedures
- ☐ Notify vendors and activate any expedited supply procedures
- ☐ Set up a call-in telephone number and instruct employees to
 - Stand by for further instructions and
 - Use personal email and cell phones for all communication until other communications resources are available
- ☐ Dispatch available IT personnel immediately to the temporary Emergency Response Center location
- Acquire office equipment – phones, PCs, laptops, servers, printers, copiers and fax – for the Emergency Response Center location
- ☐ Order communications facilities on an expedited basis
 - Order POTS lines for initial voice communication and fax capabilities
 - Order voice service with the DID of the affected location mapped to the temporary location
 - Order Internet access for the temporary location – DSL is a viable short-term alternative
- ☐ Install and configure voice capabilities
- ☐ Configure the phone systems to route incoming calls to handsets or cell phones
- ☐ Install and configure the LAN network infrastructure
- ☐ Enable connectivity between the PCs and servers
- ☐ Configure and install Exchange server and local file server

Business and Service Continuity Plan – Crown Castle Fiber

Methods and Procedures

DETAILED METHODS AND PROCEDURES

- Obtain backup tapes for Exchange server and local file servers if available
- ☒ Configure WAN connectivity
- ☒ Arrange to have mail and package deliveries forwarded to new location
- Procure temporary furniture – e.g., tables and chairs
- ☒ Procure office supplies
- ☒ Obtain a TV with cable and/or satellite feed to monitor news and events
- Order Emergency Supplies – replenish periodically as necessary
- ☒ Initiate OSS response provided in [IT Systems Continuity Strategy \(Page 65\)](#) section
- ☒ [Transfer NOC Function \(Page 50\)](#) to the Emergency Response Centers
- ☒ Report progress to external emergency management organizations
- ☒ Once location is operational, perform more detailed impact assessment for the network
 - Locations and NOC impact
 - Location inaccessibility
 - Personnel availability
 - Equipment damage
 - OSS failure
 - Network impact
 - Node failure
 - Network element failure(s)
 - Fiber cut
 - Manhole issues
- ☒ Determine access restriction to affected areas
 - Coordinate with external emergency management organizations for access to affected areas
- ☒ If Network impacted and locations are accessible, follow appropriate recovery procedure:
 - [OSP Issues \(Page 51\)](#)
 - Repair fiber cut
 - Bypass fiber cut
 - Reroute fiber
 - [Node Issues \(Page 55\)](#)
 - Repair node
 - Rebuild node
 - Bypass node
 - Deploy temporary node
 - Reroute customers
 - [Medium-Term Site Relocation \(Page 62\)](#)
- ☒ Videotape and record damage, if possible
- ☒ Keep employees informed of status, BCP Employee Alert Hotline
- ☒ Notify customers as necessary
- ☒ Notify press, if appropriate
- ☒ Notify insurance companies
- ☒ Request assistance from DoITT (NYC) and MARC at (212) 788-6600, as needed

IV. Restoration

- ☒ Return to building only upon instruction from authorities that it is safe
- ☒ Restore service and operations
- ☒ Inform and communicate to all Crown Castle Fiber employees, customers, and public as necessary
- ☒ Arrange for appropriate post trauma counseling as necessary
- ☒ Perform internal post mortem
- ☒ Perform external post mortem with authorities
- ☒ Work with insurance carriers to evaluate and make claims

3.3. Pandemic Planning



3.3.1. Planning and Response Goals

The goal of pandemic planning is to reduce transmission of the pandemic virus strain, to decrease illness amongst staff, to maintain mission critical business activities and customer service, and to reduce the economic impact of a pandemic.

Crown Castle Fiber's strategy and response to pandemic outbreaks will be based on local information from local and state public health authorities. Pandemic may refer to influenza or other contagious infections/diseases. Some of the key indicators that should be used when making decisions on appropriate responses are:

- ☐ Disease severity (i.e., hospitalization and death rates) in the community where business is located;
- ☐ Extent of disease (number of people who are sick) in the community;
- ☐ Amount of worker absenteeism;
- ☐ Impact of disease on workforce populations that are vulnerable and at higher risk (e.g., pregnant women, employees with certain chronic medical conditions that put them at increased risk for complications of influenza); and
- Factors that may affect employees' ability to get to work, such as school dismissals or closures due to high levels of illness in children or school dismissals.

3.3.2. Assumptions

- ☐ A pandemic may come and go in waves lasting from 6 to 8 weeks over a 4 to 9 month period.
- ☐ Workplace absentee rates could be as high as 25% over a 4 to 9 month period.
- ☐ The traditional workplace cannot be maintained during a pandemic without putting management and staff at increased risk of infection. To achieve maximum effectiveness, workplace closure should be initiated prior to the onset of widespread pandemic illness.
- ☐ Anticipate employee fear and anxiety, rumors and misinformation.
- ☐ It is possible that Crown Castle Fiber locations may be compelled to close by local, state, or federal health authorities regardless of its desire to remain open.
- ☐ Some employees may not be able to return home due to worsening conditions prevailing in their home or community.

3.3.3. Advanced Pandemic Preparedness Recommendations

Business and Service Continuity Plan – Crown Castle Fiber

Methods and Procedures

DETAILED METHODS AND PROCEDURES

Crown Castle Fiber's physical network should not be affected by a pandemic; however, company business will be impacted by human elements (absences, dispatch delays, supplier availability).

- ☐ Identify essential employees and other critical inputs (e.g. suppliers, sub-contractor services/products, spares, and logistics) required to maintain business operations by location and function during a pandemic.
- ☐ Forecast and allow for employee absences during a pandemic due to factors such as personal illness, family member illness, community containment measures and quarantines, school and/or business closures, and public transportation closures.
- ☐ Verify qualifications and availability of ancillary workforce (e.g. contractors, employees in other job titles/descriptions, retirees).
- ☐ Provide sufficient and accessible infection control supplies (e.g. hand-hygiene products, tissues and receptacles for their disposal) in all business locations.
- Enhance communications and information technology infrastructures as needed to support employee telecommuting and remote customer access. Crown Castle Fiber can accommodate 100 VPN users and 40 Citrix users for remote access to corporate system resources. If virtual access during an event isn't adequate then BC Chairperson will decide on what organizations get priority.
- ☐ Limit the frequency and type of face-to-face contact (e.g. hand-shaking, seating in meetings, office layout, shared workstations) among employees and between employees and customers.
- Encourage and track annual influenza vaccination for employees.
- ☐ Ensure availability of medical consultation and advice for emergency response.
 - Evaluate employee access to and availability of healthcare, mental health, and social services during a pandemic, including corporate, community, and faith-based resources, and improve services as needed.
- ☐ Identify employees and key customers with special needs, and incorporate the requirements of such persons into the preparedness plan.
- ☐ Collaborate with insurers, health plans, and major local healthcare facilities to share Crown Castle Fiber pandemic plans and understand their capabilities and plans.
- ☐ Collaborate with federal, state, and local public health agencies and/or emergency responders to participate in their planning processes, share Crown Castle Fiber pandemic plans, and understand their capabilities and plans.
- ☐ Communicate with local and/or state public health agencies and/or emergency responders about the assets and/or services Crown Castle Fiber could contribute to the community.
- ☐ Share best practices with other businesses in Crown Castle Fiber communities, chambers of commerce, and associations to improve community response efforts.
- ☐ Implement an exercise/drill to test your plan, and revise periodically.

