AT&T Business Continuity & Emergency Management

Introduction and Overview

This document outlines the strategies and procedures AT&T uses to plan, respond, and recover from events that may have potential impact to the AT&T Network. It provides an overview of AT&T's business continuity and emergency management programs, and:

- Cybersecurity
- Disaster prevention/fire prevention and code compliance
- Restoration priorities
- U.S. Government interface and partnership

Business Continuity

Planning for and responding to crises is something that AT&T performs on a routine basis. The company has extensive experience responding to a wide variety of situations, from hurricanes to floods, to power outages, work stoppage contingency planning, and man-made disasters. AT&T has a global team of experts who practice responses to these types of scenarios several times each year.

AT&T has a team of industry-leading, certified, and experienced business continuity experts engaged in AT&T's internal business continuity management program. This team requires that key business processes have documented business continuity plans that are updated and exercised on a predetermined schedule.

Exercises are designed around specific scenarios to test the plans' viability and capability. Plan development and exercise execution are based on the concept of continuous improvement with the focus on maintaining business operations. As part of that planning, AT&T has performed an extensive corporate-wide risk assessment and has implemented incident response and contingency planning on several broad fronts.

In 2015, AT&T became the first telecom service provider to be certified under the new international Business Continuity Management standard (ISO 22301:2012) for the Department of Homeland Security Voluntary Private Sector Preparedness Program (PS-Prep™). The PS-Prep™ recertification demonstrates AT&T's continued commitment to be equipped to resume business operations and product/service delivery to our customers in the vital hours and days after a disaster strikes. In the event of a disaster or emergency, we are prepared to quickly resume network traffic and field customer calls in the communities that we serve.

March 2017

In addition to ISO 22301, AT&T's business continuity management program is also:

- Certified by the Cellular Telecommunications & Internet Association (CTIA) as part of its Business Continuity/Disaster Recovery Program since 2004
- Aligned with the Disaster Recovery Institute International (DRII) Professional Practices since 2004
- Aligned with the National Incident Management System (NIMS) as suggested by the U.S. Department of Homeland Security since 2004
- ISO 27001 certified for information security since 2010
- Aligned with the Business Continuity Institute (BCI) Good Practice Guidelines since 2011

Event Management Framework (EMF) & Emergency Management Operations (EMO)

The purpose of AT&T's Event Management Framework (EMF) is to provide an incident command structure that is used to manage planned or unplanned events that impact AT&T business processes, assets, or people. The EMF defines AT&T's Emergency Management Operations (EMO), the delineation of the different entities within the EMO, and the roles and responsibilities of those entities. The EMF and the resulting EMO are an integral part of our business continuity program.

EMO Response Teams

The EMO structure establishes multiple response teams which are focused on the restoration of key business processes. These processes cover technology operations and infrastructure, customer sales and service capabilities, provisioning, maintenance, and other key areas.

The AT&T Global Emergency Management Center (GEMC) performs corporate activities during a significant event, including:

- Accounting for employees, personnel impact assessment, and work-ready status.
- Crisis communication and message management.
- Consolidated event status reports by business unit including the identification of assistance requirements, impacts on employees, customer service, and business operations.
- Corporate resources needs assessment including the engagement of senior management, if required.
- Business unit emergency management activities during a significant event, including:
  - Accounting for employees
  - Recovery of business processes and operations
  - Interfacing with customers
  - Prioritization and movement of resources

- Network emergency management activities during a significant event, including:
  - Assessment of network damage
  - Prioritization of network response
  - Provide resources and internal status

Disaster Severity Levels

The disaster severity level matrix defines events by the severity of the damage to AT&T technology assets and/or personnel. The table provides examples of the magnitude of damage, as well as examples of the associated impact for each of the four levels. It also identifies the network organization responsible for command and control of a response.

	Level 4	Level 3	Level 2	Level 1
Description	Local service disruptions that can be restored by local teams. Teams follow normal, BAU procedures.	Outage exceeds the restoration capacity of local teams.	Regional incident requiring coordination of multiple disciplines/response organizations.	Major event requiring the coordination and deployment of extensive resources.
Examples	Cable cuts, power failures, localized hazardous conditions.	Minor or regional flooding, small tornadoes.	Earthquakes and widespread weather hazards (hurricanes, multiple tornadoes, major flooding).	Cybersecurity attacks, national security attacks, major health incident, severe earthquakes.
Technology Impact	Localized, single-element failures.	Impacts more than one technical group or geographical area.	Multiple, large-scale incidents requiring dedicated teams for 3CP (Command, Control, and Communications).	Impact is so severe that enterprise management required.
Incident Command	Impacted Business Units, Local Response Center (LRC)	Event Management Technical Reliability Center (EM-TRC) and LRCs	Global Emergency Management Center, Emergency Operations Center (EOC), Global Technology Operations Center (GTOC)	Executive Command Council (ECC)

Disaster Severity Level Matrix

Network Emergency Management Centers

AT&T Network Emergency Management Centers are designated either as an Emergency Operations Center (EOC) or as a Local Response Center (LRC). These centers are elements of AT&T's Network Emergency Management Plan and are activated during events when local damage assessment or network recovery exceeds business-as-usual (BAU) capabilities. Depending upon the severity of the event or the potential impact on the business, these centers may be required to operate 24-hours a day for the duration of an event.

