(NY) Frontier Communications Business Continuity and Crisis Management Plan

Reviewed: 03-DEC-2024

PUBLIC VERSION

Table of Contents

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 facilities.

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

Strategies are in place for failover and data replication for applications which include:

- Daily data replication between data centers.
- Remote mirroring to an internal/external site.
- Daily remote vaulting of required tape/disk data.
- Hot failover equipment for specific open systems/applications between data centers.

Internal Network & Operations

- Data centers are designed to be fully redundant. Each data center has dual switches that provide ethernet connections and service routers. Each router has a connection into the network. Circuits are designed to allow data traffic to flow seamlessly from the main data center to the failover site. Data centers are geographically separated.
- Diversity is in place for much of the network that allows for auto-rerouting of customer traffic if the primary or secondary paths are impacted. For instances where there are no paths, immediate triage/investigation is completed to determine opportunities for reroute.

Emergency Supply Inventory

- Frontier has necessary emergency equipment and material staged in various warehouse locations nationally to maintain a minimal level of service during a disaster. Frontier's Logistics Department manages warehouses and inventory and helps coordinate the deployment of requested materials as soon as the area has been deemed safe for entry. Logistics has relationships with vendors/contractors who can supply emergency equipment, water, and deliver material to address outages and necessary repairs.

- Frontier maintains a supply of spare circuit cards to support switching, transport, and data networks, as well as additional tools to address outages. Equipment is stored in warehouses that are geographically separated to ensure continuity.
- Generators are fixed on major sites and tested on a monthly basis. Portable generators are available and located throughout the region for immediate deployment. Alarms received from the Network Operations Center prompt the deployment of generators.
- Fuel contingency plans are established and maintained by Frontier's Fleet Department and contain procedures for coordinating resources with outside vendors who would support bulk fuel deliveries and mobile dispensing equipment. For localized emergencies, fuel trailers are available for mobilization to the affected area.

Emergency Staff

- Frontier has access to internal and external personnel to cover any increased demand. Contracts are maintained across the footprint for construction and installation & repair resources to ensure access to flexible workforce, as needed.
- Internal performance metrics are used to drive the restoration of broadband services within 48 hours.
- In case of major disaster, Frontier delays all scheduled installation work and lower priority work to focus local resources on isolating and restoring service to impacted customers.
- Should Frontier have a service emergency requiring immediate action, the following will be put in place:
    - Minimal service requirement report will be generated to manage service orders and tickets,
    - Current interval levels will be monitored and adjusted, as needed,
    - Movement of non-critical customer intervals out to accommodate for critical customer service emergencies,
    - Capacity requirements tracking in order to forecast additional workforce needs through overtime, construction, and contractors.

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 Management 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.

<u>Frontier has identified the following triggers which would indicate an activation:</u>

1. Natural Disaster
2. Damage to Premise

3. Loss of Utility Supply
4. Cyber Attack/Loss of IT Records
5. Disclosure of Sensitive Information
6. Labor Strike
7. Act of War/Terrorism/Sabotage
8. Pandemic
9. Global Supply Chain Interruption

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.

Frontier deploys 3 phases of incident response:

Phase 1 - Monitoring - This phase is implemented when a potential impact is expected to disrupt business operations. Monitoring is completed by the ERC Region Lead. This phase may also include early communication with specified teams in order to control crisis communications or begin the preparedness stages of operations. There may be times where the impact is unplanned and immediate, and the level of response results in an activation.

Phase 2 - Activated - This phase establishes incident objectives and resolving unmet needs of business units in the response phase of an emergency. During this phase, regular meetings are held with business unit leaders to share information and other situational awareness regarding the status of the emergency and determine any additional resources that are required to successfully respond to the emergency. Contingency operations are implemented, contracted services are coordinated, and recovery plans have been activated. Crisis communications is in full force during this phase.

Phase 3 - Recovery - This phase tracks all business unit activity to report restoration timelines to commissions or municipalities. Recovery may take weeks to complete, depending on the outcome of damage assessments and the need to restore certain equipment. Crisis communications may continue during this phase for any outstanding areas of impact.