3.4. Pandemic Response Procedures

3.4.1. Pandemic Response

- ☒ Locate up-to-date, reliable pandemic information from community public health, emergency management.
 - Local authorities
 - TV/Radio
 - World Health Organization (WHO), Center For Disease Control (CDC)
- ☒ Perform impact assessment
 - Location inaccessible
 - Personnel unavailability
- ☒ Determine if disaster should be declared and BCP procedures implemented
- ☒ Implement the established emergency communications plan, including chain of communications and processes for tracking and communicating business and employee status.
 - Initiate notification process and conference capabilities (Emergency announcement, BCP [Employee Alert Hotline \(Page 83\)](#), dedicated website)
 - Notify Event Chairpersons, State and Local Public Health partners, insurance company, and building management (Notify customers as necessary)
 - Communicate pandemic status and actions to employees, vendors, and suppliers inside and outside the worksite in a consistent and timely way
- ☒ Contact resources for obtaining counter-measures (e.g. vaccines and antivirals).
- Activate policy for flexible worksite (e.g. telecommuting) and flexible work hours (e.g. staggered shifts).
- ☒ Implement policies for employee compensation and sick-leave absences unique to a pandemic (e.g. non-punitive, liberal leave), including policies on when a previously ill person is no longer infectious and can return to work after illness.
- ☒ Keep sick workers home
 - Employees who have been exposed to pandemic influenza, are suspected to be ill, or become ill at the worksite are subject to immediate mandatory sick leave or work at home status.
- ☒ Evacuate employees working in or near an affected area when an outbreak begins, and provide guidance for employees returning from affected areas. (Dependent on specific pandemic and declared phase of outbreak)
- ☒ Business-related travel will be frozen
- ☒ Consider activating altering business operations (e.g. shutting down operations in affected areas), and transferring business knowledge to key employees.

3.4.2. Post-Pandemic Response

- ☒ Return to building(s) only upon instruction from authorities that it is safe
- ☒ Restore service and operations ([Refer to IT Systems Business Continuity Strategy \(p.65\), if required](#))

- ☐ Inform employees, customers, and public as necessary
- ☐ Arrange for appropriate post trauma counseling as necessary
- ☐ Perform internal post mortem with business continuity and safety team
- ☐ Perform external post mortem with authorities

3.5. Service-Providing Network Response and Restoration Procedures

These procedures and sub-procedures cover recovery and restoration for failures of the service-providing network and the supporting infrastructure.

- A. [Transfer NOC Function \(Page 50\)](#)
- B. [Outside Plant Recovery \(Page 51\)](#)
- C. [Network Node Recovery \(Page 53\)](#)
- D. [Network Element Recovery \(Page 56\)](#)
- E. [Network Element Configuration and Restoring \(\(Page 60\)](#)

Transfer NOC Function

Response and Restoration Procedure

Crown Castle Fiber has two staffed NOC locations that work in parallel with each other, 80 Central St, Boxborough, MA and 201 Old Country Rd Melville NY. If one of these locations is damaged or unable to provide NOC services then the other location covers the NOC function until the damaged location is repaired. In the event that both NOC locations are simultaneously out of service, then Crown Castle Fiber NOC technicians can operate out of 55 Broad St, NYC, 300 Corp Blvd, Newburgh, or in a remote environment.

I. Response

- NOC Director or Manager assesses NOC personnel requirements and creates emergency coverage schedule.
- NOC Director or Manager to test NOC 800 number routing to ensure Crown Castle Fiber customer trouble reporting is being captured.
- Configure phones, PC's, laptops and client software applications to function in virtual environment. (If Necessary)
- If virtual connections for NOC personnel cannot be established to the IT Infrastructure initiate the [IT System Infrastructure Response Procedures \(Page 65\)](#) Notify the rest of the company that the BCP plan has been engaged and to call their management and the [Business Continuity Alert number \(Page 83\)](#) for updates.

II. Restoration

- Inventory damage for insurance and replacement
- Follow up with Insurance Company
- Replace damaged Crown Castle Fiber equipment and furniture
- Notify employees when safe to return to building
- Restore functions of location, e.g., NOC and/or Network Node
- Secure insurance claim payment(s)
- Investigate methods and/or design to reduce future service impacts

- Inform employees, customers, and public as necessary
- Perform internal post mortem
- Perform external post mortem with vendor and/or parties responsible for the outage
- Communicate results of post mortem with customers
- Take appropriate steps to alleviate future service disruptions

3.5.1. Outside Plant Recovery and Restoration

This section covers the recovery and restoration in the event of an Outside Plant (OSP) failure. The OSP failures include any major damage to fibers and/or splices, including fiber cuts, manhole explosions and riser damage.

The following recovery strategies are addressed:

- Repair damaged fiber
- Bypass damaged fiber
- Reroute or re-terminate the damaged fiber

Each recovery strategy ranges in the time required for recovery, as well as the coordination of resources and information. The following procedure assumes the failure has been detected by the NOC, isolated to an area of impact. The NOC should also be aware of which customers, if any, and network routes are affected by the damage by performing correlation of the various alarms and indicators received. In addition, the procedure assumes the appropriate records, and all tools, material, and equipment required for the repair are available.

Repair OSP Failure

If the event assessment determines that the quickest and best restoration is to repair the failed fiber, then the damaged fiber must be removed from the location and new fiber pulled in place. The new fiber must then be re-spliced at existing splice points. The estimated time for this recovery strategy is within 24 hours of a failure.

This strategy is similar to “Business as Usual,” but for more major failure. The steps required for this method are outlined in the [OSP Failure procedure \(Page 52\)](#) following this section.

Bypass OSP Failure

If the event assessment determines that access to a failed point is limited or the damage cannot be restored within the desired window, then a bypass may be the best-case scenario. In order to restore connectivity, it is necessary to tap into the failed fiber at locations upstream and downstream from the failure point and placing new fiber in a temporary configuration (e.g., street-level enclosures). The estimated time for this recovery strategy is within 24 hours of a failure.

The steps required for this method are outlined in the [OSP Failure procedure \(Page 52\)](#) following this section.

Reroute to Alternate Node

If splicing new fiber to recover the damaged fiber is not practical within the required recovery timeframe, it may be feasible to use available routes already in place to connect the routes and customers to another node. Customer circuits would have to be re-routed in (Circuit OSS system) and reconfigured in the network. Success of the strategy depends on the availability of secondary routes between the originating location and terminating location. The estimated time for this recovery strategy is within 24 hours of a failure. The steps required for this method are outlined in the [OSP Failure procedure \(Page 52\)](#) following this section.

Bypass outside Plant failure with Line-of-Site Technology

It may be possible to bypass lower capacity failures using line-of-site technologies, such as free space optics. New equipment would be needed, as well as roof and window rights. There are service providers and vendor who can install and provide service. The estimated time of service recovery is within 5-7 days. Follow the steps in the [OSP Failure procedure \(Page 52\)](#).

3.5.2. Outside Plant Failure Response and Restoration Procedure

I. Immediate Action

- Confirm failure by attempting multiple methods to access interrupted devices and nodes
- Use Fiber management system OSP Insight to validate physical plant records and working fiber assignments.

II. Assessment

- Determine scope of the potential interruption
- Determine initial root cause – construction, accident, fiber quality, network, environmental, structural, etc.
- Identify interim strategy to restore service – repair failure, bypass failure, reroute to alternate node.

