

## Emergency Support Function (ESF) #2: INFORMATION TECHNOLOGIES

<b>ESF Activation Contact:</b> Cornell University IT Service Desk (607)255-5500	
<b>Primary Department</b>	CIT Support PH:(607)255-5500 Contact: Wyman Miles
	Office for Supply Management Services PH: (607)255-6694
	Cornell Facilities Services PH:(607)255-5322 Contact: Facilities Customer Service
	Cornell University Police PH:(607)255-1111
	Division of Human Resources PH:(607)255-3510
	University Communications PH:(607)255-7419
	COGENT (Internet)
	Finger Lakes Technology Group (Voice)
	Google (Student Mail)
	HyperReach (Emergency notification)
	ONE COMMUNICATIONS (Internet)

### I. Purpose

- a) This ESF lists the Cornell University departments and external agencies responsible for Cornell Information Technology (CIT) related response actions that may take place during an emergency.

### II. Scope

- a) Includes information technology networks including telephone and data.
- b) Includes information technology related services and applications including web and data servers, e-mail, administrative applications, academic related services and applications and other services provided to the Cornell IT user community.
- c) Includes the response to and recovery from a loss of information technology related services.
- d) Includes the delivery of additional information technology related services to support response and recovery operations with other response entities.
- e) May be activated by the Incident Commander to respond to incidents that are beyond the capabilities of the initial emergency response actions.

- f) May be activated to respond to incidents that overwhelm normal Incident Command response actions.

### **III. Situation**

- a) Emergency Conditions and Hazards
  - i) Cornell University information technology resources, including networks, hardware, and applications support a variety of University operations and business functions. Natural and human-causes can result in loss of these services.
  - ii) Certain resources and services are critical to campus emergency response and recovery operations.
  - iii) Certain resources and services are critical to campus business and academic operations.
  - iv) Cornell University may periodically experience emergency and disaster situations that will require response by University resources and outside agencies and the restoration of essential services. Potential emergencies and disasters include both natural and human-caused incidents.
  - v) See Cornell's Risk Assessment for a description of potential emergencies.

### **IV. Assumptions**

- a) Initial emergency response capabilities may be inadequate to contain or control the hazard.
- b) Information technology resources and services may be damaged or impacted by the hazard.
- c) The full extent of technical resources, both human and otherwise, may not exist solely within the central IT organization but may be required from other organizations within the University or from outside entities.
- d) Existing information technology resources and services may need to be supplemented to support campus emergency response and recovery efforts.
- e) Initial emergency response capabilities may be inadequate to manage the incident.
- f) University resources will be quickly overwhelmed.
- g) Communication systems may fail during a major incident.
- h) Backup systems will be available but may take time to activate.
- i) Shortfalls can be expected in both support personnel and equipment.

- j) State and federal assistance may not be immediately available.

## V. Concept of Operations

### a) General

- i) The Cornell University Emergency Operations Plan provides overall guidance for emergency operations.
- ii) ESF Annexes define roles and responsibilities, planned concept of operation, and internal and external capabilities and resources.
- iii) ESF annexes are designed to provide basic information to include points of contact in case additional resources or expertise is needed at the incident scene or on an Incident Management Team.

### b) Organization

- i) National Incident Management System concepts will be used for response to all incidents.
- ii) Incident or Unified Command will be used by responding departments.
- iii) When requested, ESF personnel will report to the Incident Command Post or other location, or will participate as members of an Incident Management Team.

### c) Notification

- i) Campus incidents involving IT outages or requests for support are to be reported to the IT Service Desk (ITSD) at [itsd@cornell.edu](mailto:itsd@cornell.edu) or (607)255-5500.
- ii) Requests for additional resources shall occur under the authority of the Incident/Unified Command through the Office of the CIO.

### d) Direction, Control and Authority to Act

- i) The Incident Command System (ICS) is used by University personnel to respond to emergencies and incidents.
- ii) During the emergency response phase, all responders will be under the direction and control of the incident's Incident/Unified Command.
- iii) Responders reporting to the incident scene will report to the Incident Commander at the Incident Command Post unless otherwise directed by the Incident Commander.

iv) The Incident/Unified Command is authorized to take actions necessary to contain and control the incident to protect and reduce impact to lives, research, property, the environment, and campus operations.

e) Actions

i) Preparedness

- (1) CIT shall maintain Continuity of Operations Plans (COOP) with associated roles and responsibilities for emergency preparedness and recovery.
- (2) CIT shall provide annual training for recipients of the CIT Continuity of Operations Plan to ensure that recovery personnel are knowledgeable about the plan and are aware of their roles and responsibilities.
- (3) CIT shall maintain a “chain of command” for the organization in the event that strategic personnel are not available for executing their role during recovery operations.
- (4) CIT shall maintain disaster recovery procedures for key infrastructure services and critical systems and services.
- (5) CIT shall maintain a prioritized list of service recovery and server restart order for determining the order of service restoration.
- (6) CIT shall maintain an emergency communications strategy to include communications within CIT, to the Incident/Unified Command and to users and customers of CITs services.
- (7) CIT shall develop and maintain a list of campus, community, and vendor resources that could be requested during an emergency.
- (8) CIT shall maintain a list of personnel (at least one primary and one back-up) that can be called to serve on an Incident Management Team to manage information technology related support functions.
- (9) Develop procedures to document costs for any potential reimbursement.
- (10) CIT shall participate in exercises and training to validate this annex and any supporting plans and procedures.

ii) Response

- (1) CIT shall provide support to University responders to help ensure adequate availability of IT communications and other services.

