FRONTIER

1919 McKinney Ave., Dallas, TX 75201
Frontier.com

June 20, 2024

Via UPS

Adam Teitzman, Commission Clerk
Florida Public Service Commission
Office of Commission Clerk
2540 Shumard Oak Blvd.
Tallahassee, FL 32399-0850

REDACTED

Re: Request for Confidential Treatment
Docket 20220000-OT; Frontier Florida LLC Emergency Response and Storm Restoration Procedures and Protocols

Dear Mr. Teitzman:

In accordance with Rule 25-18.020, Florida Administrative Code, Frontier Florida LLC hereby files an updated Emergency Management Plan. For the reasons set forth below, Frontier Florida LLC requests confidential treatment of the Plan under Rule 25-22.006(4)(a) and is, therefore, filing an original and two redacted copies of it.

The information set forth in the body of the Plan on pages 4, 5, 7-12, 15, 18, 19, 25, 26 is confidential under Fla. Stat. §§366.093(3)(c), as it contains information relating to Frontier's security measures, systems, and procedures, and Fla. Stat.§ 119.0725 (2) (b), as it contains information relating to critical infrastructure. The information set forth in the body of the Plan on page 25 is confidential under Fla. Stat. § 366.093(3)(f) because it contains certain employee personnel information.

If you have any questions regarding this matter, please do not hesitate to contact me at 214-724-7719, or by email judy.geise@ftr.com.

Sincerely,

Judy Geise
Manager, Regulatory
judy.geise@ftr.com

COM ___
AFD ___
APA ___
ECO ___
ENG ___
GCL ___
IDM 1
CLK ___

Enclosures
cc: Penny Buys, PBuys@PSC.STATE.FL.US (cover letter via electronic mail; redacted Plan via UPS)

FRONTIER

(FL) Frontier Communications Business Continuity and Crisis Management Plan

Reviewed: 01-June-2024

REDACTED VERSION

Table of Contents

1. Introduction 4
2. Terms and Definitions 6
3. Business Continuity Management System 7
    3.1. Resilience and Recovery Strategy 8
    3.2. Business Continuity Team Responsibilities 9
    3.3. Labor Contingency Planning 10
    3.4. Pandemic Contingency Planning 10
    3.5. Disaster Recovery and Cyber Security 11
4. Crisis Management/Emergency Response 12
    4.1. Crisis Response 12
        4.1.1. Response Phases 13
    4.2. Command and Control 13
    4.3. Roles and Responsibilities 15
    4.4. Emergency Communication 16
5. Emergency Restoration Priorities 18
    5.1. Restoration Priority 18
    5.2. Provisioning Priority 18
    5.3. Disaster Recovery Priority 19
    5.4. Federal TSP Annual Service Reconciliation 19
    5.5. E911 Restoration Priority Procedures 19
    5.6. Documented Medical or Life-Threatening Condition, Disability, or Elderly Customers 20
        5.6.1. Medical Emergency Accounts - Overview and Processing 20
        5.6.2. Services for Customers with Disabilities 21
        5.6.3. Medical Expedites - Elderly Attribute 22
    5.7. VIP (Emergency) Organizations Hazardous Conditions Repair Process 23
    5.8. Public Reporting of Hazardous Conditions 23
6. Florida 24
    6.1. Plan Content Requirements 24
    6.2. Commission Filing Requirements 24
    6.3. Damaged Pole and Overhead Facilities Repair and Replacement Procedures 25
    6.4. Emergency Contact Information 25
7. Plan Exercising, Testing, Training and Maintenance 26
8. Review and Revision Process 27

1. Introduction

Background

Frontier Communications' purpose of Building Gigabit America provides a digital infrastructure that empowers people to create the future. Frontier is connecting millions of consumers and businesses with reliable fiber internet and multi-gigabit speeds. Frontier is a mid-level company, and our strategy is to build fiber, sell fiber, improve customer service, and simplify operations.

Planning for the business continuity of Frontier before, during and after a business impacting event is a complex task. Preparation for, response to, and recovery from an impacting event affecting the administrative and business functions of Frontier requires the cooperative efforts of multiple organizations, in partnership with the functional areas supporting the "business" of Frontier. This Plan outlines and coordinates these efforts, reflecting the analyses by representatives from these organizations.

The multiple functions of incident response are shared between organizations and agencies, with the private sector and the government having different levels of responsibility. Thus, there is a need to guide all involved parties on how to prepare for and implement effective incident response.

When multiple organizations, or different parts of one organization, are involved in the incident response:

- consensus should be sought on overall mission objectives among all involved organizations,
- structures and processes should permit operational decisions to be taken at the lowest possible level, and coordination and support offered from the highest necessary level, and
- authority and resources shall be appropriate to the mission.

Purpose

The purpose of this Plan is for Frontier to be able to support the delivery of our products and services, provide critical connectivity, and the ability to protect the integrity of its customers' accounts during an incident. The Plan provides information relative to crisis management response during an event and continuity of operations during and after the event.

The Plan is considered a living document, regularly updates so it remains current with system enhancements and organizational changes. While the severity and consequences of a crisis cannot be predicted, effective crisis management and contingency planning can mitigate and minimize the impact on Frontier's mission, personnel, and faciltiies.

Scope

This Plan provides a framework for effective incident response and provides the basics for command and control, operational information, coordination and cooperation within the organization.

Frontier requires the commitment of each employee, department, and vendor in support of the objectives required to protect Frontier assets and ensure the Company's ability to serve its

customers. This Plan highlights the functions, operations, and resources necessary to ensure the continuation of Frontier's critical business processes in the event of an emergency. This Plan applies to all Frontier operations and personnel who must be familiar with response and recovery operations and processes within their respective roles and responsibilities.