III. Response

- Dispatch an OSP repair team to the affected site
- Notify conduit or Right of Way (ROW) owner/operator
- Gain access to the manholes and poles in the affected area
- Obtain assessment from conduit or ROW owner/operator
- Assess the situation and determine the cause of the damage. If the damage was caused by a persisting and recurring problem, follow proper safety precautions before proceeding.
- Visually inspect the damaged area and verify the initial reports of the damage with the information provided by the NOC.
- Splice fibers to bypass the cut
 - Obtain new fiber assignments from Fiber Engineering if required
 - Pull a new fiber sheath through a street-level enclosure or alternative conduit between upstream and downstream points of the affected area.
 - Break the fiber at the upstream and downstream splice points. Make sure the fiber is labeled in order to ease the splicing effort for the bypass link.
 - Once the new fiber has been placed, verify the required splices and connections to restore the connectivity.
 - Splice the new fiber to the existing fiber.
 - Verify connectivity by performing OTDR testing and normal NOC test and acceptance procedures.
- Notify restoration team

IV. Restoration

- Re-engineer permanent service.
- Restore permanent service by replacing temporary bypass.
- Investigate methods and/or design to reduce future service impacts
- Inform and communicate to all Crown Castle Fiber employees, customers, and public as necessary
- Perform internal post mortem with business continuity team
- Perform external post mortem with vendor and/or parties responsible for the outage
- Communicate results of post mortem with customers
- Take appropriate steps to alleviate future service disruptions

3.5.3. Network Node Recovery and Restoration

This section covers recovery and restoration in the event of a Network Node failure. The node failures include any major damage to the buildings and infrastructure of locations designated as Crown Castle Fiber nodes.

Interim strategies for response include:

- Deploy interim capabilities in the node
- Deploy temporary node
- Rebuild the node entirely
- Bypass the failed node
- Reroute customer connections to another node

Each of the strategies range in the time required for recovery, as well as the coordination of resources and information. The recovery procedure assumes the failure has been detected by the NOC and furthermore, isolated to a specific node or group of nodes. The NOC should also be aware of which customers, if any, and network routes are affected by the damage by performing correlation of the various alarms and indicators received. In addition, the procedure assumes the appropriate records are available, and all tools, material and equipment required for the repair are available.

Interim Node Capabilities

This strategy is intended to provide the capabilities to keep an affected node operational during a disaster situation. This approach is viable for nodes and locations that are not badly damaged. The time to recovery depends on the extent of the damage and the availability of spares and new equipment. Spare equipment can be deployed while new equipment is ordered on an expedited basis to replenish the spares. In addition, new fiber may have to be pulled into risers to restore potential damage. An example of the strategy is loss of power for an extended period of time. Temporary or permanent batteries or generators may be deployed to support the power requirements of the equipment, and interim processes may have to be utilized to maintain the interim equipment. The estimated time for this recovery strategy is within 1-2 days.

Deploy Temporary Node

This strategy entails deploying spare and new equipment in temporary housing, such as a trailer or spare generator. The trailer can be equipped with basic and essential components found in all nodes in the network. Equipment such as SONET muxes and DWDM equipment would provide the network connectivity, while batteries and an external generator and HVAC unit provide the environmental protections required. Fibers at manholes or poles would have to be re-spliced to new fibers in the trailer. The trailer will be modeled as a new node attached to the Crown Castle Fiber bucket truck and dispatched using existing Crown Castle Fiber procedures. The strategy is viable for most nodes based on the amount of equipment and connectivity required. The estimated time for this recovery strategy is within 24 hours of a failure.

Rebuild Node

If the building is intact, this strategy entails having space available in the same location. The location should be equipped and configured as closely as possible to the original node configuration. Fiber risers would have to be rerouted and equipment configured. Spare equipment could be used and new equipment ordered on an expedited basis. The estimated time for this recovery strategy is within 2-3 days of a failure.

Bypass Node

This strategy entails bypassing a damaged or affected node by re-splicing the fiber in the manholes or on poles outside the node to other nodes and other customer sites. This strategy requires rebuilding circuits. It is very

similar to the recovery of an OSP failure as detailed in the OSP recovery section. It is actually a strategy that combines bypass and rerouting of connections. The steps required for this method are listed in the [Network Node Failure \(Page 55\)](#) section following this section.

Reroute Customers

If repairing, replacing, or bypassing a node to recover is not practical within the required recovery timeframe, it may be feasible to use available routes already in place to connect the routes and customers to another node. If fiber exists near the customers, and runs past another node, splicing that fiber into existing customer access fiber to route circuits to new nodes may be feasible. This strategy requires that circuit termination points be accessible to the backup node. Customer circuits would have to be re-routed and reconfigured in the network. Success of the strategy depends on the availability of secondary routes between the originating location and terminating location. In addition to fiber connectivity and splicing, fixed wireless connectivity is also feasible to establish short-term connectivity requirements. The estimated time for this recovery strategy is within 24 hours of a failure. The steps required for this method are listed in the [Network Node Failure \(Page 55\)](#) section following this section.

3.5.4. Network Node Failure Response and Restoration Procedure

I. Immediate Action

- Initiate normal escalation process
- Notify Event Chairperson
- [Transfer NOC Function \(Page 50\)](#)
- [Activate NOC Crisis Bridge \(Page 84\)](#)

II. Assessment

- Determine Scope of the potential interruption
- Determine initial root cause – fiber, network, environmental, structural, etc.
- Identify interim strategy to restore service – interim node capabilities, rebuild node, temporary node, bypass node or reroute customers
- If the failed node is the main hub, determine whether the transfer of NOC operations is required

III. Response

- If NOC facility, [Transfer NOC Function \(Page 50\)](#)
- Dispatch resources to the affected site
- Implement interim strategy
- Activate expedited ordering
- Obtain emergency equipment if needed:
 - Emergency generator
 - Trailer
 - Emergency HVAC unit
- Notify restoration team

IV. Restoration

- Return to building only upon instruction from authorities that it is safe
- Restore service and operations
- Investigate methods and/or design to reduce future service impacts

- Inform and communicate to all Crown Castle Fiber employees, customers, and public as necessary
- Perform internal post mortem with business continuity team
- Perform external post mortem with parties responsible for the outage
- Communicate results of post mortem with customers
- Take appropriate steps to alleviate future service disruptions

3.5.5. NetworkElementFailure Response and Restoration Procedure

This section covers recovery and restoration in the event of a single or multiple network element failures. The element failures include both hard failures and soft failures such as hacking, denial of service (DoS) attacks, software bugs, and broadcast storms.

The recovery strategies include:

- Reload software and configuration
- Replace network elements
- Bypass network element

Each recovery strategy ranges in the time required for recovery, as well as the coordination of resources and information. The following procedures assume the failure has been detected by the NOC and isolated to a specific element or group of elements. The NOC should also be aware of which customers, if any, and network routes are affected by the damage by performing correlation of the various alarms and indicators received. In addition, the procedure assumes the appropriate records, and all tools, material, and equipment required for the repair are available.

Reload Network Elements

If a network element configuration becomes corrupted or experiences a soft failure as a result of hacking, denial of service (DoS) attacks, software bugs and broadcast storms, the strategy for recovery is to clear the configuration and reload a clean configuration. This requires a detailed correlation with the any records and inventory information that provides the details of the connections and users affected on the device. The estimated time for this recovery strategy is within hours of a failure. The steps required for this method are listed in the [Reload Network Element \(Page 57\)](#) procedure in the following sections.

Replace Network Element

If the event assessment determines that the device is either physically damaged or the soft failure is such that the device cannot be salvaged through a reload, and then the replacement of the unit may offer the best restoration. In this scenario, the device will be replaced using either spare or new-deployment inventory. The steps required for this method are listed in the [Replace Network Element \(Page 58\)](#) procedure in the following sections.

Bypass Network Elements

This strategy entails bypassing a damaged or affected network element by patching the fiber in the node to other network elements and other customer terminations within the node. This strategy requires rerouting and rebuilding circuits. The steps required for this method are listed in the [Bypass Network Element \(Page 59\)](#) procedure in the following sections.

3.5.6. ReloadNetworkElement Response and Restoration Procedure

I. Immediate Action

- Confirm failure by attempting multiple methods to access the network element

II. Assessment

- Determine scope of the potential interruption
- Determine initial root cause – fiber, network, environmental, structural, etc.
- Identify interim strategy to restore service – reload network element, replace network element or bypass network element.