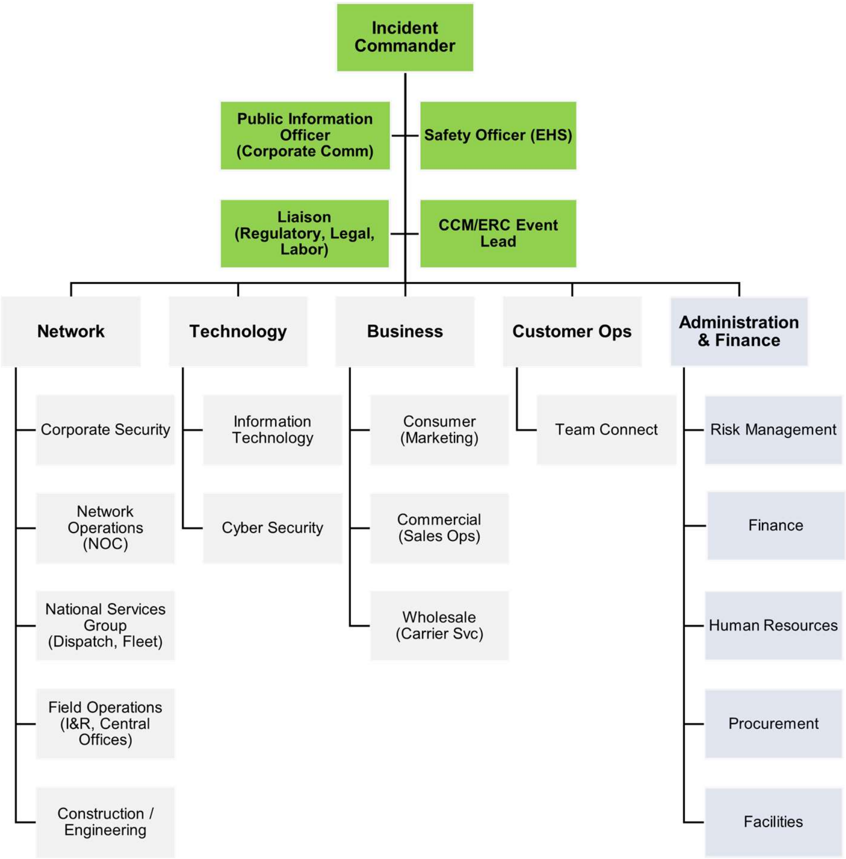
EventCon Checklists

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

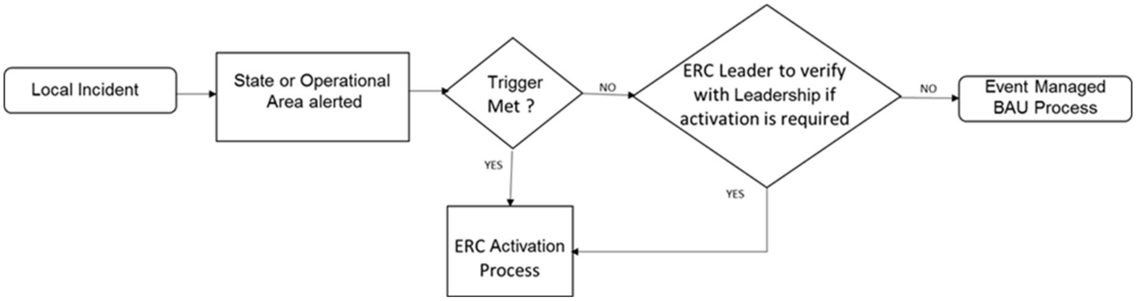
The Command and Control Structure shall be organized in such a way that the Incident Commander can delegate authority.



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.


Local Incident
State or Operational Area alerted
Trigger Met ?
NO
YES
ERC Leader to verify with Leadership if activation is required
NO
YES
Event Managed BAU Process
ERC Activation Process

4.3. Roles and Responsibilities

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

Command Staff

Incident Commander (SVP of Business Function or Corporate Security Officer) - The Incident Commander position will be led by the appropriate organizational SVP or the Corporate Security Officer, depending on the incident. The IC has overall responsibility of the incident and is the lead point of contact for team members during an emergency business situation.