Assumptions

This Plan is predicated on the validity of the following assumptions:

- During normal operations, routine or minor emergencies are within the response capabilities of each business unit organization, with minimal need for support or assistance from the Emergency Response Center (ERC).
- The emergency may occur with little or no warning and may escalate more rapidly than response organizations can manage. Resources to activate and operate the ERC will be made available by the business unit organizations supporting the ERC function.
- The situation that causes the event is larger than the region or state can control or perform restoration within their internal contingency plans. It should be noted, however, that the Plan can be functional and effective even in a localized emergency event or disaster. The priorities for restoration of essential communication services to the community will normally take precedence over the recovery of an individual organization.
- The Plan is based on the availability of personnel and support services. The accessibility of these, or equivalent support resources, is a critical requirement to the success of the restoration. The Plan is a document that reflects the changing environment and requirements of Frontier. Therefore, the Plan requires the continued allocation of resources to maintain it and keep it in a constant state of readiness.

2. Terms and Definitions

Business Continuity Management Team (BCMT) - Senior and mid-level leadership who have overall responsibility to manage all continuity related planning, response, and recovery efforts.

Continuity and Crisis Management Team (CCM) - Within the organization, the team that manages the overall strategic and operational functions of business continuity and crisis management events, procedures, and plans. This team helps manage all ERC activations and supports the CMT during crisis events.

Crisis Management Team (CMT) - Led by the Corporate Security Officer, this team consists of members of Executive Leadership and Senior leaders who will focus on strategic direction of the company during an incident.

Emergency Response Center (ERC) - The incident command system that supports effective emergency management of all available assets in a preparation, incident response, continuity and/or recovery process. This system follows guidelines set forth by the Federal Emergency Management Agency (FEMA and National Incident Management System (NIMS).

EventCon Checklist - The organizational business unit's checklist of responsibilities as it relates to emergency or continuity events.

Federal Communications Commission (FCC) - An independent agency of the U.S. federal government that regulates communications by radio, television, wire, satellite, and cable across the United States. The FCC maintains jurisdiction over the areas of broadband access, fair competition, radio frequency use, media responsibility, public safety, and homeland security.

Local Exchange Carrier (LEC) - The telephone company which operates within a local area and provides telecommunication services within that area.

Telecommunications Service Priority Program (TSP) - A program that authorizes national security and emergency preparedness (NS/EP) organizations to receive priority restoration and installation of vital voice and data circuits or other telecommunications services that may be damaged as a result of a natural or man-made disaster. TSP enables telecommunications carriers to prioritize the restoration, recovery and installation of critical circuits and voice capabilities in the event of a disaster or threat to the security of the United States. It is also the only authorized mechanism for receiving priority provisioning and restoration of NS/EP telecommunications circuits.

3. Business Continuity Management System

Frontier recognizes the importance of preparing for, responding to, and recovering from a disaster or business disruption. To that end, Frontier has developed a Business Continuity Management System (BCMS) to include critical business functions, risk mitigation strategies, crisis/emergency management, and recovery plans which are intended to minimize disruptions of service to Frontier and its employees, minimize financial loss, and ensure the timely resumption of operations. The BCMS requires an organization-wide emphasis on risks associated with the loss or extended disruption of business operations. This plan is a component of the organization's comprehensive recovery strategy and is intended to be paired with the Disaster Recovery Plan, Cyber Response Plan, and Pandemic Plan.

The BCMS is implemented in a cost-effective manner, based on a risk and business impact analysis, using generally accepted best practices and in compliance with applicable industry, legal and regulatory requirements. The benefits to this Plan are to:

- Minimize the loss of assets,
- Minimize confusion and enable effective decisions during a crisis,
- Guidance to resumption and minimize disruption,
- Avoid business failure as a result of a disaster,
- Maintain the public image and reputation of Frontier Communications,
- Facilitate the timely recovery of critical business functions.

3.1. Resilience and Recovery Strategy

Frontier's Business Continuity Management Plan is built upon the following Resilience and Recovery Strategy:

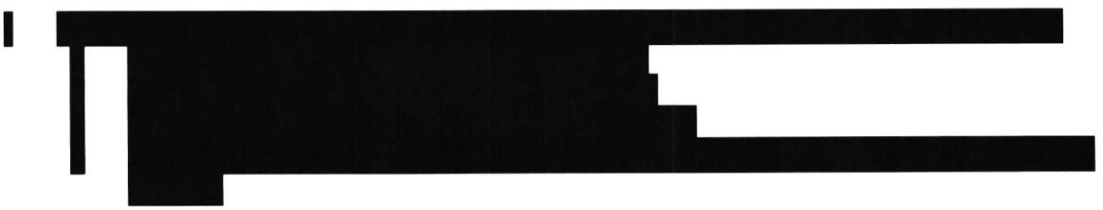
1. Conducting a business impact analysis to identify time-sensitive or critical business functions and processes and the resources that support them,
2. Identifying, documenting, and implementing actions to recover critical business functions and processes,
3. Assessing capability of recovery options to manage a business disruption,
4. Conducting testing and exercises to evaluate recovery strategies within the plan.

Frontier's Internal Audit Team conducts annual risk analysis meetings with executive leadership to determine events which could cause a major impact to Frontier's ability to provide communication services. This risk analysis process is reviewed on a regular basis with the Continuity and Crisis Management Team to ensure that changes to our critical facilities and critical business processes are aligned with our customer's service level requirements.