III. Response

- Dispatch resources to the affected site
- Engage vendor Technical Assistance Center (TAC) or on-site resources
- Reload software and configuration
 - Disconnect network element from the network.
 - Obtain element configuration and backup files from backup location
 - Obtain vendor specific information for the affected element – use either CD copies or download from vendor web site.
 - Load operating system software on the network element.
 - Go through installation procedure.
 - Verify the network element is running properly.
 - Connect the network element onto the network.
 - Verify the network element is visible from the management console and can communicate with neighbor devices.
 - Configure customer specific parameters on the network element.
 - After each customer configuration, verify that operational status of the service is up.
 - Monitor the device for a period of 72 hours for any abnormalities or additional issues.
- Notify restoration team

IV. Restoration

- Restore service and operations by implementing solutions discovered during troubleshooting – swap equipment, new fiber, etc.
- Investigate methods and/or design to reduce future service impacts
- Inform and communicate to all Crown Castle Fiber employees, customers, and public as necessary
- Perform internal post mortem with business continuity team
- Perform external post mortem with vendor and/or parties responsible for the outage
- Communicate results of post mortem with customers
- Take appropriate steps to alleviate future service disruptions

3.5.7. Replace Network Element
Response and Restoration Procedure

I. Immediate Action

- Confirm failure by attempting multiple methods to access the network element

II. Assessment

- Determine scope of the potential interruption
- Determine initial root cause – fiber, network, environmental, structural, etc.
- Identify interim strategy to restore service – reload network element, replace network element or bypass network element.

III. Response

- Dispatch resources to the affected site
- Engage vendor Technical Assistance Center or on-site resources
- Obtain spare or order on an expedited basis
- Replace network element
 - Disconnect network element from the network.
 - Obtain element configuration from backup files
 - Obtain vendor specific information for the affected element.
 - Install the new device in the rack
 - Power up the new unit
 - Verify the network element is running properly.
 - Connect the network element onto the network.
 - Verify the network element is visible from the management console and can communicate with neighbor devices.
 - Configure customer specific parameters on the network element.
 - After each customer configuration, verify that the operational status of the service is up.
- Notify restoration team

IV. Restoration

- Restore service and operations by implementing solutions discovered during troubleshooting – swap equipment, new fiber, etc.
- Investigate methods and/or design to reduce future service impacts
- Inform and communicate to all Crown Castle Fiber employees, customers, and public as necessary
- Perform internal post mortem with business continuity team
- Perform external post mortem with vendor and/or parties responsible for the outage
- Communicate results of post mortem with customers
- Take appropriate steps to alleviate future service disruptions

3.5.8. Bypass Network Element Response and Restoration Procedure

I. Immediate Action

- Confirm failure by attempting multiple methods to access the network element

II. Assessment

- Determine scope of the potential interruption
- Determine initial root cause – fiber, network, environmental, structural, etc.
- Identify interim strategy to restore service – reload network element, replace network element or bypass network element.

III. Response

- Dispatch resources to the affected site
- Engage vendor Technical Assistance Center or on-site resources
- Patch connection to alternate network element
 - Obtain new SOWs from Network Engineering.
 - Disconnect network element from the network.
 - Configure equipment at the new node in order to provide the required connectivity and services.
 - Configure customer specific parameters on the network element.
 - After each customer configuration, verify that the operational status of the service is up.
- Notify restoration team

IV. Restoration

- Re-engineer permanent service
- Restore permanent service by replacing temporary bypass
- Investigate methods and/or design to reduce future service impacts
- Inform and communicate to all Crown Castle Fiber employees, customers, and public as necessary
- Perform internal post mortem with business continuity team
- Perform external post mortem with vendor and/or parties responsible for the outage
- Communicate results of post mortem with customers
- Take appropriate steps to alleviate future service disruptions

3.5.9. Network Element Configuration and Restoration Response and Restoration Procedure

Use the files below to load a stored configuration onto a specific device. These instructions will completely replace the current configuration.

3.6. Business Process Recovery and Restoration Procedures

This section contains procedures for recovery and restoration of back-office business processes and the business supporting IT environment.

- A. [Temporary Work Location](#)
- B. [Medium-Term Site Relocation](#)
- C. [Recover Telecommunications](#)
- D. [Restore Staffing Levels](#)

3.6.1. Temporary Work Location

Response

- Move critical displaced employees to secondary worklocations
 - Create space as needed
 - Confirm minimum resources available and obtain or purchase missing resources
 - PCs or laptops with Ethernet connections
- Reserve local hotel space for critical employees
- Request other employees work from home
 - Use Virtual Private Network (VPN) capabilities to access corporate network from remote locations over the Internet [Via Citrix](#)
 - Reroute voice communications
 - Forward office phone numbers to mobile phones using IP Phone capabilities or
 - Distribute, install and use IP Softphone software on laptops to make the laptop act as an office IP phone
- Activate internet chat capabilities (Yahoo chat, AOL Instant Messenger, or MSN Messenger) or contract for Internet meeting capabilities
- Log into [Jabber Instant Messaging System](#) to communicate with other Crown Castle Fiber personnel during an emergency, if normal Crown Castle Fiber communication mechanisms unavailable

3.6.2. Medium-Term Site Relocation

Response

- Instruct all employees to initially work from home
 - This excludes employees on the Critical Event Teams
- Instruct employees to use web-based company email and cell phones for all communication until Crown Castle Fiber resources are available
- Secure temporary office space to house critical personnel and other support functions
- Dispatch available IT personnel immediately to the temporary location
- [Supplement staffing requirements](#) as necessary
- Salvage as much equipment and software as possible from affected locations
- Transport recovered equipment to temporary location
- Obtain office equipment – phones, PCs, laptops, servers, printers, copiers and fax – for the temporary location
- Order communications facilities on an expedited basis
 - Order POTS lines for initial voice communication and fax capabilities
 - Order voice service with the Direct Inward Dial (DID) of the affected location mapped to the temporary location
 - Order data connectivity to other Crown Castle Fiber locations
 - Order Internet access for the temporary location – DSL is a viable short-term alternative
 - Connect through Crown Castle Fiber Internet gateway location (Worcester) if location is accessible and WAN is installed
- [Install and configure voice network capabilities](#) – voice gateway and Call Manager
 - Configure the phone systems to route incoming calls to handsets or cell phones
- [Install and configure servers](#)
- [Install and configure the LAN](#) network infrastructure
- [Enable connectivity between the PCs](#) and servers
- [Configure WAN connectivity](#)
- Obtain a TV with cable and/or satellite feed to monitor news and events
- Order Emergency Supplies – replenish periodically as necessary
- Arrange to have mail and package deliveries forwarded to new location
- Arrange for transportation and lodging if necessary to maintain coverage
- Procure temporary furniture – e.g., tables and chairs
- Procure office supplies
- Notify restoration team

3.6.3. Recover Telecommunications

This section provides the steps required to install and configure telecommunications services – voice and fax – at a location. The required steps are:

- Salvage as much equipment and software as possible from affected locations
- Buy handsets from vendors and local retailers – Analog and VoIP
- Determine the number of telephones and lines needed
- Order voice and/or data circuits and services from provider as required.
- Assess data/voice cabling/jack availability and install additional if needed.
- Install and configure voice equipment
 - Cisco Call Manager Application
 - Voice Gateway Router
 - Voicemail server (Cisco Unity Application)
- Verify user voice/fax/voicemail configurations properly restored
- Connect SIP/PRI to gateway router
- Connect phone equipment and Initiate test calls

