Incident Annex 2 – Cyber or Technology Emergencies

Coordinating Department

Information Technology Department

Supporting Departments

Facilities Services Department, Department of Public Safety (Emergency Management), Department of Public Safety (Police Operations)

Supporting Outside Agencies

University of Colorado System (Office of Information Security), University of Colorado System (University Risk Management), Outside Contractors

Section I: Plan Activation

Scope

The scope of this Incident Annex is to describe the campus response to an emergency invovling cyber-related issues and related technological emergencies, including but not limited to significant cyber threats and disruptions, crippling cyber attacks against the Internet or critical infrastructure information systems, technological emergencies, or declared disasters.

Concept of Operations

A. General

1. The ultimate goal of response to any cyber or technology related emergencies is to maintain or restore affected systems with a minimum of disruption to end users. However, use or restoration of systems will not be accomplished if there is risk of compromise due to physical or network vulnerability.

2. Generally, cyber emergencies will be handled by the Information Technology Department (IT).

3. Technological emergencies involving computer, server, or other hardware will generally also be handled by IT resources.

4. Technological emergencies involving electrical supplies, physical network infrastructure (i.e. cables or fiber optics) may involve resources such as the Facilities Services Department or outside contractors depending on the scope of work. Coordination of such interdepartmental work is at the direction of campus leadership.

5. All activities will be coordinated through the campus Emergency Operations Center (EOC) or Incident Command Post (ICP) if activated. Department representatives may be requested to respond to the EOC or ICP for coordination.

B. Specific

1. **Response**

a) Network or hardware problems will be handled by IT, coordinated by their Department Operations Center (DOC). This DOC will work closely with campus leadership for situational awareness, public information updates, and resource requests. IT will also work closely with appropriate University of Colorado System (CU System) organizations.

b) Response by IT to accidental or deliberate breaches of network security is defined by UCCS Policy 700-005, "Computer Security Incident Response", and the "UCCS Computer Incident Response Plan" developed by IT Security. This plan describes units involved and actions to be taken in response to security breaches.

c) Preservation of critical servers and data storage is covered under IT's Technology Risk Assessment worksheets and plans. This document describes data backup processes, servers and storage, and critical operations involved. IT will be required to work closely with affected departments to prioritize work and minimize disruption to critical functional areas.

d) Physical resources required by modern technology fall generally into the categories of energy and networks. Energy resources are discussed in detail under Emergency Support Function (ESF) 12 (Tab K of this Emergency Operations Plan). Network physical infrastructure (cabling and fiber optics) will require close coordination with Facilities Services and outside contractors to access and support this infrastructure.

2. **Recovery**

a) Restoration of data storage is the responsibility of IT for designated data storage servers on the campus network. Data backup and recovery processes are detailed in IT's Technology Risk Assessment worksheets and plans. Data contained on individual or department-specific servers may be the responsibility of the host department; backup and restoration procedures should be coordinated with IT.

b) Restoration of energy resources are discussed in detail under ESF 12. Restoration of network physical infrastructure (cabling and fiber optics) will require close coordination with Facilities Services and outside contractors for access and repair.

c) Hardware may be physically damaged due to electrical, water, fire, or other damage. IT and end user departments must coordinate with University Risk

Management (URM) and Resource Management for proper and quick replacement of equipment.

Section II: Pre-Event Coordination and Planning Responsibilities

Coordinating Department

Information Technology Department

A. Mitigation

1. Educate the campus community on individual and departmental responsibilities and computer and network security in accordance with UCCS Policy 700-002, "Responsible Computing".
2. Have data backup and restoration procedures in place and tested to support critical campus operations.

B. Preparedness

1. Complete incident response and business continuity plans to address potential hazards and anticipated losses.
2. Train IT staff in incident response and related support activities.
3. Maintain surveillance and network monitoring to anticipate breaches or outages prior to actual occurrence.
4. Provide personnel contact information to the Department of Public Safety for response to after-hours IT requirements.

Supporting Departments

Facilities Services Department

A. Coordinate with IT to access, maintain, and repair campus network infrastructure.

B. Provide energy requirements for IT services per ESF 12.

Department of Public Safety (Police Operations)

A. Investigate potential deliberate network attacks or other types of denial of service in coordination with IT.

Department of Public Safety (Emergency Management)

A. Coordinate Business Continuity Planning with IT, and between the campus departments requiring IT resources.

Supporting Outside Agencies and Facilities

University of Colorado System (Office of Information Security)

A. Coordinate system-wide policies and procedures regarding IT security.

B. Provide over sight and assistance in the event of a security breach to CU System or UCCS networks.

University of Colorado System (University Information Services)

A. Provide equipment and personnel support for restoration of UCCS IT services.

B. Work in conjunction with other System campuses to provide backup to critical processes.

University of Colorado System (University Risk Management)

A. Provide loss estimation and insurance reimbursement in the event of loss of physical hardware or infrastructure, or if network outage or equipment downtime created a monetary damage.

Outside Contractors

A. Provide services to support hardware, network infrastructure, or other technology replacement or repair in accordance with contract provisions.