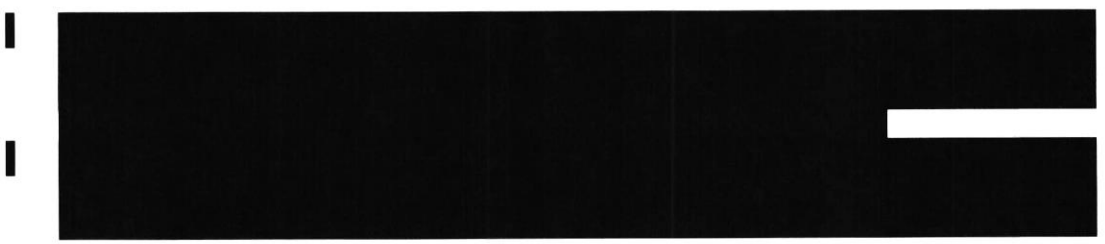
Frontier has processes and procedures at all levels to maintain a resilient network and incorporate mitigation measures for high-risk areas to help prevent an impact on our customers. Resilience efforts are based on all-hazards planning, which includes adoption of climate resilient features in ensuring the following:

- redundant network systems,
- information support systems such as climate observation and early warning systems,
- materials to provide additional insulation to our fiber networks to help protect from water, weather, and temperature extremes, and
- emergency services/utilities that can provide more reliable assistance during natural disasters and emergencies.

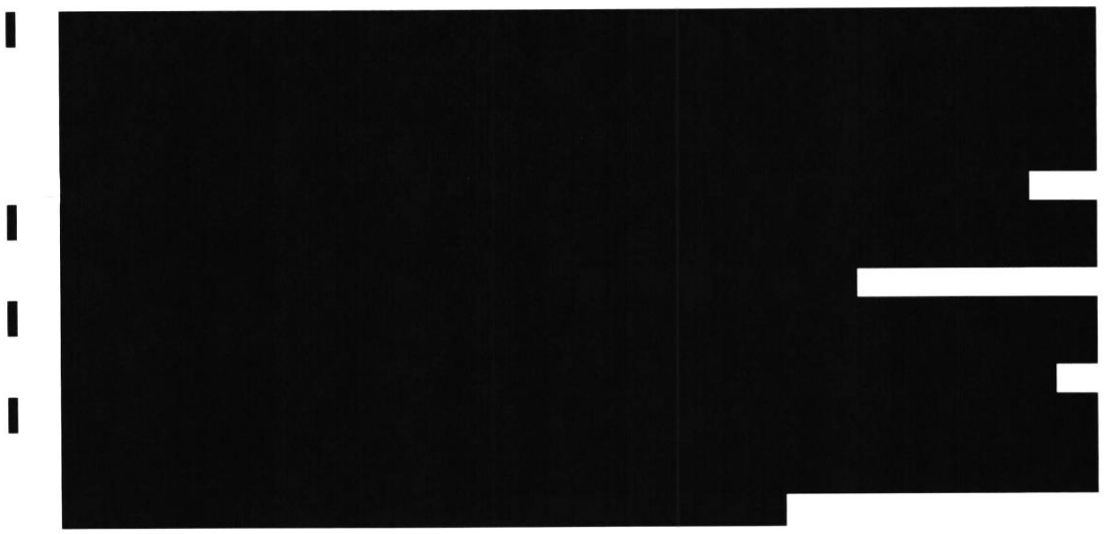
Failover/Redundancy



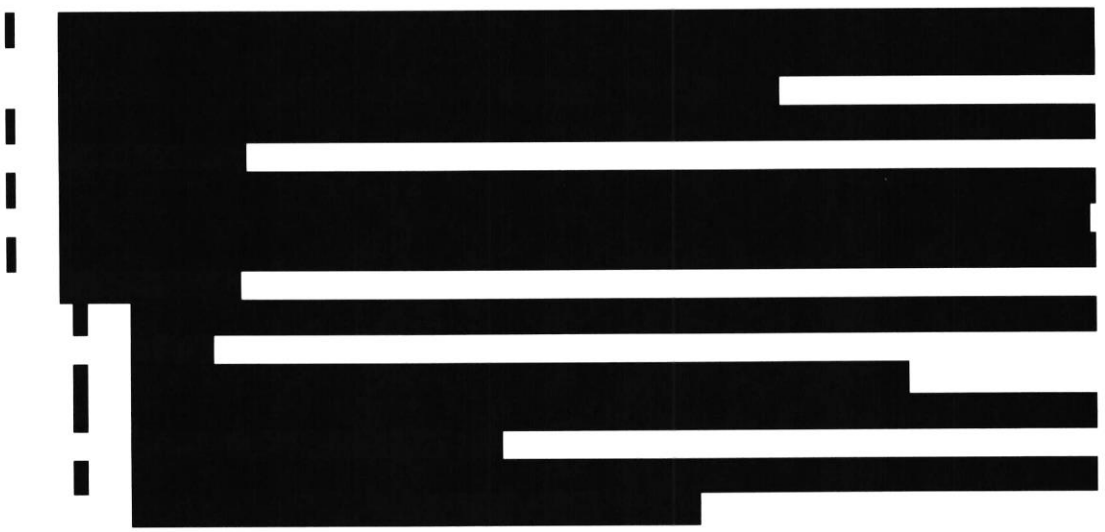
Internal Network & Operations



Emergency Supply Inventory



Emergency Staff



3.2. Business Continuity Team Responsibilities

Business Continuity Senior Leadership Team (EXCO/Crisis Management Team)

- Continues core business processes in case of disaster or emergency management.
- Declares a disaster.
- Directs the BC Sponsor to activate BC plans and recovery teams.
- Strategic business decision-making.
- Liaises with Company stakeholders and civil authorities.

Business Continuity Sponsor (BC Sponsor)

- Manages corporate business continuity improvement initiatives and oversees the implementation of a response plan to recover from disaster scenarios.

