EMERGENCY SUPPORT FUNCTION 2 - COMMUNICATIONS

CEMP - ANNEX IV DOCUMENTATION

08/03/2021

Jim Loter

Date

Acting Chief Technology Officer
Seattle Information Technology Department

Curry Mayer
Curry Mayer (Aug 3, 2021 16:49 PDT)

08/03/2021

Curry Mayer, Emergency Manager

Date

Note: This Emergency Support Functions (ESF) is part Annex IV of the Comprehensive Emergency Management Plan (CEMP) and this version includes the 2021 revision. Seattle Information Technology Department (ITD) acts as the current ESF Coordinator and collaborated with many partners for respective input.

TABLE OF CONTENTS

TABLES

FIGURES

No table of figures entries found.

1. STAKEHOLDERS

Table 1

PRIMARY AGENCY	ESF COORDINATOR
Seattle Information Technology Department	Seattle Information Technology Department

Table 2

SUPPORT AGENCIES	
Auxiliary Communications Services	City of Seattle Departments

2. INTRODUCTION

2.1 Purpose

Electronic communications and information technology are a vital component to preventing, preparing for, responding to, and recovering from incidents, both natural and human based. This document describes the technology and telecommunications support the City of Seattle's capabilities, and how those capabilities will be managed during time of the incident.

This document is an external plan as defined by the City of Seattle Emergency Management Program Planning Policy and follows the maintenance process, which includes a method and schedule for evaluation and revision, as described therein.

2.2 Scope

This document applies to the departments, organizations, or agencies with a lead or support role for this ESF. It discusses the requirements, business approach, and objectives of ESF 2 communications role and information technology including programs and operations before, during, and after an incident.

ITD is charged with management, operations, and maintenance for most of the City government's telecommunications and information technology infrastructure. ITD is responsible for coordinating operational services for the telecommunications and information technology infrastructure.

ITD is also charged with support for most IT applications (e.g., computer-aided-dispatch, work management) used in City government. These applications are dependent upon the information technology infrastructure (data centers, computing systems, and communications networks) being operational.

ITD's Department Director has the additional responsibility as the Chief Technology Officer (CTO) for the City, and, as such, sets standards which all departments are expected to follow when acquiring and implementing technology and telecommunications. During cybersecurity incidents, other incidents, and Emergency Operations Center (EOC) activations, the CTO and the CTO's designees in the EOC direct the activities and coordination with other departments which support telecommunications and information technology for City government.

At this time, ITD manages Seattle's portion of the King County emergency radio system. The countywide system supports more than 16,000 radios used by all police and fire agencies in King County as well as a number of other general government agencies and functions. This system also supports interoperable communications with responders in Snohomish County and portions of Pierce County.

3. SITUATION

3.1 Emergency Conditions and Hazards

The City of Seattle, its citizens, and transportation infrastructure are exposed to a variety of natural and human caused disasters such as severe weather, earthquakes, and acts of terrorism. The Seattle Hazard Identification and Vulnerability Analysis (SHIVA) identifies Seattle's hazards and examines their consequences so we can make smart decisions about how best to prepare for them. It provides information regarding potential impacts of hazards to the people, economy, and the built and natural environments of the City of Seattle. The SHIVA provides a foundation for all the City of Seattle's disaster planning and preparedness activities. The list of all natural and human-caused hazards includes: Emerging Threat, Geophysical Hazards, Biological Hazards, Intentional Hazards, Transportation and Infrastructure Hazards, and Weather and Climate Hazards.

The information below supplements the SHIVA with certain specifics relevant to telecommunications and information technology. Communications have been developed to support all components of response, continuity of government and operations, and recovery plans, and redundancies have been provided in case of failure of primary systems. The Emergency Management Program has considered all operating environments and the systems that may be impacted based on hazards.