ERC Lead (Continuity & Crisis Management) - The ERC Lead coordinates activation and planning of incident management activates, supporting the Incident Commander. The ERC Lead is responsible for establishing command schedules, conducting ERC meetings when necessary, collecting and disseminating information during the incident, assisting in coordination of resource requests, and cooperating with external agencies and municipalities.

Information Officer (Corporate Communications) - The Information Officer serves as the conduit for information to and from internal and external stakeholders, including the media or other organizations seeking information directly related to the incident or event. The Information Officer is the lead for the Joint Communications Team, coordinating a consistent message both internally and externally.

Liaison Officer (Regulatory, Legal, Labor) - The Liaison Officer may vary depending on the incident or event and is the individual responsible for communication with other agencies or organizations.

Safety Officer (Environmental, Health & Safety) - The Safety Officer monitors safety conditions and develops measures for assuring the safety of all assigned persons during an incident or event.

General Staff

Administration and Finance - This section is responsible for managing financial, administrative and cost analysis aspects of an incident or event. This section manages contracts and vendors, completes insurance requirements, manages the status of Frontier buildings, and provides logistical support for the incident or event. Administration and Finance is broken down into 5 branches to include: Risk Management, Human Resources, Finance, Procurement, and Facilities.

Business - This section supports the Consumer and Commercial needs of the business during an incident or event. Teams create and distribute relevant information to both customers and wholesale carrier partners. This section may also support emergency sales orders during an incident.

Customer Operations - This section is responsible for communication to all Frontier customers during an incident or event and consists of national and overseas based call center operations. Through a web-based platform, state-mandated rights of customers affected during an incident or event is communicated.

Network Operations - This section coordinates response and recovery efforts during an incident, reports on customer and 911 outages, conducts damage assessments, and coordinates with local police and fire departments, public utilities and emergency management agencies for restoration priorities. Network is broken into 5 branches to include Operations

(Field and Central Offices), Construction/Engineering, National Services Group (Fleet/Dispatch), Network Operations Center and 911 Support, and Corporate Security.

Technology - This section is responsible for monitoring all cyber, software/hardware, and connected systems within the company. This section supports internal staff access needs during labor events and interruptions through the management of the Disaster Recovery Plan.

Joint Communications Team - This team is comprised of those business units who manage communication to Frontier's customers, employees, the public and the media. The Joint Communications Team is led by Corporate Communications.

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/text communication to impacted customers covering the lifecycle of the outage event. Email notifications are sent for the initial outage communication and at the time of restoration.
First point of contact is a proactive outage notification that is sent at the time the outage is identified.
Email message example: *"We've confirmed there's a service outage in your area. We're working to resolve the issue and estimate it to be completed within the next 8 hours. Don't*

worry – we'll keep you updated as we work to address the problem and let you know once your service is restored. You can continue to check the status of it here or on the MyFrontier app."

SMS/text message example: "*Hi, it's Frontier. There's a service outage in your area. We realize this may impact you, so our team is working hard to restore service and expects the service to be restored by (time, date)*."

Subsequently, SMS/text outage updates are sent every six hours until the outage is resolved.

SMS/text message example: "*Hi, it's Frontier. We understand this outage might be impacting you and are working hard to fix it. There's no need to call us. We'll send updates as we make progress. Service is expected to return by (time, date). You can also check the status anytime at Frontier.com/outage."*

Final notification is sent at the time the outage is resolved and services are restored.

Email message example: "*Great news! We've fixed the outage at your address, and everything is expected to be back up and running. You may have to restart your router/modem by pressing the power button or unplugging it from the wall. Please give it up to 5 minutes to restart. If you still have issues, visit our Help Center (hyperlink) or chat with us (hyperlink)*".

SMS/text message example: "*Great news, we've resolved the outage and your service at (address) 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.*"

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.