- Activates respective BC plans.
- Assumes operational control over its department(s) during declared emergency incidents and has full authorization to procure and expense on behalf of Frontier.
- Escalates and/or resolves issues from the business units requiring approval, facilitating the approval process.
- Acts as the liaison between the BC Senior Leadership Team and other teams and external entities for the purpose of information dissemination.
- Participates in after action reports on incidents and disasters.

Business Continuity Operations Leadership Team

- Executes their respective BCP and assists in the business continuity initiatives and activities planned by the BC Sponsor.
- Conducts risk identification and assessments, developing processes and procedures, facilitating training for all support, response, and recovery team members.
- Responsible for maintenance and testing of business continuity plans.
- Serves as lead in the Emergency Response Center (ERC), directs the activation of BCP recovery teams and tasks during disasters or business interruptions.
- Directs tactical operations during business interruptions and reports outcomes and resource needs to the ERC during disasters.
- Creates the development plan from remedial actions and issues raised through or resulting from BC tests.
- Participated in after action reports on incidents and disasters.

Business Continuity Support Team

- Coordinates the discovery and documentation process for their respective department(s) business continuity plan entries into the company's business continuity software platform.
- Assists the BC Operations Leadership Team in the development and maintenance of the BCP, policies, procedures, processes, and supporting documents for their respective department(s).
- Serves as a liaison, coordinating with interdepartmental functional groups and units.

3.3. Labor Contingency Planning

Frontier's Labor Contingency planning maintains a high level of preparedness, consistent with its unique role in furnishing critical telecommunications and information services. Frontier has an established plan regarding continuity of operations and a continuity of management, including centers, alerting lists, and alternate temporary locations deemed necessary to facilitate the installation, maintenance and restoration of critical telecommunications and information services under conditions of workforce events.

Essential service should be maintained for the duration of a work stoppage event. Every reasonable effort should be made to present the public with business as usual. Service priorities will be coordinated between business unit leaders and the BCMT, with objectives established weekly as to what level of service is desirable and/or attainable.

Frontier maintains a **Labor Contingency Planning Handbook**, which addresses the planning, communication, work assignment, travel requirements, safety and security, and time recording required during a work stoppage event.

3.4. Pandemic Contingency Planning

Frontier's Business Continuity Plan for pandemic illness would be similar to any other disaster that results in the loss of the availability of personnel for an extended period of time, there are unique factors resulting from a pandemic illness that must be addressed.

According to the World Health Organization, a pandemic results with the emergence of a disease new to the population that infects humans and causes serious illness, and which spreads easily and sustainably.

If Frontier is affected by the loss of the availability of critical personnel upon a declaration from local agencies, the **Pandemic Plan** would be activated.

3.5. Disaster Recovery and Cyber Security

If Frontier is affected by a cyber-attack that results in the loss of the technology or internal network capabilities which disrupt critical business functions, the Cyber Security team would be notified, and the **Cyber Response Plan,** in coordination with the **Disaster Recovery Plan** would be activated.

4. Crisis Management/Emergency Response

4.1. Crisis Response

Crisis Management Team (CMT)

As soon as an incident is confirmed to meet the criteria to be defined as a crisis, the Crisis Managment Team (CMT) should be established. The CMT takes over the strategic management and direction of the company for the incident. The CMT members should have sufficient authority to allow for immediate, urgent decisions to be made, taking into account the potential liability of the incident. It is important the CMT remains small and is comprised of members who will contribute specific technical knowledge of the incident, reducing the risk of the team becoming too large and ineffective.

Emergency Response Center (ERC)

The Emergency Response Center (ERC) may also be established to help coordinate the tactical response of the company. Lines of business affected by the incident should be represented by a member who can provide clear and concise information on the tactical objectives their business unit is taking in response to the incident. The ERC will also coordinate any needs for information or resource requests throughout the incident.

The objective of the Emergency Response Center (ERC) is to enable business units to carry out efficient incident response, independently as well as jointly, with all other involved parties, to support all measures to restore critical services. The ERC follows the guidelines set forth by the Federal Emergency Management Agency (FEMA) and National Incident Management System (NIMS).

The ERC shall be:

- Scalable for different incident types and involved organizations
- Adaptable to any type of incident
- Able to integrate different incident response organizations and involved parties
- Flexible to the evolution of the incident and outcome of incident responses

To fulfil these tasks, an ERC shall include:

- A command and control structure
- A command and control process
- The resources necessary to implement the command structure and process

Activation Triggers

Frontier has identified activation triggers that would mandate an activation of the CMT/ERC. These triggers will be agreed upon by the Incident Commander, in coordination with the ERC Region Lead. The activation phase begins with select trigger points that signify different levels of trouble volume, or when significant damage to a facility has occurred. During this phase, EventCon checklists will be utilized to direct efforts to protect life, property, and operational stability. Security over the area is established, when necessary, by local support services, such as Police and Fire Departments enlisted through existing regional and state mechanisms.

[redacted]

[redacted]

4.1.1. Response Phases

Corresponding to the predefined strategic and tactical command structure, Frontier has categorized a scale of incident severity levels. This is in order to implement, as soon as reasonably practicable, the appropriate level of command and control. Disasters will be determined based on geographical scope and anticipated impacts.