- All disasters. During any major disaster in the region, the region's normal communications networks will be overloaded – these include the public switched telephone network (PSTN), cellular telephone networks, and internet service provider (ISP) networks. Generally, the City's internal telephone, radio, and data networks are segregated from the public networks and will operate normally. Normal traffic is designated for internal government communication; exceptions would be out-dialing or inbound traffic from outside the City. Generally, the PSTN and public cell phone networks will continue to operate, but only a small percentage of telephone calls will be connected. Internet service may also be slowed during the initial stages of the disaster. City employees may continue to try and use the cellular network and email for low-priority and non-emergency communications. City employees should use e-mail functions of their smart phone and similar devices and the text messaging features of their cellular phones which should continue to operate, although somewhat slowed during the initial stages.
- Earthquake. When an earthquake occurs, the ground motion will potentially continue for some time. All critical radio IT assets (servers, radio transmitters, etc.) are earthquake braced and generally in modern facilities built to withstand most anticipated earthquakes. A serious earthquake, however, could damage some interconnection paths for networks (e.g., microwave, fiber optic cable). The City's network designs include multiple redundant paths and technologies such as SONET and microwave with self-healing rings for critical sites. This design concept will help ensure service is available. ITD has completed building out a secondary data center site outside the geographic threat zone of the primary data center with all redundant critical infrastructure systems in place. This will provide the City with a fully operational data center in response to earthquake damage within the City of Seattle and help in recovery of critical information technology systems. The primary data center site and the secondary data center have equipment located on base isolation pads. The buildings containing the data centers have full seismic retrofits and advanced security features with robust generator support.
- Cybersecurity Incident. Cybersecurity incidents vary in nature, complexity, and impact and include computer viruses and malware, ransomware, theft and corruption of data and system and network penetration and denial of service attacks. The nature of systems and technology subject to such incidents is increasingly complex and vast, including City-controlled computers

and networks as well as mobile phones, networked devices, sensors, and third-party services. ITD has a separate cybersecurity incident response plan administered by the City's Chief Information Security Office. This plan is designed to identify, mitigate, and respond to real threats. These incidents do not require EOC activation. However, a truly significant cybersecurity incident adversely affecting the control systems for the City's critical infrastructure, for example, would require EOC activation to address the physical and operational effects of the incident.

3.2 Cybersecurity incident coupled with terrorist attack.

It is possible that a terrorist attack (such as a CBRNE event) could be coupled with a cybersecurity incident adversely affecting the City's information technology systems, assets, operations, and/or infrastructure. Such incidents will require activation of the EOC to deal with the physical and operational incident and the City's cybersecurity incident response plan to address the systems, technology, and data.

As stated before, Seattle ITD is charged with management, operations, and maintenance for the majority of the City government's telecommunications and information technology infrastructure. ITD is responsible for helping ensure operational service for the telecommunications and information technology infrastructure. ITD will rely on its department operating center, the Information Technology Operating Center (ITOC), to assist in coordination of IT resources during response to an incident.

The City communicates life-safety notifications to the community in ways that can be understood, regardless of language, as a foundational part of response during incidents. Specific communications strategies have been developed to ensure notification to those with limited-English proficiency (LEP). Details can be found in the Alert & Warning Support Operations Plan.

The City's comprehensive incident response policies, strategies, and practices can be found in the City Emergency Operations Plan (EOP).

The City-specific operational procedures supporting response policies, strategies, and practices are maintained separately. Please refer to the Reference Section of this document, if applicable procedures have been identified at this time.

4. CONCEPT OF OPERATIONS

4.1 Organization

The EOC is organized using Incident Command System, which emphasizes concepts such as unity of command/coordination, modular organization, management by objectives, manageable span of control, etc. Under EOC Operations there are four branches; Police, Fire, Human Services, and Infrastructure.

The Seattle ITD's ESF 2 Coordinator staffs the Infrastructure Branch Director position if the EOC is activated in response to a cybersecurity incident; in other incidents the position supports the Infrastructure branch for communications and information technology services.

The ESF 2 Coordinator works closely with the other organizations and with outside private service providers for cell services.

During an EOC activation, the ITOC, in coordination with the ESF 2 Coordinator, assigns IT resources from the Seattle ITD to restore services.

The Seattle ITD supports the computer infrastructure components that provide emergency notification of staff and the public. These altering systems include a primary channel for the City's externally hosted WordPress blog (Alert.Seattle.gov). Other notification systems that are also supported by the computer infrastructure include the Emergency Notification System (ENAS) and various blog sites. These systems will be fully described within the Alert and Warning Support Operations Plan.

4.2 General Response

At the time the EOC is activated, the ESF 2 Coordinators and ITD Executive Team will be notified.

ITD's designated ESF 2 Coordinators will coordinate among themselves to determine who will report to the EOC initially and who will relieve the reporting individual.

The ESF 2 Coordinator will call in any additional roles that are required.

Seattle ITD's Director, in coordination with the ITD Executive Team and the ESF 2 Coordinator, will decide whether to activate the ITOC and will communicate their decision to the ITOC Operating Center Manager.