Customer Restoration Priority (Including but not limited to)	Priority Level
Hospital or Emergency Medical Facilities	1
Main Utility and Communications Facilities	1
Water and Wastewater	1
Emergency Shelters	1
Fire, Police, Paramedics and Rescue Facilities	1
Emergency Management Offices	1
Main Flood Control Structures	1
Nursing Homes and Dialysis Centers	1
Support for Other Critical Government Functions	1
Prisons and Correctional Facilities	1
Communications (radio, TV, etc.)	1
Large Employers and Other Key Customers	1
Event Specific Concerns	1
Other Government Buildings, Schools, and Colleges	1

Customers Providing Key Products and Services	1
Residential developments with large elderly populations or other similarly vulnerable establishments as coordinated with county officials	1
Telecommunications Service Priority Customers	1
Life Support and Other Special Needs Customers	1

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.

	Class 1	**Class 2**	**Class 3**
# of Customers Affected (e.g., < 50, > 1,000)	Refer to Section 4		
Geographic Scope (e.g., street, town, county)	Refer to Section 5		
Expected Time to 100% Restoration	Refer to Section 5		
Type of Damage (e.g., storm or other emergency events)	Refer to Section 4		
Company Personnel Alone or Company and Supplementary Non-Company Personnel Required	Refer to Section 4		
Other			

	Electric Utility	Telephone /Cable Company	Emergency Management Agency	Public Works Agency
Name and Title of Company Personnel Responsible for Coordination	National Grid: 800-642-4272 NYSEG: 800-572-1131		NY state of Emergency Management josephp@co.jefferson.ny.us	
Job Functions to Coordinate	Power restoral, joint phone poles		Regulatory requests	
Methods or Means of Coordination	Phone, email		Phone, email	

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 Communications provides a dedicated 911 Customer Care Center (CCC). All critical Frontier 911 customers have a dedicated 911 Service Manager for the area in which the customer is located and is available 24 hours per day to assist in any service matter. As a matter of Frontier's Standard Operating Procedure, all major 911 service issues are automatically escalated to your designated 911 Service Manager.

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

Frontier identifies and applies medical expedites to customer accounts that are 75 years and older.

[redacted]

[redacted]

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

VIP / MT Repair Toll Free Numbers:

- All States including an option for CA & MN **877-486-5667**
- California **877-677-0730 (special CA line for specific municipalities)**
- Connecticut **844-834-4361**
- Minnesota **888-671-6122** (special MN line for customers to call)

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. New York

State Statutes & Rules - Case 22-M-0180, 16 NYCRR 603.05(a) and 16 NYCRR 603.6

603.5 Service Interruptions

(a) Each service provider shall establish and implement procedures regarding the construction, operation, and maintenance of its network, which are intended to minimize service failures, including but not limited to cable cuts, sudden increases in traffic, employee absences, fires, severe storms, and floods and which are intended to maintain, to the extent practical and reasonable, continuous operation of its service in the event of commercial power loss [except where such power is provided by the consumer].

603.06 Major Service Provider Emergency Contingency Plans

(a) This section applies only to Major Service Providers as defined in this section. Major Service Providers are required to incorporate the requirements of this section into the emergency contingency plans pursuant to section 603.5(b)(1). These requirements are primarily intended to ensure adequate response for storm and storm-like emergencies; however, some aspects of these additional requirements will have application to virtually all events noted in section 603.5(a) and should be used accordingly.

(b) Definitions:

(1) Major Service Provider. A Major Service Provider is defined as (i) any service provider that is an incumbent local exchange provider, or (ii) any facilities-based service provider with over 500,000 access lines, or (iii) a certificated 911 service provider as defined in section (b)(2).

(2) 911 Service Provider. A 911 service provider is any entity that is certified under the Public Service Law that provides 911, E911, or NG911 capabilities such as 911 call or information transport, selective routing, ALI, ANI, or the functional equivalent of any of those capabilities., NG911 core services, directly or indirectly intended for or to a Public Safety Answering Point (PSAP), statewide default answering point, or appropriate state, regional or local 911 authority, or that operates facilities that directly serve a PSAP or state, regional or local 911 authority. For the purpose of these rules, a provider "directly serves a PSAP" if it: hosts a selective router or ALI/ANI database; provides functionality equivalent to NG911 capabilities and core services; or is the last service provider facility through which a 911 trunk, SIP connection, or administrative line passes before connecting to a PSAP.