[redacted]

[redacted]

[redacted]

[redacted]

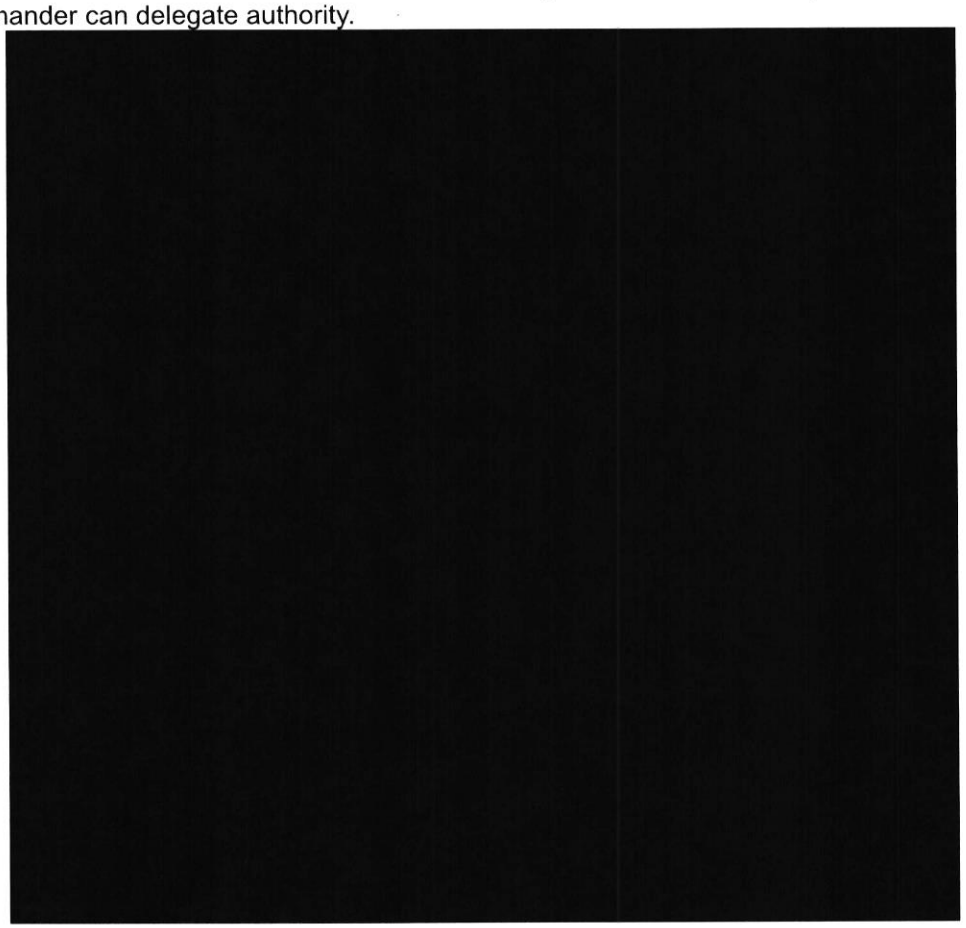
EventCon Checklists

EventCon checklists are incident/event management checklists established within each business unit for actions that take place at certain phases of response within an incident.

EventCon 0 - Business As Usual/Training/Testing Occurs
EventCon 1 - Preparedness
EventCon 2 - Activation
EventCon 3 - Recovery

4.2. Command and Control

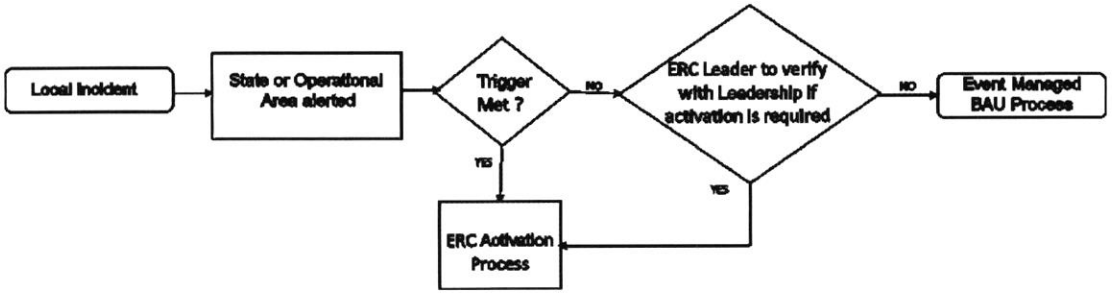
The Command and Control Structure shall be organized in such a way that the Incident Commander can delegate authority.



Frontier has a command and control process which is ongoing and includes the following activities:

- Observation;
- Information gathering, processing and sharing;
- Assessment of the situation, including forecast;
- Planning;
- Decision-making and the communication of decisions taken;
- Implementation of decisions;
- Feedback gathering and control measures.

The command and control process is not limited to the actions of the incident commander but also applicable to all persons involved in the incident command team, at all levels of responsibility.



4.3. Roles and Responsibilities

Roles and Responsibilities of business unit organization during an incident are as follows:

Command Staff

[redacted]

General Staff

[redacted]

4.4. Emergency Communication

Frontier will coordinate appropriate communication depending on the incident/event. During emergencies, communication is managed by Frontier's Crisis Management Team (CMT), in coordination with Corporate Communications and the Joint Communications Team. These teams ensure all initial and on-going communication is shared with the public, its customers, its employees, and the media. A continuous schedule of communication will depend on the extent of the incident/event and will be shared with the public and the media, as appropriate.

Joint Communications Team

Frontier has an established Joint Communications Team, which is made up of department personnel responsible to handle both staff and customer communication during an emergency. Upon activation, the Joint Communications Team will convene to determine a single, unified message is delivered to both staff and customers. The team is led by Frontier's Corporate Communications Department.

Emergency Mass Notification System

Frontier manages a multi-channel, geo-targeted mass communications platform which is used to alert all staff within the vicinity of a disaster or emergency. The emergency communication system can also be deployed to activate emergency response personnel before, during, and after a disaster, as well as conduct employee wellbeing checks following an emergency.

