BLINN COLLEGE DISTRICT

EMERGENCY RESPONSE PLAN (ERP)

August 2024, V.1.2

Blinn College District Emergency Management

Blinn College District Safety and Risk Management

UNIFIED CAMPUS SAFETY PROGRAM (UCSP)

PAGE INTENTIONALLY LEFT BLANK

PROMULGATION STATEMENT

This Emergency Response Plan (ERP), and contents within, provide guidance for how the Blinn College District conducts various emergency responses specific to all District campuses and facilities. The ERP is written in support of, and as an addendum to, the Washington County Emergency Operations Plan (EOP), sometimes referred to as an Emergency Management Plan, Annex "G," Law Enforcement, and shall be considered an "interactive support document" to that EOP. For Blinn College District campuses and facilities in Brazos County, Fayette County, and Austin County – the ERP will serve as the primary response plan for all critical incidents having significant impact on District operations.

APPROVAL AND IMPLEMENTATION

The Blinn College District Board of Trustees has officially adopted the National Incident Management System (NIMS) as the guiding structure for District Emergency Management and the ERP. The Blinn College District's Emergency Management Coordinator (EMC) shall be responsible for ERP oversight and coordination with applicable stakeholders. The ERP is flexible in its use and the entire plan may be activated based on the specific emergency and decision by Blinn College District senior leadership.

This ERP and its supporting contents, including all annexes, are hereby approved and become effective immediately upon the signing of all signatory authorities noted below.

Additionally, the ERP supersedes both the existing ERP of 11/4/14 and the Emergency Procedures Manual of 10/21/14, combing and updating the concepts and response protocols of both documents into a singular plan.

Approved: Signed copy on file   Date:

_____   _____

Dr. Mary Hensley, Chancellor
Blinn College District

Approved: Signed copy on file   Date:

_____   _____

John R. Chancellor, Chief of Police
Emergency Mgmt. Coordinator
Blinn College District

PAGE INTENTIONALLY
LEFT BLANK

TABLE OF CONTENTS

ACRONYMS USED IN THE EMERGENCY RESPONSE PLAN (ERP)

AAR	After Action Report
AED	Automated External Defibrillator
ADA	Americans with Disabilities Act
BCD	Blinn College District
BCDPD	Blinn College District Police Department
BIT	Behavioral Intervention Team
CIRT	Critical Incident Response Team
COOP	Continuity of Operations Plan
CPR	Cardiopulmonary Resuscitation
DHS	Department of Homeland Security
DPS	Texas Department of Public Safety
EMS	Emergency Medical Services
EOC	Emergency Operations Center
EOP	Emergency Operations Plan
EPG	Executive Policy Group
ERP	Emergency Response Plan
ERT	Emergency Response Team
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Administration
FERPA	Federal Education Rights and Privacy Act
HAZMAT	Hazardous Material
HIPAA	Health Insurance Portability Act
HR	Human Resources
HSPD	Homeland Security Presidential Directive
IAP	Incident Action Plan
ICP	Incident Command Post
ICS	Incident Command System
IMT	Incident Management Team
IT	Information Technology
JIS	Joint Information System
LO	Liaison Officer
MACS	Multi-Agency Coordination Center
MOU	Memorandum of Understanding
NGO	Non-Governmental Organization
NIMS	National Incident Management System
PIO	Public Information Officer
PPE	Personal Protective Equipment
SDS	Safety Data Sheets (Materials)
SITREP	Situation Report
SO	Safety Officer
SOP	Standard Operating Procedure

PURPOSE, SCOPE AND LEGAL AUTHORITY

This Emergency Response Plan (ERP) outlines additional operational concepts and procedures specific to the Blinn College District (also referred to as the District within the ERP) and its various campuses and controlled facilities as otherwise not stated in "Annex G: Law Enforcement" of the Washington County, Texas (BASIC) Emergency Operations Plan. In the event of an emergency that expands beyond Blinn College District boundaries or beyond the Blinn College District's response capabilities, the response protocols of the Washington County EOP will take precedence. For campuses and facilities outside of Washington County, response partners from those jurisdictions will respond via standard mutual-aid agreements.

In addition to applicable state and federal law, Blinn College District Board Policy (CGC), Blinn College Administrative Regulation – Emergency Response Plan, effective November 1, 2014, stipulates that:

The Emergency Response Plan (ERP) provides general guidance for an all-hazards approach to emergency management activities and an overview of Blinn's methods of mitigation, preparedness, response and recovery. The ERP describes Blinn's emergency response organization and assigns responsibilities for various emergency tasks. The ERP is intended to provide a framework for more specific functional annexes that describe in more detail who does what, when, and how. The ERP applies to all Blinn officials, departments and agencies. The primary audience for the ERP includes: Chancellor, college administration, department and agency heads and their senior staff members, leaders of local volunteer organizations that support emergency operations and others who may participate in Blinn's mitigation, preparedness, response and recovery efforts.

The ultimate priority of the Blinn College District, within the limits of its resources, capabilities, and emergency response partnerships, is the safety and well-being of students, guests, faculty and staff in the event of a critical incident, disruption, and/or significant interruption of the District's mission of building stronger communities by providing quality, comprehensive education, and empowering students to achieve excellence in their educational careers and personal goals. To that end, the District must ensure the ability to rapidly restore services and carry out critical functions essential to the combined success of all stakeholders.