- (2) CIT shall coordinate other IT professionals across campus and, where appropriate, external vendors to support the communication and IT services need appropriate to the situation.
- (3) CIT shall act as liaison with other IT resources both internal and external as needed.
- (4) When requested, provide personnel to respond to the incident command post or other location to serve on an Incident Management Team to manage information technologies related support functions.
- (5) In conjunction with the Incident Commander, CIT shall coordinate emergency information for public release through ESF-17 Communications.

iii) Recovery

- (1) CIT shall coordinate the recovery, configuration and use of CIT resources to assist in the efficient recovery of Cornell operations.
- (2) As feasible, CIT shall assist the recovery, configuration and use of Cornell IT resources external to CIT to assist in the efficient recovery of Cornell operations.
- (3) CIT shall ensure that ESF-2 personnel, departments or agencies maintain appropriate records of costs incurred during the event.

## **VI. Responsibilities**

- a) Primary Department: Cornell University Information Technologies: Support
  - i) Serve as the lead agency for information technology related support functions and support the response and recovery operations after ESF activation.
  - ii) Develop, maintain, and update plans and procedures for use during an emergency.
  - iii) Identify, train, and assign personnel to serve as ESF-2 representatives at an Incident Command Post or on an Incident Management Team (IMT) when a University IMT is assembled.
- b) Support Departments
  - i) Develop, maintain, and update plans and procedures for use during an emergency.
  - ii) Identify, train, and assign personnel to assist the primary department at the Incident Command Post or on the Incident Management Team as needed.

- iii) Support the primary department as needed.

## **VII. Capabilities**

### **a) Cornell University Information Technologies**

- i) CIT is capable of troubleshooting, restoring and reconfiguring as the situation requires communication media to include the wired, wireless and telephony networks.
- ii) CIT is capable of troubleshooting, restoring and reconfiguring as the situation requires IT services as required for the response and continued operations of Cornell administrative and academic needs, such as:
  - (1) e-mail, including bulk mail, e-mail lists, and shared e-mail addresses for groups or events (“special mailboxes”),
  - (2) web- and video-conferencing
  - (3) live streaming of video-to-web
  - (4) blogs
  - (5) surveys,
  - (6) on-line collaboration spaces and wikis (Confluence, SourceForge, Box, etc.)
  - (7) web site design, creation, production, hosting, administration and horizontal-scaling for high-volume sites,
  - (8) digital signage,
  - (9) central administrative systems
  - (10) file services (sharing, storage, etc.),
  - (11) netIDs and password services (creation, reset, etc.)
  - (12) recovery of data previously backed-up through the central service (EZ-Backup),
  - (13) calendaring,
  - (14) printing,
  - (15) software acquisition and licensing,
  - (16) news and entertainment television over the data network (IPTV / Direct TV from Campus Televideo)
  - (17) Videon-Demand (a “You-Tube” like video service)

- (18) Instructional technologies, including iClickers, course management, and classroom technologies.
- iii) CIT is capable of installing, configuring and troubleshooting desktop systems to University personnel as required for continued operations of University business.
- iv) CIT is capable of providing technical resources to other campus units in the event emergencies not impacting CIT services directly, including:
  - (1) Desktop support
  - (2) Communications infrastructure consulting and design
  - (3) Security consulting and incident response
  - (4) Server administration
  - (5) Application administration
  - (6) Database administration
  - (7) Video production
  - (8) Audio/Video consultation and equipment recommendation
  - (9) Instructional technologies support
  - (10) Communications services (technical writing)
  - (11) IT Training services
- b) Administrative and Logistical Operations
  - i) CIT will maintain Business Operations Recovery Team procedure to facilitate restoration of administrative and logistical support operations for CIT personnel during an emergency.
- c) IT Vendors
  - i) As part of CIT's emergency plan, CIT shall maintain a list of IT vendors and their capabilities in the event that vendor utilization will be required in the event of an emergency.

## **VIII. Resources**

- a) CIT Resources
  - i) Physical resources that CIT has available to support efforts; i.e., Disaster response kits, phone banks, public computing labs, hardware, cable, etc.
  - ii) Staff resources that can aid in the recovery of other campus services.

- iii) CIT emergency procedures are available to other University IT units, on request.
- b) Support Department Resources
  - i) Disaster Recovery Procedures
  - ii) Standard Operating Procedures
  - iii) Alternate location for the CIT Network Operations Center (NOC)

## **IX. Policies and Procedures**

- a) University
  - i) University Policies as stipulated by the University Policy office, <http://www.dfa.cornell.edu/treasurer/policyoffice/>
- b) Environmental Health and Safety
  - i) Policies and Procedures related to emergency preparedness and response, <http://sp.ehs.cornell.edu/em/Pages/default.aspx>
- c) CIT Policy and Law Office Policies and Procedures
  - i) This documentation may be found at <http://www.cit.cornell.edu/policies/>. See also, University Policies, Volume 5, <http://www.dfa.cornell.edu/treasurer/policyoffice/policies/volumes/informatio ntech/index.cfm>.
- d) CIT Processes and Procedures related to emergencies:
  - i) [Procedure 2011-001, Emergency Planning and Recovery Teams](#)
  - ii) [Procedure 2011-003 Managing the CIT Unit Emergency Plan](#)
  - iii) Incident and event management procedures (formerly “NOCDocs”).

## **X. Attachments**

- a) None



Plan Review and Revision History

<b>Summary of Changes</b>	<b>Date</b>	<b>Completed By</b>
Version 2.0 updates	9/12/2017	Office Emg. Mgmt.