Federal, State and Local Communication

When an outage occurs, Frontier has designated representatives responsible for communicating with Federal, State and Local partners. The Continuity and Crisis Management Team activate the Emergency Response Center and coordinate with state and local emergency management officials. Frontier has the capability to send local representatives to public utility or county emergency management offices for enhanced situational awareness and collaboration. Frontier's Regulatory Team is responsible for communication to the state commissions.

Customer Communication

When an outage is detected, Frontier sends SMS communication to impacted customers covering the lifecycle of the outage event. If there is not a mobile telephone number on file, an auto-dialer call is made using the customers BTN on file.

First point of contact is a proactive outage notification that is sent at the time the outage is identified.

> Frontier: *"We're working to resolve an outage affecting service in your area. No need to contact us; we'll keep you updated as we work to resolve the issue and will let you know when your service is restored. You can also check the status of your services on Frontier.com/outage."*

Subsequently, the customer is updated via SMS/auto-dialer with outage updates. First update is sent 2 hours after the initial notification; then every 6 hours until the outage is resolved. Once resolved, the customer will receive a notification that the outage has been resolves and services should be back up.

> Frontier: *"Great news, we've resolved the outage and your service is up and running. You may need to restart your router/modem by pressing the power button or unplugging it from the wall. Please allow up to 5 minutes for the device to restart. AUTOMATIC MESSAGE - DO NOT REPLY."*

Media Reporting

Only authorized personnel from Frontier Communications should communicate in any form with the media. This includes, but is not limited to, phone, texts, blogs, and/or posting messages online regarding any incident or disaster related to Frontier.

Refer to **Frontier's Crisis Communications Plan** for additional information.

5. Emergency Restoration Priorities

Telecommunications Service Priority (TSP) Program

The Federal Communications Commission (FCC) established the TSP Program to provide priority treatment of national security and emergency preparedness telecommunications services. Frontier is required to provision and restore services with TSP assignments before non-TSP services. TSP provides for priority treatment for provisioning and restoring voice and data telecommunications service that:

- Serve our national security leadership;
- Support the national security posture and U.S. population warning systems;
- Support public health, safety, and maintenance of law-and-order activities.

Frontier's Emergency Response Center (ERC) focuses efforts on high-priority restoration and repair first, such as Public Service Answering Points, E911 Service, TSP circuits and services, hospitals, government facilities, and similar locations. Many activities to restore critical services can and will occur simultaneously. Should there be a competition for recovery resources, the following order of restoration guidelines will be followed:

1. Communications necessary to manage the event recovery
2. TSP Services
3. Essential Government Services
4. Public Safety Services
5. Network Infrastructure
6. Priorities of Federal, State, and Local governments
7. Other Services

5.1. Restoration Priority

Frontier will dispatch personnel outside normal business hours if necessary to restore TSP services assigned a restoration priority of 1, 2, or 3. Frontier is required to dispatch personnel outside normal business hours to restore TSP services assigned 4 or 5 only when the next business day is more than 24 hours away. Frontier is required to convey the TSP assignment to subcontractors and interconnecting carriers. Frontier is responsible for verifying the restoration priority assigned, ensuring the information is correctly recorded on the service record.

5.2. Provisioning Priority

If Frontier receives more than one Emergency TSP service request from customers, Frontier will provision them in order of receipt. The customer is immediately liable to pay the prime service vendor any authorized costs associated with provisioning the service within a shorter than standard interval.

5.3. Disaster Recovery Priority

When resolving conflicts, the restoration or provisioning of TSP services follows the below sequence:

1. Restore TSP services assigned restoration priority 1.
2. Provision Emergency TSP services assigned provisioning priority E.
3. Restore TSP services assigned restoration priority 2, 2, 4, or 5.
4. Provision TSP services assigned provisioning priority 1, 2, 3, 4, or 5.

Frontier Response / Outside Aid

Frontier deploys all personnel to recovery efforts following a disaster/storm. If the scope of work exceeds the levels for local personnel, Frontier has procedures to handle priority incidents with relief workers and has the capability to activate mutual aid contracts with vendors to bring in additional staffing to address the disaster.

Support Services

Frontier will manage any outside aid response in accordance with the policies and procedures outlined in its Relief Worker process. Accommodations and access to equipment and supplies will be handled at the local level by the appropriate Operations Director or Local Manager.

5.4. Federal TSP Annual Service Reconciliation

TSP Reconciliation is upon request by the Department of Homeland Security. This process requires a verification of records that involves comparing Frontier Communication's TSP service information with the TSP Program Office's TSP database and resolving any discrepancies.

5.5. E911 Restoration Priority Procedures

Frontier has also adopted the **911 Compliance Manual**, which contains 911 operating procedures that must be followed to ensure compliance with the FCC 911 regulations and requirements.

5.6. Documented Medical or Life-Threatening Condition, Disability, or Elderly Customers

If a customer is documented as a medical/life-threatening condition customer, Frontier will flag them manually and will prioritize these customers in the dispatch process.

Medical emergencies are allowed in all properties based on local business practice, and in some states, it is tariffed. Customer must provide letter on Doctor's Office letterhead or State Board of Health with the following information:

- State registration number or licensed physician;
- Name and address of seriously ill person;
- Any services beyond local exchange service that may be necessary to reach customer's doctor and, that absences of such services would be a serious risk of inaccessibility of emergency medical assistance; and
- Signature of licensed physician or public health official certifying illness or medical emergency.

5.6.1. Medical Emergency Accounts - Overview and Processing

The purpose of a medical emergency account notation is to signal Plant Service Center of service repairs and outages associated with residential customers that have health conditions requiring minimal interruptions of access to Frontier's services.

IMPORTANT NOTE: Medical emergencies are applied to the customer's account for one year from the receipt date of the medical provider's certification.

New York Certification: Frontier runs a semi-annual bill message in June and December informing customers how to seek priority medical emergency status.