(e) Sensitive and confidential information. Any Major Service Provider may request that the commission designate as confidential any information required to be submitted in emergency contingency plans. Confidential information may include, for example, names and telephone numbers of its employees and outside contact persons, any information which, in the opinion of the service provider, could compromise its ability to protect the network against vandalism, terrorist acts, or other potential threats to the network. Such requests shall be filed in accordance with section 6-1.3 if the Commission's regulations.

(f) Commission review and approval. Upon receipt and review of emergency contingency plans or amendments files pursuant to this Part, the commission may require any such Major Service Provider to modify such plans or amendments or otherwise prescribe conditions for compliance with the requirements of this Part.

6.1. Plan Content Requirements

Each Major Service Provider's emergency contingency plan shall provide a current, detailed description of its service restoration plan and shall include the following information:

1. Table of Contents

2. Introduction. A statement of the purpose, policies and objectives of the plan.

3. Emergency classifications. ***Refer to Section 4 - Crisis Management/Emergency Responses, Section 4.1.1 - Response Phases, and Section 5.3 - Disaster Recovery Priority***

- Specify classifications of a storm emergency or other emergency by severity and the criteria or guidelines used for determining each classification. The guidelines should include, but need not be limited to,
    - the geographical scope of the emergency,
    - the estimated time required to restore service to business-as-usual levels,
    - the type of expected damage to the provider's network, i.e., from a storm or other storm-like emergency, and
    - an indication of whether company personnel alone or company and supplementary, non-company personnel will be needed to repair network damage.

4. Emergency response training program. ***Refer to Section 7- Training & Exercises***

- State the Major Service Provider's program to provide emergency response training for those personnel assigned service restoration responsibilities that are different from their normal duties.
    - Identify person(s) responsible for managing and evaluating the effectiveness of the program.
    - Include procedures for conducting a minimum of one (1) annual storm drill simulating a response to either a storm, or storm-like emergency that would be classified at the highest or next highest level of severity.
    - State the extent to which any personnel outside the company may be involved in a storm drill.
    - Include as well, provisions for critiquing the drill procedures and for giving staff a minimum of 2 weeks' advance notice of a scheduled drill.

5. Advance planning and preparation. ***Refer to Third Parties Appendix***

- Specify the on-going actions that the Major Service Provider expects to take throughout each year to plan and prepare for an emergency. The procedures should include the corporation's plans to stockpile emergency restoration tools and supplies.
    - State also, provisions for the preparation and distribution of literature or other forms of communication with information on customer storm preparations. Such information should address storm survival without electric power, and/or telecommunications service, and safety precautions regarding electrical hazards such as downed wires and the use of portable generators.
    - State procedures to update at least semiannually, its list of contact persons, with titles, addresses, phone numbers and other pertinent data for the following:

    - All provider personnel assigned service restoration responsibilities;
    - External storm restoration vendors and contractors, additional (non-NY) internal staffing;
    - All life support and other special needs customers;
    - Medical facilities and other human services agencies;
    - Print and broadcast media;
    - State, county and local elected officials, law enforcement, 911 dispatching centers, and emergency management offices; and
    - Critical equipment and supply vendors.
  - At least annually, in accordance with the requirements of section 603.6(c)(2), the corporation shall verify that the preceding data is current. At least semiannually, the corporation shall issue updated lists of known changes to its employees that have plan implementation responsibilities,

6. Emergency anticipation. ***Refer to Section 4.1 - Activation Triggers***

- Identify the preparatory measures corporate management would implement in anticipation of a potential storm or network emergency expected to affect the service territory within hours or days.
- Identify the criteria under which key personnel with service restoration responsibilities would either be notified of an impending emergency or deployed to assigned areas, and any special precautions that would be taken.