- Domestic – local and long distance
- International
- Services – 411 and 911
- Internal – other extension and conference
- Document the network configuration and connectivity specifics

3.6.4. Restore Staffing Levels

This section provides the steps required to supplement or restore staff at a specific location or for a specific recovery and restoration function. The required steps are:

- Account for all employees in and around the affected area
- Determine missing or unavailable staff members
- Verify that teams have sufficient staff to cover all critical tasks assigned to Critical Event Team
- Verify that the company has sufficient staff to cover critical tasks and other responsibilities during the disrupting event
- If teams are not fully staffed, identify other Crown Castle Fiber resources who can fill open positions or areas of responsibility
- Initiate notification and callout
- Give replacement staff a description of the event, the recovery process, and their role in the recovery and restoration
- If additional resources are required contact HR or staff supplementation vendors directly
 - Provide the quantity and skill set of desired resources
 - Interview and acquire the quantity of employees required with specific skill sets
 - Track time using timesheets for accurate billing
- Arrange for transportation and lodging if necessary to maintain coverage

4. IT Systems Business Continuity Strategy

Summary

Crown Castle Fiber's IT infrastructure is designed for very high availability and a number of strategies are employed to reduce the risk of a service-disrupting event and to recover critical business systems quickly in the event of a service disrupting event.

Mitigation Strategy

Mitigation consists of capabilities deployed to reduce the risk and impact of an event:

- Data storage redundancy
- Server redundancy/resiliency
- Application redundancy
- Data replication
- Data backup to tape

The IT server/application infrastructure is broken down into three overall protection categories:

Redundant – Systems that are supported by two or more servers and run in a parallel configuration across two or more diverse locations. The loss of any single system would have no operational impact and the failed/destroyed system would be restored or replaced as soon as possible.

Stand-by – Systems that are set-up to replicate data to secondary "shadow" servers located in a separate facility. In the event of a loss of any of the primary systems, the required steps to restore availability and overall end-user impact would be minimal, as data would be readily available and users would only have to re-point their applications to the stand-by data source.

Recovery – Systems in this category would undergo the standard process of restoring a failed/destroyed server on a replacement server, based on most current back-up data (from tape) available.

Response Strategy

Response involves short-term strategies for working around a problem. In the event of a disrupting event affecting Crown Castle Fiber IT infrastructure, an assessment will be made of whether the primary server equipment or any specific applications can continue to operate. If any are impacted, steps will be taken to bring up the standby servers and applications at the secondary location. At a high level this involves:

- Insuring that connectivity is available
- Configuring the standby/backup environment
- Insuring that data has been replicated or recovered from tape backups
- Reconciling missing data
- Re-pointing clients and users to the new, active applications

Restoration Strategy

Restoration means reverting to normal, "business as usual" operations. Restoration involves either restoring the full capabilities of the original site, server or application or establishing a new permanent data center at another location.

4.1. System / Application Mitigation and Response Strategy Table

4.1. Mitigation and Response Strategy (Continued)

4.1. Mitigation and Response Strategy (Continued)

4.2. Application/Server Failure

Response

Stand-By Category Systems

In the event of a failure of any application or system that falls into the “Stand-By” category, the following process will be followed:

- Assess the application or system associated with the failure, in person or remotely (via Remote KVM, server ILO, or RDP).
- Update the Event Chairperson on the status of the situation after the initial assessment is complete or within 30 minutes (whichever is less).
- If the problem cannot be readily identified or the recovery of the primary application or system is not expected to be achievable within one-hour (during normal work day hours of 8am to 5pm, M-F) or within 3 hours outside of normal work day hours, migration to the applicable Stand-By system will commence:
 - Verify availability of the Stand-By system(s)
 - Validated the Stand-by application server and/or database(s) as functioning and applicable data is current.
 - If the primary application server fails, re-point the Stand-by application server to the production database server via DNS changes.
 - If the primary database server fails, re-point the production Application server to Stand-by database server via DNS changes.
 - Test the reconfigured Stand-by environment for proper operation.
 - Notify the end-user base of the availability of the migrated Stand-by environment and provided verbal and/or written instructions specific to any special access/login procedures.
 - Monitor the migrated Stand-by environment for proper operation until the primary application server and/or database is restored.
- Provide the Event Chairperson regular updates regarding the status of the recovered environment, and alert them to any restoration plans back to the primary system(s), if applicable.

Recovery Category Systems

In the event of a failure of any application or system that falls into the “Recovery” category, the following process will be followed:

- Assess the application or system associated with the failure, in person or remotely (via Remote KVM, server ILO, or RDP).
- Update the Event Chairperson on the status of the situation after the initial assessment is complete or within 30 minutes (whichever is less).
- If the problem cannot be readily identified or the recovery of the primary application or system is not expected to be achievable within one-hour (during normal work day hours of 8am to 5pm, M-F) or within 3 hours outside of normal work day hours, migration to a suitable alternate server will commence:
 - Determine the availability of current server hardware which may include:

Business and Service Continuity Plan – Crown Castle Fiber

Methods and Procedures

DETAILED METHODS AND PROCEDURES

- Pre-staged base server equipment in the various IT data center locations.
- Existing server equipment that may be re-missioned or re-configured for dual-use to accommodate the recovery of the failed server/application (see [Attachment Crown Castle Fiber IT Server Inventory](#)).
- Spare equipment maintained in IT storage
- If spare/staged equipment is unavailable, replacement equipment will be ordered on an expedited basis.
- Obtain appropriate software and associated licenses (see [Attachment Crown Castle Fiber IT Deployed Software Summary](#))
- Contact vendors for technical or on-site/hands-on assistance if required (see [Attachment IT Vendor Contact List](#))
- Install server equipment in a secure, climate-controlled environment at one of the Data Center locations (Westborough, 111 8th Ave, Marlborough, Worcester, J-Dye or Boxborough, Canonsburg).
- Configure server equipment with the proper name and IP address
- Install Base OS software on each server
- Obtain necessary backup tapes (or confirmation of accessibility to remote back-up data)
- Recover recent application data
- Verify connectivity of the servers on the network
- Document server configuration and connectivity specifications.
- Advise end-user base of the availability of the recovered server environment and provided verbal and/or written instructions specific to any special access/login procedures.
- Monitor recovered server environment for proper operation, and determine if recovered environment will be deemed “permanent” or if a subsequent migration back to original server equipment and/or location is required.
- Provide the Event Chairperson regular updates regarding the status of the recovered environment, and alert them to any restoration plans back to the original server equipment/location, if applicable.

Restoration

Regardless of the category (Redundant, Stand-by or Recovery) of system or application that was disabled as the result of an event, once any immediate “Response Strategy” actions have been completed and business operations have been restored to an acceptable level, the following steps must be taken to ensure impacted servers are migrated back to a normal operating environment:

Data Center Environment

- Assess the damage or destruction of an IT Data Center location.
 - If the original site can not be repaired, then a new location will be chosen.
 - If the impacted site can be repaired:
 - Restore necessary network connectivity, all racking and shelving, climate control, and back-up power (generator and/or UPS)
 - Purchased any additional equipment as required

Servers & Applications

- Determine if servers already sourced and configured as part of the “Response Phase” are adequate and an available option to accommodate the permanent restoration of the systems/applications that were impacted.
- If current server hardware used for the Response Phase does not provide a suitable long-term option, the availability of other server hardware will be assessed to include:
 - Existing server equipment that may be re-missioned to accommodate the restoration of the servers and applications to be restored (see [Attachment Crown Castle Fiber IT Server Inventory](#).)
 - Spare equipment maintained in IT storage
- If spare/staged equipment is unavailable, replacement equipment will be ordered on an expedited basis.
- Obtain appropriate software and associated licenses (see [Attachment Crown Castle Fiber IT Deployed Software Summary](#))
- Contact vendors for technical or on-site/hands-on assistance if required (see [Attachment IT Vendor Contact List](#).)
- Install Server equipment in the designated IT Data Center location.
- Configure Server equipment with the proper name and IP address
- Install Base OS software on each server
- Verify connectivity to the servers on the network
- Schedule a controlled cut-over from temporary, “Restored” systems
- Migrate applications and associated data from the Restored systems to the replacement servers by either restoration of a current back-up tape or network-based data copy
- Test restored system for proper operation.
- Document restored server configuration and connectivity specifications

4.3. DHCP Failure

Response

DHCP (IP assignment) services are provided for the user base by the network of Domain Controllers located across the network (one DC per office location, as well as in both the primary and back-up IT Data Centers). In the event the DHCP service was interrupted at any location, there would be minimal impact, as IP addresses are configured to be “leased out” for eight hours upon issuance. In the event of a DHCP problem, the service would be restored on a different server. As an interim step, a new “address pool” for the impacted office IP range could be configured on any of the remaining, operable Domain Controllers that are accessible within the corporate network.