Important information about priority medical status
Customers with a physician-verified health condition, such as a heart condition or asthma, may sign up for Frontier's priority medical emergency status. Customers who submit a completed medical certification will receive priority handling with respect to service installation and repair. Frontier will restore service of customers with priority medical emergency status at all hours, consistent with the medical needs of the customer and personal safety of utility personnel. For further information or to enroll, customers can go to Medical Emergency Priority Status Overview | Frontier or contact customer service at 1-800-921-8101.

Annual Certification
A letter/document must be received from the customer's medical provider ***annually***, certifying that the medical emergency exists, and that Frontier service is essential to the customer. If the customer would like a copy emailed or mailed to their billing address, the Frontier version of the form can be requested. Staff would visit The Hub Task - Inquire - Low Income Programs/Offline Mailing (ftr.com) for this option. The letter or document must contain the following information:

- Medical provider's state registration or license number (not required in MN) (An authorized user with Power of Attorney is permitted to assist or submit a medical certification by a medical provider).
- Name and address of Frontier customer.

- Name, signature of licensed physician or public health official (nurse or physician's assistant) certifying customer illness or medical emergency and date.
- Optional: Any services beyond local exchange service that may be necessary, and that absence of such services would be a serious risk of inaccessibility of emergency medical assistance.
- Customer should be instructed to mail the letter/document to the Frontier correspondence address.

IMPORTANT NOTE: If the customer is requesting assistance with a past due account due to a medical condition, the customer must speak with a Collections Agent. Staff are directed to follow the Collections Medical exemption process Collections - Medical Override (MED) Treatment Type (ftr.com).

5.6.2. Services for Customers with Disabilities

Call Procedure:

- Hearing or speech impaired customers, using either a Telecommunications Device for the Deaf (TDD) or a computer keyboard can call the Frontier Customer Center Disabilities (FCCD) number 1-877-462-6606.
- Customers can also dial 711 to be connected with a Telecommunications Relay Services Communication Assistant. Hearing person will give communication assistant calling number, called number and type of call. Communication Assistant will complete the call and will act as a translator from TDD to voice and voice to TDD for the duration of the call.

Access Availability:

- Dual Party Relay Service (DPRS) will give the hearing and/or speech impaired telephone user communication comparable to that of the hearing/voice telephone user. Service is available 24 hours a day / 7 days a week.
- Types of calls provided: DPRS shall only complete intrastate calls. Calls may be placed person-to-person and station-to-station.
- Types of calls handled by DPRS include:
  - Non-coin sent paid
  - Third Party
  - AT&T Card or other telephone credit card
  - Collect
  - Call Limitations
- Types of calls not handled by DPRS include:
  - 976 calls
  - DIAL-IT 900 service
  - Weather and other recorded announcements
- DPRS will make every effort to handle calls to 911 and other emergency calls. This service is offered to our customers at no extra cost. Calls will be billed according to the rate period in existence at the time the call is placed.

Certification:

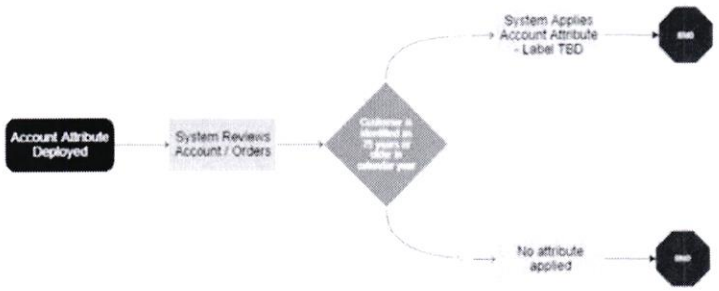
- Customer must be certified in writing as hearing or speech impaired by licensed physician, otolaryngologist, speech-language pathologist, audiologist, or authorized representative of official **'State'** agency as having hearing or speech disability. Pre-existing conditions establishing the impairment of hearing or speech, such as those which qualify a person with a disability for Social Security benefits on the basis of total hearing

impairment, or for use of facilities of an agency for persons with hearing or speech impairment can also be used.

5.6.3. Medical Expedites - Elderly Attribute

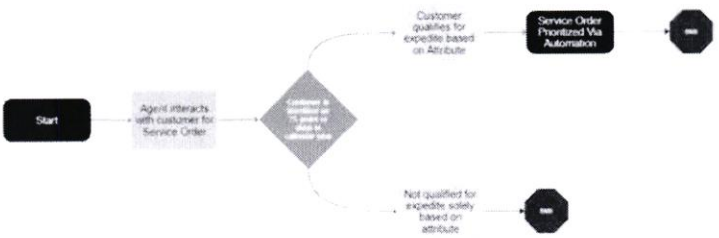
[redacted]

Attribute application



Attribute Trouble Ticket Escalation

Attribute Install Order Escalation



5.7. VIP (Emergency) Organizations Hazardous Conditions Repair Process

Public Safety, Law Enforcement, and other emergency organizations require a quick, efficient avenue to report trouble to Frontier Communications. VIP organizations are defined as emergency and safety agencies which may report trouble requiring immediate resolution, such as a pole or cable down in the road. Emergency organizations have been advised to call the established numbers for hazardous conditions repair. Examples of these organizations include:

- Police Departments and other law enforcement agencies
- Fire Departments
- Public Utilities
- Local Managers

5.8. Public Reporting of Hazardous Conditions

The public can make a report to Frontier at any time during a disaster if damage is identified. To report damages to poles, downed wires/cable, or other hazardous conditions, the public can dial 1-877-486-5667. For other customer service reported outages, the public can dial 1-855-981-4544.

To report 911 service issues, the public can dial 1-877-245-3511.