As on-call and EOC-reporting employees arrive at their designated locations, they will determine the status of technology systems and report the status of those systems to the ITOC Operating Center Manager. Priority of systems for status determination and repair are the following list:

- 800 MHz Public Safety Radio network;
- Wireless data network for first and second responders (provided by AT&T/FirstNet and Verizon);
- The City's telephone network;
- The City's data communications network including fiber and internet connections;
- Email;
- The City's website (seattle.gov); and
- The City's television channel (Seattle Channel).

After ascertaining the status of the City's IT assets and networks, the ITD Incident Commander will coordinate with the ESF 2 coordinator at the EOC and designate the priority for restoring IT networks and systems. The ITD Incident Commander will work with other appropriate employees and supervisors to direct resources as required.

Once ITD employees reporting to the EOC have established the complete operation of technology systems, the ITD Incident Commander can release those employees for other work restoring or maintaining critical IT networks and systems.

4.3 Public Safety Radio System Interoperability and System Redundancies

Seattle ITD manages Seattle's portion of the King County emergency radio system. The countywide system supports more than 16,000 radios used by all police and fire agencies in King County as well as a number of other general government agencies and functions.. Numerous redundancies are designed into the Public Safety Radio system to provide alternative means of communications in the case of failure of primary components. These redundancies are described within Section 6. Resource Requirements table.

An overall Tactical Interoperable Communications Plan (TICP) was established in 2005 and updated to specifically address system interoperability changes within the Public Safety Radio network. The TICP is for the Seattle Urban Area which includes King, and Snohomish Counties and the portions of Pierce County that are serviced by Tacoma Regional Network. This plan is intended to document what interoperable resources are available within the urban area, who controls each resource and what rules of use or operational procedures exist for the activation and deactivation of each resource. The TICP is used for interoperable operational communications across jurisdictions, disciplines, and various responder levels. This plan is developed to communicate both internally and externally with all Emergency Management Program stakeholders and emergency personnel while meeting the requirements of the National Incident Management System requirements. Radio system interoperability has been addressed in design of the network, development of the operating procedures and throughout the TICP Plan.

In addition to the Public Safety Radio network, Seattle City Light and Seattle Department of Transportation operate separate radio systems that provide additional radio communication capabilities to support their departments' operations.

Regional radio caches have been developed. These caches have been used across the urban area for various activations including the landslide in Snohomish County in 2013.

The Seattle urban area, including the Washington State Patrol, has created COML lists that are shared across the region. This aids in faster radio patching capability during an event.

4.4 Direction and Control

The direction and control for the ESF 2 in the field will be coordinated through the ITOC, which is led by Seattle ITD. This operating center, in coordination with the ESF 2 coordinator located at the EOC, is responsible for all information technology direction and control in the field during a disaster or other EOC activation.

5. RESPONSBILITIES

5.1 Prevention and Mitigation Activities

A detailed listing of the actions to eliminate or reduce the degree of long-term risk to life, property, and the environment to be taken by the departments, organizations or agencies with a lead or support role for this ESF. Many areas needing mitigation will be identified during the preparedness, response, and recovery phases of emergency management.

All City departments need to update their respective department Continuity of Operations Plans (COOP) so that the City's critical services are identified and the information technology systems and applications which are critical to operations are also identified. The systems and applications should have recovery time objectives listed as well as recovery point objectives. Each element is critical to be able to plan for system recovery and mitigation of the risk associated with losing the system.

5.2 Preparedness Activities

The ESF 2 lead role is to develop a command and control structure that when activated will ensure continuity of operations for telecommunications and information technology in support of the City government. The response activities section fully describes the structure that has been established. Activation of this structure during exercises and activations has increased overall preparedness within the various duty positions.

5.3 Response Activities

Upon direction of the CTO; or the EOC activation; or whenever requested by the EOC Director or the determination of a major incident that impacts Seattle IT's services or ability to deliver essential functions incident command will be established, the incident management team will be activated and the department operations center opened to ensure continuity of operations for telecommunications and technology in support of the City government. See Table 3 below which describes position responsibility.

The Radio Manager will ascertain the proper reporting location based on the nature of the incident. Some technical analysis and configuration of the radio system can only be supported from the radio network master site.