Restoration

Once any immediate “Response Strategy” actions have been completed and business operations have been restored to an acceptable level, the following steps must be taken to ensure an impacted DHCP server is migrated back to a normal operating environment:

- Assess impacted server and determine whether it can be repaired/re-built or needs to be replaced.
- If a repair/re-build is possible, obtain the needed spare parts for the repair from IT inventory or ordered on an expedited basis (see [Attachment Crown Castle Fiber IT Server Inventory](#).)
- If server hardware replacement is required, equipment will be ordered on an expedited basis.

-
- Contact vendors for technical or on-site/hands-on assistance if required (see [Attachment IT Vendor Contact List](#))
 - Re-installed base OS software on the server (If necessary)
 - Verify connectivity
 - Schedule a controlled cut-over from temporary “Restored” system.
 - Migrate applications and associated data from the Restored systems to the repaired or replacement server
 - Current back-up tape
 - Network-based data copy.
 - Test the restored system for proper operation.
 - Document restored server configuration and connectivity

4.4. Domain Controller Failure

Response

The Domain Control servers provide user authentication services, DHCP and in some cases, print services within the network. Crown Castle Fiber maintains dedicated Domain Controllers in each office as well as both IS data center locations throughout its network. In the event of a failure of any Domain Controller, the remaining Domain Control server(s) will provide necessary authentication services automatically and can be quickly configured to provide DHCP and print services for users outside of their normal area of control. If all Domain Controllers are disabled, a Domain Controller will have to be rebuilt.

Restoration

Once any immediate “Response Strategy” actions have been completed and business operations have been restored to an acceptable level, the following steps must be taken to ensure the impacted Domain Controller is migrated back to a normal operating environment:

- Assess impacted server and determine whether it can be repaired/re-built or replaced.
- If a repair/re-build is possible, obtain the spare parts required for repair from IT inventory or ordered on an expedited basis (see [Attachment Crown Castle Fiber IT Server Inventory](#))
- If server hardware replacement is required, equipment will be ordered on an expedited basis.
- Contact vendors for technical or on-site/hands-on assistance if required (see [Attachment IT Vendor Contact List](#))
- Re-installed base OS software on the server (If necessary)
- Verify connectivity
- Schedule a controlled cut-over from temporary “Restored” system
- Migrate applications and associated data from the Restored systems to the repaired or replacement server
 - Current back-up tape
 - Network-based data copy.
- Test the restored system for proper operation.
- Document restored server configuration and connectivity specifications

4.5. Personal Computer Loss

Response

In the event of a loss of multiple personal computers across one or more locations, the following, immediate recovery steps will be taken:

- Salvage as much usable PC equipment and software as possible from affected locations
- Identify spare PC equipment maintained by IT
- Identify available PC equipment owned by the end-user (i.e home PCs) for potential, short-term use until permanent replacement equipment is obtained and configured. This could include relocating end-user/owned PCs to Crown Castle Fiber sites or configuring those systems for remote home use via VPN or Citrix.
- Order replacement (new or refurbished) PCs from vendors on expedited basis; purchased directly from local retailers
- Obtain applicable software and licenses
- Install Base OS software
- Configure Network parameters
- Installed and configured user/department-specific applications
- Configure devices to the appropriate users on a priority basis based on job function and overall impact severity to any specific departments.
- Test Connectivity
 - Access to email
 - Access to internal servers (user and departmental files)
 - Internet connectivity
 - Remote access

Restoration

Once any immediate “Response Strategy” actions have been completed and business operations have been restored to an acceptable level, the following steps must be taken to ensure permanent, replacement PCs are acquired and distributed accordingly:

- Obtain PCs from vendors on expedited basis or from local retailers
- Obtain software and licenses, if required
- Utilize standard configuration template for general users
- Install software on the PCs
- Configure network parameters
- Configure application parameters
- Deploy the devices to the appropriate users
- Connect users to LAN
- Test connectivity
 - Access to email
 - Access to internal servers (user and departmental files)
 - Internet connectivity
 - Remote access

4.6. Internal LAN/WAN Failure

Response

Data Center LAN/WAN

In the event of a loss of one or more data communications components at an IT data center location, the following, immediate recovery steps will be taken:

- Salvage networking equipment and software from the affected location (if possible)
- Obtain any required network equipment from:
 - Existing IT inventory
 - Vendors (on an expedited basis)
 - Local retailers (through direct purchase)
- Relocate affected IT server/application resources to the closest alternate IT data center location
- Install replacement networking equipment
- Connect relocated server and application resources to the LAN
- Assign new IP addresses to relocated equipment
- DNS changes will be made (if needed)
- Test connectivity and accessibility
- Document restored network configuration and connectivity specifics

Office Location LAN/WAN

In the event of a loss of one or more data communications components at an office location, the following, immediate recovery steps will be taken:

- Salvage networking equipment and software from the affected location (if possible)
- Order circuits and connectivity as need (if primary office location is unusable):
 - Provide connectivity via Crown Castle Fiber network if new location is on-net
 - Private line to other Crown Castle Fiber locations
- Order Internet access – DSL is viable short-term alternative
- Existing, internal wiring will be assessed. If no internal wiring exists or it is insufficient, steps to cable the location with CAT5 wiring through the use of internal, Operations staff, IT personal or contracted 3rd party vendors will commence.
- Obtain required network equipment from:
 - Existing IT inventory
 - Vendors (on an expedited basis)
 - Local retailers (through direct purchase)
- Install replacement equipment
- Configure routing, access to resources, and user privileges (if necessary)
- Test connectivity based on affected infrastructure
- Document restored network configuration and connectivity specifics

Restoration

If the network infrastructure was impacted due to the damage or destruction of an IT Data Center or business office location, a determination as to whether the original site will be repaired must be made. If the site will not be repaired, a suitable, permanent location to house the displaced servers or staff must be identified (this could be the location used for the initial Response Strategy). Whether the impacted site is repaired or replaced, the following steps will be taken:

- Determine if existing internal wiring (if any) can be re-used.
- Contact data wiring vendors for assistance (as required)
- Obtain required network equipment from:
 - Existing IT inventory
 - Vendors (on an expedited basis)
 - Local retailers (through direct purchase)
- Install replacement wiring and equipment
- Test connectivity
- Relocate displaced server equipment and/or end-users to repaired/replaced space
- Document restored network configuration and connectivity specifics

4.7. System Monitoring

Crown Castle Fiber's IT/IS organization utilizes a 3rd-party application to monitor the server and application environment. This tool has the capability to monitor a number of parameters ranging from basic server connectivity (Ping) tests, to disk space and CPU utilization and specific transaction types (i.e. HTTP, SMTP, etc.)