7. Service restoration procedures. ***Refer to Section 5- Emergency Restoration Priorities***

- Provide the corporation's procedures for mobilizing its personnel, materials, and equipment in order to survey system damage and implement measures to ensure timely, efficient and safe restoration of service to customers in areas damaged by a storm or other storm-like emergency or loss of commercial power or telecommunications service.
- Procedures need to identify restoration priorities to ensure that restoration time is minimized, while ensuring critical customers' needs are met.
- Include a listing of the priorities for service restoration among customer groups in these procedures, including TSP customers.
- For those severe emergencies when field damage assessments are needed, describe the methods for making, within 24 hours, broadscale preliminary assessments of the nature and extend of system damage based on rapid surveys of damaged areas and other data sources, and for making, within 48 hours, more detailed estimates of system damage based on systematic field surveys.
- Describe how field reports of system damage will be integrated with damage reports or indicators from other sources, such as customer call-ins, to make a responsibly accurate assessment of system damage and reliable projections of the personnel, equipment, materials and time that will be needed to rapidly and safety achieve service restoration goals in all damaged areas.
- Provide procedures for deploying company and contractor crews to work assignment areas, monitoring crew activity, reassigning crews as necessary, and releasing crews, both under centralized and decentralized command modes.
- Describe the methods and means that will be used to communicate with damage survey crews and service restoration crews.
- Identify procedures for coordinating company restoration procedures with the restoration efforts of electric utilities, other telecommunications and cable television service providers, and with state and local emergency management and public works agency efforts.

- State the procedures to coordinate efforts with the service territory's electric utility provider for restoring electric service to priority telecommunications facilities.

8. Personnel responsibilities. ***Refer to Section 4.3 - Roles & Responsibilities, Section 4.2 - Command & Control***

- Provide a narrative and chart of the organization and operational assignments of personnel to be mobilized for each emergency classification identified.
- State areas of management and supervisory responsibility and functions to be performed at each emergency classification level.
- Include procedures for contacting and managing all personnel assigned duties under the emergency restoration plan at both the corporate and operating division level.

9. Customer contacts. ***Refer to Section 4 - Communication Process, Section 5 - Emergency Restoration Priorities***

- Provide the Major Service Provider's procedures and facilities for handling the extraordinary volume of customer calls that are normally placed during emergency events.
  - Include a description of the type of messages that may be given to all-in customers regarding projections for service restoration or other pertinent information.
- State the overall corporate goals for answering customer calls during emergencies including, but not limited to
  - Plans for staffing levels
  - Number of positions activated
  - Use of pre-recorded messages
  - Means of providing updated information to customer service representatives, and
  - Means of monitoring calls received and answered at the Major Service Provider's customer service centers.
- State procedures to coordinate efforts with the service territory's electric utility provider for restoring electric service to priority facilities.
- State procedures to contact and restore telecommunications service to special needs customers such as the elderly, vision-impaired, hearing and speech-impaired, mobility-impaired and human service agencies representing these customers, along with policies for handling inquiries and request for assistance from them.

10. Communications.

- Provide the Major Service Provider's procedures and facilities for establishing and maintaining both pre and post storm external communications exchanges regarding damage and restoration progress with customers in general, human service agencies, the media, the Department of Public Service, the Division of Homeland Security and Emergency Services and other state agencies, county and local governments, emergency response services, and law enforcement agencies, etc.
- Include identification of any dedicated phone lines, the designation of any special company representative to act as liaison with government entities, and any special provisions that may be required for dealing with critical facilities.
- State the Major Service Provider's planned frequency of communication updates to the media.

11. Outside Aid. ***Refer to Section 5.3 Disaster Recovery Priority***

- State the corporate policy and criteria governing conditions under which requests for service restoration aid from other service providers, contractors, government agencies or others would be made and the procedures to be followed in obtaining outside aid.

12. Support services. ***Refer to Section 5.3 Disaster Recovery Priority***

- Describe the actions that will be taken, the department and personnel responsible for implementing them, to sustain and support restoration crew activities. These shall include:
  - vehicle management
  - crew and vendor accommodations (e.g. housing, food, transportation)
  - distribution of warehouse supplies (e.g. materials, tools, equipment needed in the restoration process)

6.2. Commission Filing Requirements

Plans shall be filed annually by **January 31.**

(g) Compliance with emergency contingency plans.

