Tarrant County College

Information Technology Annex

RECORD OF CHANGES

CHANGE #	DATE OF CHANGE	DESCRIPTION	CHANGED BY

APPROVAL & IMPLEMENTATION

Information Technology Annex

Vice Chancellor for Information and Technology

Date

INFORMATION TECHNOLOGY ANNEX

I. AUTHORITY

See Section 1 of the Basic Plan for general authorities.

II. PURPOSE

The purpose of this annex is to define the organization, operational concepts, responsibilities, and procedures to accomplish emergency information technology requirements for communications. This annex is applicable to the TCC Information Technology Department and personnel assigned functional Information Technology responsibilities.

III. EXPLANATION OF TERMS

A. Acronyms

DDC	Disaster District Committee
EMP	Electromagnetic Pulse
EOC	Emergency Operations Center
FEMA	Federal Emergency Management Agency
IC	Incident Commander
ICS	Incident Command System
IP	Internet Protocol
IT	Information Technology
JIC	Joint Information Center
NIMS	National Incident Management System
NRF	National Response Framework
SOC	State Operations Center
SOP	Standard Operating Procedures
RACES	Radio Amateur Civil Emergency Service
TLETS	Texas Law Enforcement Telecommunications System

B. Definitions

Local Computer Network	Local, Regional, or Wide-Area Networks.
State Warning Point	Warning Point for the state operated by the SOC.

IV. SITUATION AND ASSUMPTIONS

A. Situation

1. As noted in the general situation statement in the basic plan, we are at risk from a number of hazards that could threaten public health, safety, personal and District property. A reliable and interoperable information system is essential to obtain the most complete information on emergency situations and to direct and control our resources responding to those situations.

B. Assumptions

1. Adequate information systems are available for effective and efficient communications, warning, response and recovery operations.

2. Any number of natural or manmade hazards may neutralize or severely reduce the effectiveness of systems currently in place for emergency operations.

3. Additional communication equipment required for emergency operations may be located in more than one location owned or leased by Tarrant County College

4. Additional communications equipment required for emergency operations may be made available from business, volunteer organizations, and/or other governmental agencies.

V. CONCEPT OF OPERATIONS

A. General

1. A common operating picture within the District provides the framework of our communications capabilities. This framework is made possible by interoperable systems. Extensive communications networks and facilities are in existence throughout the District to provide coordinated capabilities for the most effective and efficient response and recovery activities.

2. The existing communications network at Tarrant County College District serves to perform the communications efforts for emergency operations comprised of:
   - Internet protocol (IP) telephone systems
   - E-mail
   - Internet connectivity
   - Campus based electronic signage
   - Emergency notification system allows voice and text messaging via electronic devices, emails, computers, network phones, PA systems, fire alarm systems and integration through multiple systems.

   IP phone systems for each District campus serve as the primary means of communication with other communication systems as a backup. Secondary resources may be cell phones, radio or other electronic wired and wireless devices.

3. During emergency operations, all District departments will maintain their existing equipment and procedures for communicating with their personnel. They will keep the EOC informed of their operations and status at all times.

4. To meet the increased communications needs created by an emergency, various state and regional agencies, amateur radio operators, and business/industry/volunteer group radio systems may be asked to supplement communications capabilities. These resource capabilities will be requested through local and regional mutual-aid agreements and/or the Disaster District, as required.

B. Activities by Phases of Emergency Management

1. Prevention

   a. Maintain a current technology based, reliable, interoperable, and sustainable information technology communications system.

   b. Ensure communication systems meet the District's needs.

c. Ensure intelligence and other vital information networks are operational.

2. Preparedness

   a. Review and update this communications annex.

   b. Develop procedures that are documented and implemented through operating instructions.

   c. Thoroughly and continually review these systems for improvement including the implementation and institutionalized use of information management technologies.

   d. Ensure communications requirements for Emergency Operations Center (EOC) are regularly reviewed.

   e. Review After Action Reports (AAR) of actual occurrences, exercises, and other sources of information for lessons learned.

   f. Ensure the integration of mitigation plans and actions into all phases of emergency management as applicable.

   g. Acquire, test, and maintain information communications equipment.

   h. Ensure replacement parts for communications systems are available and make arrangement for rapid resupply in the event of an emergency.

   i. Educate personnel on appropriate equipment and communication procedures as necessary.

   j. Conduct periodic communications drills and make communications a major element during all exercises.

   k. Review assignment of all personnel.

   l. Review emergency notification list of department leads.