As many community members rely on non-verbal communication or have limited English skills, the City of Seattle will deliver key messages via Web, social media channels, AlertSeattle, and Seattle Channel, in a timely manner, to as many language groups as possible based on the City's Inclusive Outreach & Public Engagement (IOPE) practices and consistent with Title II of the Americans with Disability Act (ADA).

5.4 Recovery Activities

Disaster-related response and restoration can be very costly. While not all costs are reimbursable, it is in the City's interest to make best use of funding that may become available through federal agency programs, such as FEMA, and insurance.

To assist with this effort, departments, organizations, or agencies with a lead or support role for this ESF are responsible for tracking and documenting of actual and anticipated costs related to the incident. Costs should be tracked based on guidance from OEM or the home organization.

The department will provide recovery activities for the various information technology operational components, which are defined in (Section 6. Resource Requirements). The description defines the specific scope of recovery responsibility for the Seattle ITD. The support and maintenance section defines the support and maintenance for specific components that affect city-wide information technology operations.

Table 3

EOC Reporting Matrix for IT Support			
Duty Position	**Duty Location**	**Responsibilities**	**Designees**
ESF 2 Coordinator	EOC	Staff the ESF 2-Communications role. Coordinate response by ITD resources to support EOC missions.	Sr. Emergency Management Advisor Sr. Manager, Network & Communications Technologies ITSM Process Owner Disaster Recovery Program Manager Client Engagement Team
ESF 7 Logistics Section Seattle IT, Intake, or Resource Tracking Coordinator as assigned	EOC	Per Emergency Support Function 7 – Resource Support & Logistics assist with acquiring, intaking, and tracking information technology resources.	Finance manager and staff Client Engagement Team Advisor
Radio System Manager	EOC or radio system master site or designated location	Monitor and reconfigure the public safety radio network as required to keep it operational during the incident.	Radio Manager or Radio Shop Supervisor
Radio System Technician	Radio system prime site	Monitor and reconfigure the public safety radio network as required to keep it operation during the incident.	Radio Technicians (2)
Citywide PIO Team Responder	EOC	Participate in City PIO team activities at EOC.	ITD Public Information Officer
Public & Internal Information	EOC	Update the City's public website and InWeb using blogs, Ingeniux CMS, or SharePoint	Web Content Moderators/PIOs
Technology Support–Public	Virtual	Technical support for existing public web platforms and processes.	Digital Services staff
Technology Support-Internal	Virtual	Technical support for existing internal web platforms.	SharePoint staff

EOC Reporting Matrix for IT Support			
Seattle Channel Media Relations	EOC or Seattle Channel Studio	Manage broadcast-live or taped television from EOC or other locations with information from EOC incident commander, Mayor or other elected official or designees.	Seattle Channel Managers (2)
Seattle Channel Headend	Seattle Channel	Manage Seattle Channel end of EOC needs	Seattle Channel Staff (2)
Seattle Channel EOC Television Operators	Seattle Channel	Perform television operations related to camera operations.	Seattle Channel Staff (5)
EOC Technology Support Staffing	EOC	Report to EOC and immediately to ascertain status of all critical technology necessary to support EOC functioning. Repair systems or assist EOC responders as required. Employees will be released from EOC by ESF 2 Coordinator once the systems are determined to be operational.	Device Support Technician (1) Telephone Technician (1) Network Technician (1) On-call engineers: Messaging/Active Directory Services Server Operations Virtual & Data Infrastructure Internet/Network Security Engineer
CTO, ITD Director	ITD Offices, Seattle Municipal Tower EOC Policy Room or as identified by Mayor's Office	Ensures accountability and safety for all ITD personnel immediately after an incident. Designates and deploys channels to communicate with ITD employees during an incident. Serves on Mayor's Emergency Executive Board.	Chief Technology Officer Deputy CTO Collaboration & Workplace Technologies Deputy CTO Applications Technology Infrastructure Director
ITD Incident Commander	ITOC Operating Center, Seattle Municipal Tower; also can be located at the ITD Radio Shop, Western Data Center or in a virtual environment	Lead and manage the City of Seattle's cybersecurity incident response. Order, direct, and control ITD incident response resources and activities. Communicate with ESF 2 Coordinator to determine necessary department actions and resources to support response activities of Lead City Departments and EOC coordination priorities Prepare IT operational status reports.	Deputy CTO Collaboration & Workplace Technologies Deputy CTO Applications Technology Infrastructure Director Chief Information Technology Officer Chief Privacy Officer Sr. Manager, Frontline Support and Services

EOC Reporting Matrix for IT Support			
			Manager, Workplace Productivity and Automation Sr. Manager, Solution Desk and Service Management Sr. Manager, Digital Engagement & Collaboration Sr. Emergency Management Advisor Communications Infrastructure Manager Radio Communications Manager Platform Technologies Manager Network Services Manager Systems Operations Manager Telecommunications Manager

6. RESOURCE REQUIREMENTS

The City's communications infrastructure has the following components that are critical asset requirements for the City of Seattle.