(1) Each Major Service Provider shall comply with the guidelines and practices set forth in its effective emergency contingency plans. Each Major Service Provider shall comply with any additional emergency contingency plan requirements that may be imposed by the commission.

(2) Within 30 days following completion of service restoration in an emergency where the restoration period exceeds 3 days, and if requested by the Director of the Office of Telecommunications or the Director of the Office of Resilience and Emergency Preparedness, a Major Service Provider shall file with the commission as assessment by requirement of each required Major Service Provider emergency contingency plan action against its actual preparation and system restoration performance.

(3) Within 60 days following completion of service restoration in an emergency where the restoration period exceeds 3 days, as requested by the Director of the Office of Telecommunications or the Director of the Office of Resilience and Emergency Preparedness, a Major Service Provider shall file with the commission a full review and assessment of all aspects of its preparation and system restoration performance, including compliance with required Major Service Providers emergency contingency plan actions.

(4) Within 60 days following completion of service restoration in an emergency where restoration exceeds 3 days, a Major Service Provider shall identify instances where, under emergency conditions, it modified its storm response from that in the filed emergency contingency plan to the extend required to restore service in a safe and efficient manner and the circumstances that caused such modification.

6.3. Commission Notification Rules

Initial reports should be made within 1 hour after the outage is first recognized by the provider, reports should be to a designated Department staff member via a "live" telephone conversation. Status reports should be provided on any ongoing major outage. The first status report should be provided within 3 hours of the initial report.

6.4. Commission Specified Outage Level Response, Recovery or Restoration Strategies

- A service problem or newsworthy event caused by, for example, a major storm, flood, fire, job action, sabotage, civil unrest, death, a cyber or physical security breach at a service provider's building(s), or other event;
- A service problem affecting public access to 911, operator services, Telephone Relay Service, police, fire departments, or emergency medical services;
- A service problem that disrupts the delivery of Emergency Alert System (EAS) provided emergency information to the public. Excluded from this are temporary EAS equipment outages as permitted under the rules of the Federal Communications Commission;
- A major network node and/or telecommunications traffic concentration point (e.g. head-end, central office, toll office, packet switch, router) failure lasting more than 5 minutes;
- Extensive network congestion;
- Any failure (e.g. outside plant cable damage) affecting 1,000 or more subscribers;
- A service problem affecting a public transportation terminal, hospital, national defense installation, or large residential and commercial building or complex, or other major customer.

6.5. Emergency Drill Requirements

This plan must be tested at least once a year through ERC activations, ERC monitoring events and/or exercises internally and externally with public utility companies and local governments who would normally be included in service restoration responses.

*Refer to **Section 7***

6.6. Emergency Contact information

Contact Name	Operational Area	Contact Number	Contact Email
Cassandra Knight	Regulatory	[redacted]	[redacted]
Aimee Pidgeon	Business Continuity	[redacted]	[redacted]
	911 PSAP Trouble Reporting	877-245-3511	
Emmett Larry	Central Office Operations	[redacted]	[redacted]
Tom Rayeski	Central Office Operations		[redacted]
Scott Manion	Central Office Operations	[redacted]	[redacted]

Chris Cornell	Central Office Operations	[redacted]	[redacted]
Lawrence Washbon	Field Operations	[redacted]	[redacted]
Michael Williams	Field Operations	[redacted]	[redacted]
Nathan Barber	Outside Plant	[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 Continuity and Crisis Management Team.

Name	Title	Responsibility	Contact Information
Daryl Hayes	Specialist- Business continuity	ERC leader (East region)	[redacted]

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 Management team.

Appendix A. Associated Applications/Technologies

There are no Associated Applications/Technologies.

Appendix B. Associated Sites (Data Center, Network Center, Critical Warehouse)

There are no Associated Sites (Data Center, Network Center, Critical Warehouse).

Appendix C. Associated Departments

There are no Associated Departments.

Appendix D. Associated Department Business Functions

There are no Associated Department Business Functions.

Appendix E. Associated Relationships

There are no Associated Relationships.