Emergency Operations Centers

AT&T has Emergency Operations Centers (EOCs) with defined geographic responsibilities in the United States. The EOCs are strategically placed in AT&T's Central, Northeast, Southeast, and West regions. There are numerous Local Response Centers supporting the United States, Puerto Rico, and the U.S. Virgin Islands.

The EOC members are key corporate organizational representatives who, during a widespread and/or multi-state disaster, work together to:

- establish restoration priorities
- make provisioning decisions
- provide overall event command and control

The response team members are empowered to develop strategies and to make decisions for the organizations they represent.

Local Response Centers

Local Response Centers (LRCs) are usually focused on a specific territory and will handle local emergency events that exceed BAU capabilities. They provide command and control for damage assessment and field restoration efforts. If the disaster or emergency is regional, or if multiple LRCs are activated, an EOC will be activated and will take overall control providing prioritization of AT&T resources across the impacted area.

Activation and Notification
The decision to activate an LRC or EOC is made by the AT&T Emergency Management Center (EMC) leadership team.

Alternate EOC and LRC Succession Planning
Each LRC and EOC has an emergency management center plan that allows an LRC or an EOC to transfer its work and responsibilities to a neighboring center. This provides for continuity of the command and control functions if a primary center's capabilities are compromised.

EOC/LRC Communications
Each EOC and LRC is equipped with redundant communications channels to guarantee continuity of communications to and from the EOC/LRC. These tools include wired communications from redundant central offices, wireless communications, satellite communications, and high frequency radios. AT&T is a NCS SHARES member.

EOC/LRC Emergency Power
Each EOC and LRC has emergency power sources that will automatically carry the center's critical load to ensure continuity of operations throughout the emergency event and to maintain EOC/LRC integrity.

EOC/LRC Security
Access to an EOC or LRC is allowed only to EOC/LRC team members and other EMO authorized personnel. Identification badges are issued upon entrance, worn by all personnel while in an EOC/LRC, and are surrendered to an EOC/LRC manager when personnel leave.

Global Technology Operations Center

The AT&T Global Technology Operations Center (GTOC) (formerly known as the Global Network Operations Center [GNOC]) monitors and proactively manages the entirety of the AT&T Network (domestic and global) twenty-four hours a day, seven days a week on a business-as-usual (BAU) basis. It is the overall command and control center for the AT&T Network. Any information about the AT&T Network that is communicated, internally or externally, is validated by the GTOC acting as the single "voice" of the network. The EOCs and LRCs provide event status information to the GTOC as part of the overall network assessment.

Exercises

Exercises are designed to validate various aspects of AT&T's disaster response capability and to identify any processes requiring further development or training. Each EOC/LRC is required to exercise annually. Critiques are conducted immediately following each exercise. Findings and recommendations are shared with the appropriate management teams and improvements are integrated into updated plans.

Types of EOC and LRC Exercises
Tabletop exercises are usually the smallest in scope and are the easiest to conduct. Participants are presented with a scenario and specific simulated emergency situations without time constraints. The exercises are designed to elicit constructive discussion among participants as they examine and resolve problems based on existing disaster response plans.

Functional exercises involve external "simulators" who transmit messages concerning simulated emergency events to the participants. Participants determine what action should be taken and convey decisions and directions back to the simulators.

Cybersecurity

The AT&T Chief Security Office (CSO) establishes policies and requirements, as well as comprehensive programs, to incorporate security into all facets of AT&T's computing and networking environments. The AT&T program implements security policies through a rich set of initiatives, processes, and procedures administered by the AT&T security organization worldwide. The program is certified to meet the ISO/IEC 27001:2005 Information Security Management Standard.

These program initiatives are executed on an ongoing basis by each region and are supported by global network security teams. The goals of the program are to protect AT&T's Global Network, service offerings, and all internal/customer information and resources as outlined below.