3. Response

   a. Select personnel required for emergency operations according to the incident.

   b. Incident communications will follow ICS standards and will be managed by the IC using a common communications plan and an incident-based communications center.

c. All incident management entities will make use of common language during emergency communications. This will reduce confusion when multiple agencies or entities are involved in an incident.

d. Ensure emergency equipment repair on a 24-hour basis.

4. Recovery

All activities in the emergency phase will continue until such time as emergency information communications are no longer required.

VI. ORGANIZATION AND ASSIGNMENT RESPONSIBILITIES

A. General

1. Our emergency network communications system is operated by the Department of Information Technology and includes a variety equipment.

B. Task Assignments

1. The Associate Vice Chancellor for Information technology will:

   a. Be responsible for all activities enumerated in this annex in Section V. B - Activities by Phases of Emergency Management.

   b. Supervise the technology staff that support the communications network and equipment - Network Administrator, Telecomm Administrator, and technicians.

2. The Network Administrator and Telecom Administrator will:

   a. Coordinate common information network procedures.

   b. Develop and maintain a resource inventory.

   c. Ensure a communications capability exists between the Police Communications Center of the TCC Police Department and the Emergency Operations Center.

   d. Ensure network restoration procedures are developed.

   e. Develop recall rosters for essential personnel.

VII. DIRECTION AND CONTROL

A. General

1. The Vice Chancellor for Information Technology establishes general policies for emergency information network communications.

3. The Network Administrator is under the supervision of the Associate Vice Chancellor for Information Technology and is directly responsible for network equipment and District information system operational readiness.

4. Information security will protect emergency operations functionality, and respond to threats against emergency operations functionality.

5. Personnel from individual departments and support agencies, while under control of their own department or agency and operating their own equipment, are responsible for knowing and following the procedures outlined in this annex.

6. During emergency situations involving multiple agencies and/or jurisdictions, the various code systems used for brevity will be discontinued and normal speech will be used to insure comprehension. In addition, local time will be used during transmissions.

7. During emergency situations, communications will be maintained between the Disaster District and the District EOC.

B. Continuity of Government

The Department for Information Technology shall establish a line of succession for essential personnel.

VIII. READINESS LEVELS

A. Readiness Level IV - Normal Conditions

See the prevention and preparedness activities in paragraphs V.B.1 and V.B.2 above.

B. Readiness Level III - Increased Readiness

1. Alert key personnel.

2. Check readiness of all equipment and facilities and correct any deficiencies.

C. Readiness Level II – High Readiness

1. Alert personnel for possible emergency duty.

2. Monitor situation of possible issuance of warning or alerts.

D. Readiness Level 1 – Maximum Readiness

1. Institute 24-hour operations.

2. Conduct periodic communication checks.

IX. ADMINISTRATION AND SUPPORT

A. Facilities and Equipment

Maintain a listing of essential equipment.

B. Maintenance of Records.

All records generated during an emergency will be collected and filed in an orderly manner so a record of events is preserved for use in determining response costs, settling claims, and updating emergency plans and procedures.

C. Preservation of Records

Vital records should be identified and protected from the effects of disaster to the maximum extent feasible. Should records be damaged during an emergency situation, professional assistance in preserving and restoring those records should be obtained as soon as possible.

D. Communications Protection

The physical protection of information network equipment and facilities will be maintained under normal and emergency operations to help ensure continuity of operations.

E. Security

1. Measures will be taken to ensure that only authorized personnel will have access to the District Data Center, communications closets, and remote collocation facilities.

2. Information security will be maintained in accordance with national, state, and local requirements.

F. Training

1. The Department for Information Technology assigning personnel to the EOC for Information Technology purposes is responsible for making certain those persons are familiar with their operating procedures.

2. The Associate Vice Chancellor for Information Technology will provide additional training on emergency network information equipment and procedures as necessary.

G. Support

If requirements exceed the capability of local communications resources, the Chancellor will request support from nearby jurisdictions or state resources from the Disaster District.

X. ANNEX DEVELOPMENT AND MAINTENANCE

A. The Associate Vice Chancellor for Information Technology will be responsible for maintaining this annex.

B. This annex will be updated in accordance with the schedule outlined in Section X of the Basic Plan.

XI. REFERENCES

A. Federal Emergency Management Agency (FEMA), Comprehensive Preparedness Guide (CPG-101)

B. Division Of Emergency Management *Local Emergency Management Planning Guide.* (DEM-10)