Table 4

City Communications Infrastructure		
Component	**Description**	**Support and Maintenance**
Microwave	Microwave radio infrastructure connecting radio transmission sites. Provides backbone for 800MHz radio network but also carries some telephony and data.	First and second level support by ITD Radio Shop. SCL maintains some independent links. Vendors: Harris, for equipment and remote technical support.
Fiber	Over 550 miles of fiber optic cable reach almost every major and many smaller City facilities, including fire stations, police precincts, libraries and schools. Provides that backbone for telephone and data communications networks, plus some radio transmissions and traffic signals. Fiber network also supports numerous other public agencies including UW, Seattle Community Colleges, Seattle Public Schools, King County, KC Metro Transit, NOAA, FBI, US Coast Guard, WSDOT, and connections between the WA State EOC and EOC's in King, Pierce, and Snohomish Counties.	Engineering and first-level support by ITD Communications Infrastructure team. Fiber construction and repair by contractors under ITD management. SCL installs and maintains a connected network for electric network management. SDOT installs and maintains a connected network for traffic management purposes. Vendors: Prime Electric and Link Communications for fiber installation, repair.
Radio – 800 MHz Public Safety	Seattle operates a Motorola Smartzone radio network with 5 transmission serving the City and about 4400 mobile and portable radios used by Police, Fire, Public Utilities, and others. 25 simulcast frequencies and hundreds of talk groups. Three levels of redundancy: trunked operations, site trunking, failsoft. The Seattle network is a part of a linked and jointly operated King County network including more than 16,000 radios used by all police and fire agencies in the County.	First and second level support by ITD Radio Shop. Vendors: Motorola, for equipment and remote technical support.
Radio – TRIS	TRIS is the Tri-County Radio Interoperability System. TRIS was implemented in 2005 using a combination of federal funds and urban area security initiative funds. TRIS allows	First and second level support by ITD Radio Shop.

City Communications Infrastructure		
	some public safety answering points (PSAPs) to patch talk groups between these radio networks in the urban area: King County 800 MHz trunked, Snohomish Emergency Radio System (SERS), Tacoma 800 MHz radio, Port of Seattle 800 MHz radio, Washington State Patrol, and the Federal Integrated Wireless Network (IWN) which supports a number of DOJ and DHS agencies, including FEMA.	
Interoperable Communications Van	The Seattle Police Department acquired a communications van in 2005 which allows for interoperable wireless communications at an incident site. The wireless communications include multiple radio networks used by most government agencies operating in Seattle, interoperable switched using an Infinimode© switch. The van also has Wi- Fi, video and other capabilities.	First and second level support by ITD Radio Shop. ITD End User Support is responsible for Wi-Fi, and video capabilities.
Communications and command vehicles	Seattle Fire has a mobile command and communications vehicle. Seattle Police has multiple mobile precincts (command vehicles). These mobile command posts have both communications capabilities with radio, and computer/printer assets.	First and second level communications support by ITD Radio Shop. Information technology assets inside the vehicle supported by ITD Public Safety Applications teams.
Radio – 800 MHz SCL	Seattle City Light operates a four-channel radio network used by SCL crews and other operations. The network is active both in Seattle and the Skagit valley. About 400 mobile and portable radios.	First and second level support by SCL staff. Vendors: Motorola, for equipment and remote technical support.
Radio – 440 MHz Amateur radio and 462 MHz GMRS radio, Emergency Management	The Seattle EOC support volunteer radio system operated as auxiliary communications networks. These include a network of 146 and 440 MHz amateur radio repeaters, as well as a network of 462 MHz GMRS repeaters.	First and second level support by volunteers through the EOC. Support is provided through the ITD Radio Shop on an as-requested basis. Vendors: Motorola, for equipment and remote technical support.
Radio – 450 / 150 MHz Transportation	Seattle Department of Transportation operates a 450 / 150 MHz radio network for transportation crews with about 400 mobile and portable radios.	An SDOT employee oversees the system and does some first- level maintenance. Most installation and maintenance is accomplished by contractors. Vendors:
Radio - various	Various other special-purpose radio networks are installed and operated by various departments. For example, Public Utilities	Employees in the departments oversee contractors who maintain and install these