6. Florida

Rule 25-18.020

6.1. Plan Content Requirements

Rule 25-18.020 (5) Emergency Response and Storm Restoration Procedures and Protocols.

Each communications services provider must provide a copy of its emergency response and storm restoration procedures and protocols to the Division of Engineering.

(a) The procedures and protocols must include the following:

1. A description of the communications services provider's procedures and protocols for communicating with federal, state, and local emergency operations officials; ***Refer to Section 4.4 Emergency Communications***

2. A description of how the public can contact the communication services provider to report issues with its poles, such as broken poles, downed overhead facilities, or obstructed vegetation; and ***Refer to Section 5.8 Public Reporting of Hazardous Conditions***

3. A description of the communication service provider's procedures to repair and replace damaged poles and overhead facilities, including protocols for coordinating with public utilities, through emergency response and storm restoration efforts.

A ***Hurricane Preparedness and Response Plan*** includes the following elements:

- storm monitoring,
- emergency governance,
- standard operating procedures for emergencies,
- business unit preparedness plans,
- asset preparation,
- asset inventory,
- contractor and vendor lists,
- recovery/restoration efforts, and
- plan testing.

6.2. Commission Filing Requirements

Rule 25-18.020 (5)

(b) If the communications services provider makes changes to its emergency response and storm restoration procedures and protocols, the communications service provider must file the updated emergency response and storm restoration procedures and protocols with the Division of Engineering within 30 days of the change.

(c) Every three calendar years, each communications service provider must notify the Division of Engineering in writing that it has reviewed its emergency response and storm restoration procedures and protocols.

6.3. Damaged Pole and Overhead Facilities Repair and Replacement Procedures

Following a storm event, Frontier will conduct a facilities damage assessment and will work in conjunction with other pole owners, electric utilities, and/or third party attachers to determine the appropriate entity to lead the repair or replacement of infrastructure and the order of preference for repairing aerial facilities. If Frontier owns a damaged pole with no electric utility facilities on it, Frontier will replace the pole and reattach its serial facilities. Once completed, Frontier will notify other attachers that they are permitted to move their cables to the new pole. If Frontier owns a damaged pole that also has electric utilitiy facilities attached, or if Frontier has aerial facilities on a damaged pole that it does not own, Frontier will wait for notification from the electric utility that the pole has been replaced and Frontier is permitted to reattach its aerial faciltiies. In a major storm event impacting electric utility-owned poles, the electic utility will coordinate replacement and broadly notify impacted attachers once rebuilding is compelted in a designated area. Upon notificaiton, Frontier will proceed with reattaching to the electric utility poles thorughout the area.

6.4. Emergency Contact Information

Contact Name	Operational Area	Contact Number	Contact Email
[redacted]	Regulatory	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
	911 PSAP Trouble Reporting	[redacted]	
[redacted]	Central Office Operations	[redacted]	[redacted]
[redacted]	Field Operations	[redacted]	[redacted]
[redacted]	Field Operations	[redacted]	[redacted]
[redacted]	Field Operations	[redacted]	[redacted]
[redacted]	Outside Plant	[redacted]	[redacted]
[redacted]	Outside Plant	[redacted]	[redacted]
[redacted]	Outside Plant	[redacted]	[redacted]
[redacted]	Outside Plant	[redacted]	[redacted]
[redacted]	Liaison to Hillsborough Co EOC	[redacted]	[redacted]
[redacted]	Liaison to Pasco Co EOC	[redacted]	[redacted]
[redacted]	Liaison to Polk Co EOC		[redacted]
[redacted]	Liaison to Manatee Co EOC	[redacted]	[redacted]
[redacted]	Liaison to Sarasota Co EOC	[redacted]	[redacted]
[redacted]	Laision to Pinellas Co EOC	[redacted]	[redacted]

7. Plan Exercising, Testing, Training and Maintenance

The Continuity of Operations Plan will be tested annually. Enhancing capacity for emergency response must occur in all areas of the business. Training and exercises should include a variety of practical activities and include different business units. Effective exercises test capabilities of personnel and equipment. Exercises test the weaknesses in procedures and equipment, but at the same time should be basic enough to allow inexperienced staff to learn the emergency response functions.

A comprehensive training and exercise program will allow the organization to:

- Identify gaps in processes and procedures
- Identify opportunities to integrate public and private stakeholders
- Identify areas of cross-training
- Training or technology advancement opportunities

A minimum of one (1) training exercise will be held annually, simulating a storm or other activation trigger incident. Staff involved in the training will receive notification in advance of the exercise date. Frontier will make every attempt to include external partners in the exercise.

Business Continuity Operations Leadership Team members will assist in training the elements of their business continuity plans. Training shall be developed as appropriate for different levels of employee's involvement in the recovery process.

Following an exercise, after action reviews will be completed to capture any gaps in the process and allow for development plans to be put in place. Effectiveness of the program will be led by the Continuity and Crisis Management Team.

Maintenance

This Plan is considered a living document and should be updated as major changes occur within the organization that have an effect on critical departments and/or the IT infrastructure designed to support these departments and/or the designated team members that are assigned specific tasks for assessment, recovery and/or restoration within both areas. The BC Operations Leadership Team are responsible for this comprehensive maintenance task for each of their business units. The overall Plan maintenance will be conducted by the Cotninuity and Crisis Management Team.

8. Review and Revision Process

On an annual basis, the BC Operations Leadership Team ensures their business continuity plans undergoes a formal review to confirm incorporation of all changes. Each activation should trigger a Plan review with after action improvement items being added to processes included in the Plan. Any revisions will be reviewed by the Business Continuity Sponsor within the organization for functional and accurate process review.

An overall annual review of this Plan will be conducted by the Continuity and Crisis Managment team.