4.8. Data Backup and Retention

Crown Castle Fiber backs-up data from all servers on a regular basis. Four different back-up methodologies are employed based on the criticality of data and desired ease of access and recovery in the event of a system failure:

Data Replication – Certain key databases are replicated in real-time to “shadow” systems, in diverse locations. This provides the ability to quickly re-point applications to the replicated database in the event of a failure of the primary database

Data Snapshots – Certain key databases are backed-up during the course of the business day utilizing a “snapshot” approach in order to maintain multiple instances of the data in the event a system needs to be “rolled-back” in the case of a production problem. The availability of the snapshot data back-ups makes the process of rolling-back easy and limits the amount of data re-entry that would otherwise be required if a rollback to the prior day's full back-up were required.

On-site Back-ups – All system back-ups are written to an on-site data back-up appliance (EMC Data Domain) which provides de-duplication and high compression of data. This allows back-up files to be retained on-site for a minimum of six months, providing a method of fast and easy recovery of back-up data if required. In addition, the back-up appliance provides an efficient intermediate data source from which back-up tapes are created for off-site storage.

Tape Back-ups – System back-ups are generated from the Data Domain back-up appliance to tape for long term offsite storage.

4.9. Password Management

Crown Castle Fiber manages access to its internal network and application/data server environments through the use of passwords. In order to maintain a high level of security, passwords must meet certain minimum requirements with regard to minimum length and the use of combined letters, numbers and/or special characters. In addition, passwords are set-up with the requirement that they be changed on a regular basis as follows:

End-User Access Passwords – Must be changed every 90 days.

Server/Network Infrastructure Passwords – Must be changed every 180 days.

In order to ensure operational continuity in the event of an event during which Crown Castle Fiber’s IT personnel are unavailable, all IT infrastructure passwords are maintained in a clearly referenced file, located in the IT department’s “shared/Servers” directory. In addition a sealed/hard copy of this document is provided to the Executive Vice President of Engineering and Operations.

4.10. Supporting IT Documentation

[This section was a duplication of section 6 below](#)

5. Appendix

The appendices contain ancillary procedures, contact information, forms to be used in emergency situations and necessary information such as circuit IDs.

- I. Ancillary Procedures
 - a. [General Fire and Evacuation Safety Procedures](#)
 - b. [Fire / Evacuation Leads](#) and Assembly Points
 - c. [Emergency Purchase and Cash Procedures](#)
 - d. [Panic Avoidance Measures](#)
 - e. Business Continuity [Alert Hotline](#)
 - f. [NOC Crisis Bridge](#)
 - g. [Cisco IP Phone User Guide](#)
 - h. [IS-003 Document](#)
 - i. [Citrix User Doc](#)
 - j. [Instant Messaging System](#)
 - k. [IT Management Notification System](#)
 - l. [Telecommunications Service Priority \(TSP\)](#)

- II. Contact information
 - a. [Corporate Directory](#)
 - b. [Authorities](#) and Critical Services
 - c. [Vendor Contacts](#)
 - d. [Type II Providers](#)

- III. Forms
 - a. [Critical Event Summary Form](#)
 - b. [Critical Event Logging Form](#)
 - c. [Damage Assessment Form](#)
 - d. [Purchase Order Form](#)

5.1. Ancillary Procedures

5.1.1. General Fire/Evacuation Procedures

Evacuating Personnel from the Building

Upon being notified of a Fire or Emergency evacuation, personnel will immediately exit the building using the quickest and safest route possible. These routes are identified on the evacuation maps posted throughout the building. Crown Castle Fiber Fire and Safety coordinators are responsible for ensuring that their employees are aware of the evacuation and are exiting the building.

Designated personnel will be assigned to each stairwell, after training. These Stairwell Monitors will assist in the evacuation of the building by providing information as well as obtaining assistance for anyone that is physically unable to use the stairs. This will include both employees and visitors.

Signage/ Evacuation Maps

Emergency exit signs are illuminated throughout the building. The maintenance of these signs is the responsibility of the building management company. Any issues with the emergency lighting or signs should be immediately reported to the building management company.

Business and Service Continuity Plan – Crown Castle Fiber

Evacuation maps are posted in hallways throughout the entire building. These maps use a shaded coloring scheme to indicate the evacuation zone and a black dot to mark your location in the zone. Each evacuation zone has a minimum of two routes that lead out of the building.

Fire / Evacuation Drills

Crown Castle Fiber will coordinate drills with Building Management and Crown Castle Fiber Fire and Safety coordinators on a quarterly basis. The department heads are responsible for ensuring their personnel are available for this quarterly training.

Accounting for Personnel

Once outside the building, personnel will move, at a safe distance from the building, to the designated (Assembly Point), Managers are responsible for verifying the members of their department that are at the meeting point. They will then provide this information to the Crown Castle Fiber Fire and Safety coordinators or the person designated to gather the headcount. The manager should provide a last seen location for any missing personnel. An attempt to contact the missing people should be made via cell phone, if possible.

Maintain a Safe Distance

Employees should not reenter the building without prior authorization from emergency personnel (fire department, police). Employees should also remain a safe distance from the building to allow for emergency vehicles and emergency personnel to access the building. Assembly points for 55 Broad St., 900 Corporate Dr, 80 Central St, and 201 Old Country Rd Melville NY are listed in a table on page 85.

Fire / Evacuation Warden Responsibilities

Objective:

To direct the evacuation of your floor in the event of a required evacuation.

Procedure:

1. Follow building specific evacuation procedures, if available
2. Report to Warden Station when alarms are heard.
3. Determine if an evacuation is required for your floor.
4. Communicate with building services via the warden phone
5. Ensure Deputy Wardens have notified all floor occupants.
6. Evacuate the fire floor and floor above (*if necessary*).
7. Determine which stairway should be used to evacuate. (*if applicable*)
8. Notify the Event Chairperson of status
9. Ensure elevators are NOT used.
10. Ensure any handicapped persons are assisted during evacuation.
11. Ensure Crown Castle Fiber personnel rally at assembly location
12. Take headcount and identify missing personnel
13. Report to the Emergency Response Center after evacuation to provide a report.
14. If the building cannot be entered within one (1) hour proceed to secondary location (see table)

Fire / Evacuation Warden Responsibilities

Objective:

To direct the evacuation of your office in the event of a required evacuation.

Procedure:

Business and Service Continuity Plan – Crown Castle Fiber

1. Check your office for smoke or fire when alarm sounds.
2. Report your findings to the Fire Warden on your floor who will be positioned at the Fire Warden phone
3. Return to your office area after instructions are given.
4. Prepare your office for evacuation (*if necessary*).
5. Determine which stairway should be used to evacuate. (*if applicable*)
6. Lead evacuation down stairs. (*if applicable*)
7. Ensure elevators are NOT used.
8. Ensure any handicapped persons are assisted during evacuation.
9. Maintain order and remain calm.
10. Regroup at assembly point and take a headcount.
11. Report to the Emergency Response Center after evacuation to provide a report.

Searchers Responsibilities

Objective:

To ensure restrooms and other locations are checked in the event of an evacuation and to assist the Deputy Warden during evacuation.

Procedure:

1. Establish contact with Deputy Warden in your office when alarm sounds.
2. Search restrooms for occupants.
3. Inform occupants that they should return to their office.
4. Return to your office and search all conference rooms & storerooms.
5. If any door is locked, knock on door and announce that people must evacuate (*if necessary*).
6. Ensure that all doors are closed but not locked.
7. Ensure that elevators are NOT used.
8. Communicate with Deputy Warden to determine if evacuation is necessary and what stairway is to be used. (*if applicable*)
9. Remain in rear during evacuation down stairway. (*if applicable*)
10. Report any issues to Deputy Warden.