City Communications Infrastructure		
	operates a low-band network in its watersheds.	networks.
Telephone Network	The City operates a private telephone network composed of 18 PBX switches and over 12,000 telephone instruments at about 300 City business locations. This system is designed to operate even when the public and cellular networks are inoperative. The network operates largely on the City's own fiber optic cable network, but also uses City-owned copper cable plant, leased circuits, and data network infrastructure. Related services include automatic call distribution systems (ACD), interactive voice response systems (IVR), and voicemail.	First and second level support by ITD Telecommunication Engineering & Operations. Vendors: Avaya provides remote access technical support for PBX equipment. Fujitsu for SONET equipment and remote technical support.
Telephone Network Interconnection to Local and Long-Distance carriers	The City maintains connections to the public switched telephone network (PSTN) through two commercial providers: CenturyLink and Level-3. All Local trunks are provided via leased circuits. Level-3 circuits are transported from Level-3's Central Office to a City site via the City's SONET network.	First and second level support by ITD Telecommunication Engineering & Operations. Carrier service support provided by: CenturyLink and Level 3.
Data Network	The City operates a private data network which connects end user computing devices, data centers, and the internet. The network operates largely on the City's fiber optic cable network between buildings and uses fiber and copper for distribution within buildings. This data network supports a wide variety of computer applications used for emergency management, including electronic mail, computer aided dispatch, work management systems, etc.	First and second level support by ITD Network Engineering & Operations. Vendor support provided by Cisco on a remote basis.
Internet connection	The City provides internet connections through redundant, diverse internet service providers (ISP). Circuit connections are routed over fiber.	First and second level support by ITD Network Engineering & Operations Vendors: Western Data Center (WDC)---Cogent and Zayo; Eastern Data Center (EDC)—Level-3 and Zayo; Guest Wireless—Cogent and Comcast
Wireless data network—Internal City	The City provides secure internal wifi service and an open guest wifi service throughout Seattle Municipal Tower (SMT), Seattle	First and second level support provided by ITD Network Engineering & Operations.

City Communications Infrastructure		
wireless access points	Justice Center (SJC) and City Hall as well as other strategic sites in the City.	Vendor support provided by Cisco on a remote basis. ISP support provided by ISP vendors (see Component: Internet Connection above).
Wireless data network for mobile computing network	The City provides a wireless mobile computing infrastructure using LTE cellular technology. Access to the City network is provided via a leased circuit (backhaul) for Seattle Fire Department and Seattle Police, and via the City internet connection for other departments	Wireless support is provided by Verizon Wireless. Backhaul circuit support is provided by Verizon. City data network connectivity support is provided by ITD Network Engineering & Operations. ISP support provided by ISP vendors (see Component: Internet Connection above).
Cellular telephones	The City provides cellular service to over 2,000 users. The City primarily uses two service providers: AT&T and Verizon. ITD manages the City's relationship with the service providers, but the departments manage details of their own service effective 09/30/2016.	First level support by various business units. ITD End User Support provides vendor relations and coordination and enterprise level service outages. Second level support by service providers (AT&T and Verizon)
Text Messaging	Text messaging is available on standard cellular phones and smart phones.	Support provided by service providers.
Radio - 450 MHz Seattle Fire Department paging system	Seattle Fire Department operates a three site UHF simulcast alphanumeric paging system that provides alerting to belt worn pagers. The same infrastructure also provides back-up alerting to fire stations in the event of a failure of the Locution IP alerting network.	Support provided by ITD Radio Shop.
Paging (non- Fire)	The City provides access to a general paging service via SPOK Wireless (formerly USA Mobility). This service is for all non-Seattle Fire Department pagers. Pagers are managed via the ITD Radio Shop. Because this network is fully owned and operated by a commercial service provider, city staff are limited to managing paging devices and have no network support responsibility.	First level support provided by ITD Radio Shop. Infrastructure support provided by SPOK.
Electronic mail and Office 365	The City currently has over 13,000 active user email accounts.	First level support provided by ITD Enterprise Services.
WebEOC	ITD provides support of the WebEOC servers.	First level support provided by ITD Systems Operations.