- Support technology services for global incident response, network-based security services, and managed security services, assist account teams with customer engagements, and perform applied security research for emerging services.
- Collaborate with Business Units to ensure that AT&T employs the highest standards in protecting both AT&T and customer's assets, evaluate threats, determine protective measures, create response capabilities, and ensure compliance with best security practices.
- Maintain a comprehensive global Information Security organization dedicated to the security of the AT&T global network and its service offerings. AT&T is committed to protecting its customers' and its own information and resources from unauthorized access, disclosure, corruption or disruption of service.

Disaster Prevention

AT&T uses many techniques to prevent disastrous events from impacting customer service. Many of these techniques are proprietary and are not described in this document. However, some portions of our disaster prevention program are either required by state/local codes or are federal/state mandates, including:

- Fire Prevention Program/Code Compliance
- Federal Interface Requirement
- Business Continuity Planning
- Pandemic Planning/Management
- Cybersecurity Programs

Fire Prevention Program/Code Compliance

The AT&T Fire Protection Program protects our employees from fire hazards and safeguards AT&T central office facilities from major service interruptions due to fire. The program establishes preventative measures, proper emergency response processes, and recovery mechanisms.

The AT&T Fire Safety Program and Emergency Plan (OP130) requires that each AT&T Network organization follow the rules, standards, codes of the National Electric Safety Code (NESC), National Fire Protection Association (NFPA), American National Safety Institute (ANSI), American Society for Testing and Materials (ASTM) and government safety laws, codes and mandates as they relate to fire protection and life safety.

Restoration Priorities

AT&T follows special procedures to restore service after an event causes widespread and/or severe damage or when other emergency conditions exist. Our ability to effectively restore service may require the prioritization of restoration efforts to support the emergency response.

When a city, county, or state has an order declaring a major disaster, an extraordinary situation or other emergency, the restoration and provisioning of telecommunication services will be done in accordance with the National Response Plan and the FCC's Telecommunications Service Priority (TSP) procedures.

AT&T begins coordinated restoration prioritization as soon as safety and working conditions permit. The period required for restoring service throughout an impacted area, state, or region will vary widely due to differences in the location and severity of an event, the complexity of our network infrastructure, central office equipment impacted, and the type of services provided in an area (e.g., broadband, wireless). In general, in the absence of any additional priority service requirements, service restoration will be met in the following sequence:

1. Telecommunications Service Priority (TSP): priority repair and installation of critical infrastructure services as required by the FCC's TSP program.
2. Public Safety: communications to essential community agencies (e.g., E-911, fire, police, hospitals) not already addressed by the TSP program.
3. Restoration of the full community and outside service using permanent and/or temporary facilities (whichever is the most expedient and practicable).

Telecommunications Service Priority

AT&T fully supports the FCC's Telecommunications Service Priority (TSP) program. It establishes the legal basis for service providers to act, when authorized by the FCC, on a priority basis in the provisioning and restoration of services supporting NSEP mission requirements. TSP is applicable to services such as dedicated private lines, access lines, dial-tone lines, high-capacity digital systems, and trunks between another carrier's switching or wireless nodes. Many activities to restore critical services will occur concurrently and may be influenced by the direction of government agencies.

Government Sponsored Priority Service

Government Emergency Telecommunications Service
Government Emergency Telecommunications Service (GETS) is a calling card program supporting wireline services that is available to federal, state, local, and other government-authorized National Security Emergency Preparedness (NSEP) critical users in the public or private sector. GETS calls receive priority treatment in the network and have a higher probability of completion when a disaster occurs or in situations that result in wireline network congestion.

Wireless Priority Service
Wireless Priority Service (WPS) is a dial program supporting wireless services that is available to federal, state, local, and other government-authorized NSEP critical users in the public or private sector. AT&T Mobility supports NSEP critical users' needs for priority wireless call processing. AT&T Mobility manages all WPS related operations and administration in accordance with National Communication System guidelines. WPS capability can be enhanced when used with GETS priority treatment.

U.S. Government Interface and Partnership

AT&T has full-time U.S. National Coordinating Center (NCC) representation for the National Security Emergency Preparedness (NSEP) programs. As the primary interface for the enterprise, the representative is involved in matters associated with national security and emergency preparedness response. AT&T NSEP/NCC representatives work regularly with the:

- National Communications System (NCS)
- Federal Emergency Management Agency (FEMA)
- Federal Department of Homeland Security (DHS)
- DHS National Cybersecurity and Communications Integration Center (NCCIC) Unified Coordination Group (UCG)

AT&T maintains partnerships with federal agencies as well as with many state, county and local governments, which serve to reinforce and strengthen AT&T's emergency preparedness programs. This strategy includes information sharing, mutual exercises, and often leads to joint methods of understanding (MOUs) and Disaster Recovery Plan (DRP) interdependencies with government and other critical infrastructure segments.