5.1.2. Fire / Evacuation Leads

Fire / Evacuation Leads

LOCATION	WARDEN	DEPUTY WARDEN	DESIGNATED SEARCHERS
80 Central St, Boxborough, MA			
300 Meridien Centre Blvd Rochester NY			
900 Corporate Dr, Newburgh, NY			
201 Old Country Rd Melville NY			

Business and Service Continuity Plan – Crown Castle Fiber

Fire / Evacuation assembly points

LOCATION	ASSEMBLY POINT
80 Central St, Boxborough, MA	
900 Corporate Dr, Newburgh, NY	
300 Meridien Centre Blvd Rochester NY	
201 Old Country Rd Melville NY	

Secondary work locations

LOCATION	ALTERNATE WORK SPACE
80 Central St, Boxborough, MA	<div style="background-color: black; width: 150px; height: 15px; margin-bottom: 5px;"></div> 55 Broad St. NYC Home / Remote
900 Corporate Dr, Newburgh, NY	<ul style="list-style-type: none"> 300 Meridien Centre Blvd Rochester NY Home / Remote
80 Central St, Boxborough, MA	<div style="background-color: black; width: 150px; height: 15px; margin-bottom: 5px;"></div> 900 Corporate Dr, Newburgh, NY Home / Remote
201 Old Country Rd Melville NY	505 8 th Ave, New York, NY 900 Corporate Dr, Newburgh, NY 80 Central St, Boxborough, MA Home / Remote

Business and Service Continuity Plan – Crown Castle Fiber

5.1.3. Emergency Purchase and Cash Procedures

It is expected that normal Purchase Order and Cash Disbursement procedures will be followed in a critical situation. In the event that emergency purchases and disbursements are required, employees can use their corporate cards, personal credit cards or cash to make emergency purchases within the limits of authorization. Normal reimbursement procedures will be used.

Single source vendor selection may be made in a critical situation within the limits of authorization.

The normal Purchase Order procedure is as follows:

- Requestor fills out (IR) Item request
- E-mails requests for approval to authorized approver(s).
- Finance Team sends out approved PO to vendors

The Purchase Order procedure is

- Requestor fills out PO request and e-mails immediate supervisor
- Approver(s) prints out and signs PO and informs Requestor
- Requestor mails or faxes approved PO to vendor

5.1.4. Panic Avoidance Measures

In an emergency situation, panic increases risk to people and property. It is important to take measures to avoid or reduce panic.

- ☐ Step away from a stressful situation for a time to regain composure
- ☐ Keep people informed with facts so that rumors and fear do not spread
- ☐ Speak to people in neutral tones. Avoid extreme terms.
- ☐ Give people a sense that an appropriate response to a situation is known and planned for
- ☐ Let people know if help is on the way
- ☐ If possible, make critical decision away from affected areas
- ☐ Do not make telephone calls compulsively. Be clear on who you are calling and why.

5.1.5. Business Continuity Plan (BCP) Employee Alert Hotline

The BCP alert hotline number is 978-264-6800 and is used to inform employees and others of the status of the response and restoration activities. To activate the BCP alert hotline:

- ☐ Go to a Crown Castle Fiber IP telephone
- ☐ Press the Message Button
- ☐ Press *
- ☐ Press #
- ☐ Mailbox
- ☐ PIN
- ☐ When it says to record message follow system prompts to record.

Primary Operator	Director, NOC
------------------	---------------

Business and Service Continuity Plan – Crown Castle Fiber

Secondary Operator	NOC Manager
--------------------	-------------

5.1.6. NOC Crisis Bridge

NOC alert hotline number is and is provided by. This hotline is used to inform Operational Personnel and others of the status of the response and restoration activities. To activate the NOC Crisis Bridge:

- ☐ Dial
- ☐ You will be asked for a conference code, enter
- ☐ Press #
- ☐ You will be placed into conference
- ☐ If you are the chairperson, press * then enter code

5.1.7. IT Management Notification System

In the event that Crown Castle Fiber’s infrastructure is severely impacted or unreachable, the IT Department has a text message based notification system that can be used to send alerts and updates outside of the Crown Castle Fiber network.

The emergency text message notification is sent directly to Crown Castle Fiber mobile devices from the IT department.

5.1.8. Telecommunications Service Priority (TSP)

Telecommunications Service Priority (TSP) is a ‘program that authorizes national security and emergency preparedness organizations to receive priority treatment for vital voice and data circuits or other telecommunications services.’

Crown Castle Fiber BCP operating and restoration procedures will be conducted in accordance with the TSP System. TSP services are identified in the Order Management and Circuit Inventory Systems at Crown Castle Fiber, this allows authorized Crown Castle Fiber customers to receive priority restoration on specific telecommunications services. A customer who provides a TSP declaration and TSP authorization code will receive priority attention by Crown Castle Fiber before a non-TSP classified service.

Additional information on the TSP program can be found at <http://tsp.ncs.gov/>

Business and Service Continuity Plan – Crown Castle Fiber

5.2. Forms

5.2.1. Critical Event Summary Form

The Critical Event Summary Form is completed after the event and summarizes information about the initiation and resolution of the incident. Steps taken and incidents during the critical event are recorded in the [Logging Form](#)

Date of Event	<input type="text"/>	Time of Occurrence	<input type="text"/>
Type of Event	<input type="text"/>	Location	<input type="text"/>
Event Chairperson	<input type="text"/>	Time Notified	<input type="text"/>

Description

Recovery Team Members	Restoration Team Members
<input type="text"/>	<input type="text"/>

Recovery Method	Duration
<input type="text"/>	<input type="text"/>

Restoration Method	Duration
<input type="text"/>	<input type="text"/>

Root Cause

Reports

Internal Post Mortem	Yes/No	External Post Mortem	Yes/No
Customer Report Written	Yes/No	Customer Report Delivered	Yes/No

Business and Service Continuity Plan – Crown Castle Fiber

Methods and Procedure

APPENDIX

5.2.2. Critical Event Logging Form

The Critical Event Logging Form is maintained during the critical event and records all steps, incidents and progress during the event. It is used to provide a complete and accurate history of the event, which is then summarized in the [Summary Form](#)

Date of Event
Type of Event

Time of Occurrence
Location

Date/Time	Initials	Description of Event and Actions

Business and Service Continuity Plan – Crown Castle Fiber

Methods and Procedure

APPENDIX

5.2.3. Damage Assessment Form

Date of Event

Time of Occurrence

Type of Event

Location

Item	Location	Status (Recoverable/Lost)

Business and Service Continuity Plan - Crown Castle Fiber

Methods and Procedure

APPENDIX

5.2.4. Purchase Order Form

Order Date: _____						For Purchasing Use Only Master PO/ Contract #: P.O. Order #:	
Delivery Date: _____						<u>Shipping Information</u> Ship to: _____ Attention: _____	
<u>Vendor Information</u> Vendor Name: _____ Vendor Address: _____ Attention: <input style="width: 80px; height: 20px;" type="text"/>						<u>Billing Information</u> Bill To: Crown Castle Fiber, 80 Central St, Boxborough, MA01719 Attention: Accounts Payable	
Detail of Order							
Item Name/ #	Line Description	Qty.	\$/unit	Project	Account #	Amount	
			\$ -			\$ -	
						\$ -	
						\$ -	
						\$ -	
						\$ -	
			\$ -			\$ -	
			\$ -			\$ -	
			\$ -			\$ -	
			\$ -			\$ -	
Notes:						Subtotal	
						\$ -	
						Tax	
						Shipping & handling	
						TOTAL	
						\$ -	
						Signature:	