City Communications Infrastructure		
Seattle.gov website global alert banner	There is a global banner that can be displayed across all Seattle.gov web pages. All communication via these channels is controlled by the JIC Supervisor.The Digital Services Team provides 24-hour technical support for public web platforms at the JIC. This requires a computer with browser and internet connection at the JIC. Additional Citywide Web Team staff support the JIC remotely and need access to a computer and internet connection particularly for a longer-term event.	First level technical support for public web platforms is supported by ITD Digital Services Team.
Department Websites	Communications staff provide incident updates to the public through their web pages with the Ingeniux content management system. All communication via these channels is controlled by the JIC Supervisor.	First level support provided by department communications staff
Department Blogs	Communications staff provide incident updates to the public through their blogs, including Alerts.seattle.gov, with the WordPress content management system. All communication via these channels is controlled by the JIC Supervisor.	First level support provided by department communications staff
Social Media	Communications staff provide incident updates to the public through their social media accounts. The Mayor's Office owns the Citywide social media accounts. All communication via these channels is controlled by the JIC Supervisor.	First level support provided by department communications staff
Department newsletters/listservs	Communications staff may provide incident updates to the public through newsletters and listservs. All communication via these channels is controlled by the JIC Supervisor.	First level support provided by department communications staff
InWeb	All communication via these channels is controlled by the JIC Supervisor.	

7. MAINTENANCE

This document is an external plan as defined by the City of Seattle Emergency Management Program Planning Policy and follows the maintenance process, which includes a method and schedule for evaluation and revision, as described therein. Lessons learned from exercises, special events, incidents, or disasters may result in a decision to evaluate portions of the documents ahead of the schedule.

ITD, as the ESF 2 Coordinator, has primarily responsibility for this document and will ensure it is evaluated as outlined in the schedule with updates and revisions being made to ensure guidance remains current. ITD will facilitate the evaluations in consultation and coordination with OEM.

Table 5

RECORD OF CHANGES			
DATE	TYPE	CONTACT	SUMMARY
March 25, 2021	Update	Dave Sutton	Administrative changes: Updated position changes from last ITD reorg; added EMAP-compliant verbiage.
August 7, 2018 July 26, 2018	Revision	C Kaku / L Eichhorn L Meyers	Completed revision. Document voted and approved by DMC and EEB. Significant changes to how ITD activates and manages a major incident that impacts the department's ability to provide information technology services and deliver its mission essential functions. This includes establishing incident command, activating the incident management team and opening its department operations center (ITOC).
December 2016	Update	V Wills L Meyers	Completed annual update.
May 2015	Update	K Neafcy	Completed annual update.

8. TERMS AND DEFINITIONS

Nothing identified at this time.

9. ACRONYMS

ACD: Automatic Call Distribution System
ADA: American with Disabilities Act
CBRNE: Chemical, Biological, Radiological, Nuclear, or Explosive
CEMP: Comprehensive Emergency Management Plan
CMS: Contract Management System
COOP: Continuity of Operations
CTO: Chief Technology Officer
EDC: Eastern Data Center
ENAS: Emergency Notification System
EOC: Emergency Operations Center
EOP: Emergency Operations Plan
ESF: Emergency Support Function
FBI: Federal Bureau of Investigation
ICS: Incident Command System
IOPE: Inclusive Outreach & Public Engagement
ISP: Internet Service Provider
ITD: Information Technology Department
ITOC: Information Technology Operations Center
ITSM: Information Technology Service Management
IVR: Interactive Voice Response System
IWN: Integrated Wireless Network
LEP: Limited English Proficiency
NOAA: National oceanic and Atmospheric Administration
OEM: Office of Emergency Management
PIO: Public Information Officer
PSAP: Public Safety Answering Point
PSTN: Public Switched Telephone Network
SERS: Snohomish Emergency Radio System
SHIVA: Settle Hazard Identification and Vulnerability Analysis
SJC: Seattle Justice Center
SMT: Seattle Municipal Code
SONET: Synchronous Optical Networking
TICP: Tactcal Interoperable Commnications plan
WAMAS: Washington State Intrastate Mutual Aid System
WDC: Western Data Center
WSDOT: Washington State Department of Transportation

10. REFERENCES

Washington State Intrastate Mutual Aid System

Detailed procedures, departmental plans, and other documentation are kept in hard-copy at the EOC, shared drive within the department, and a SharePoint site location.