GENERAL CONSIDERATIONS

Although threats associated with acts of violence presents an immediate danger to students, faculty, staff, and visitors of the Blinn College District, these are not the only areas of concern as additional "man-made" and natural hazards can, and often do, pose a threat to District operations and general well-being. When these life-threatening incidents occur, they will require specific and immediate response actions in order to stop an attack, minimize injuries and loss of life, mitigate damage to district property and begin recovery efforts.

The ERP reflects and incorporates the primary goal of the Blinn College District to protect lives, preserve property, and provide for the resumption of essential services and normal activities as soon as possible. Implementation of the ERP as a response to active threats, acts of violence incidents, severe weather, etc. involves making management and executive decisions during emergencies which may affect campus operations, schedules, and work assignments in the campus community. This plan applies to all Blinn College District sponsored incidents on campus and all public or private college-sanctioned activities on Blinn College District property.

DIRECTION, GUIDANCE AND ACTIVATION

For most emergency functions, successful operations require a coordinated effort from a number of college departments and groups. Generally, the primary responsibility for an emergency management response will be assigned to the Blinn College District Emergency Management Coordinator (EMC), in direct coordination and contact with the Blinn College District Chancellor, or their designee, who shall be responsible for executing Executive Policy Group (EPG) Responsibilities during ERP activation.

The Blinn College District Chief of Police has been designated as the EMC for the Blinn College District and has the authority to activate the ERP and marshal personnel and resources, as necessary, to accomplish response objectives based upon the emergency presented. Additionally, activation of the ERP may be made at the discretion and direction of the Blinn College District Chancellor, or their designee, and coordinated through the EMC.

In the absence of, or at the direction of, the EMC the Blinn College District Assistant Chief of Police or Blinn College District Director of Safety and Risk Management may activate the ERP and be designated as the EMC for the emergency at hand.

The EMC is responsible for providing the following direction and plan guidance activities:

1. Serve as a staff advisor to the Blinn College District Chancellor on matters concerning emergency management.
2. Ensure that the EPG is apprised of preparedness status, current response, planned response, and emergency management needs.
3. Coordinate local planning, preparedness and response with supporting emergency response providers and external jurisdictions.
4. Oversee the operations of the Emergency Operations Center (EOC) during ERP activation by occupying the role of EOC Manager or Incident Commander, depending on the scale of the event and Incident Command System (ICS) positions required to effectively manage the critical incident or emergency.
5. Occupy an ICS staff position, as needed, during an expanding critical incident having direct impact to Blinn College District property and falling under a multi-jurisdictional, county-wide, or regional response.

The Blinn College District Chancellor, or their designee, is responsible for the management of the Executive Policy Group (EPG) and will:

1. Retain the ultimate authority to designate individuals responsible for the management of any Blinn College District emergency response should ERP activation be required.
2. Manage the activities and response of the EPG in support of the ERP.
3. Initiate the Blinn College District Continuity of Operations Plan (COOP) and ensure that the regular operations of the District, facilities and campuses (within the non-impacted area) successfully continue to the fullest extent possible.
4. Ensure that the Blinn College District Board of Trustees and key stakeholders are apprised of the emergency situation and response, as necessary.
5. Coordinate with the Blinn College District Public Information Officer (PIO) to ensure that students, staff, faculty and public are apprised of the emergency and response, as necessary.

CONCEPT OF OPERATIONS – OVERALL APPROACH

Active threats, specifically acts of violence include, but are not limited to, the following: an active shooter incident, explosive incident or bomb threat, barricaded subject, or armed intruder. Additional threats include, but are not limited to, biological agents, hazardous materials exposure, threats to sensitive electronic information (cybersecurity), structural fires, terrorism, utility disruptions, floods, tornadoes, winter storms and freezes, infectious diseases and pandemics, and food borne illnesses. The Blinn College District Police Department is the primary law enforcement agency of jurisdiction for active threats and acts of violence on Blinn College District campuses and will respond in accordance with Blinn College District Police Department policies and procedures.

In the event of expanding critical incidents that impact areas outside of Blinn College District controlled property and/or beyond the response capabilities of the Blinn College District in the City of Brenham, the Washington County EOP and associated response protocols will take precedence within Washington County. For Blinn College District property and facilities in the counties of Brazos (City of Bryan), Fayette (City of Schulenburg), and Austin (City of Sealy) – mutual aid for emergency response will be enacted.

The Blinn College District has adopted the National Incident Management System (NIMS) in accordance with Homeland Security Presidential Directive 5 (HSPD-5). The adoption of NIMS provides a consistent approach to the effective management of situations involving natural, technological or man-made disasters, including active threats and acts of terrorism. NIMS assists the District integrate its response activities using a set of standardized organizational structures designed to improve interoperability between all levels of government, the private sector, non-governmental agencies (NGOs) and all Blinn College District campuses and facilities during emergency responses to critical incidents.

Regardless of the hazard or threat and associated emergency response, Blinn College District leadership must implement appropriate population protection activities, issue timely emergency notifications, coordinate public information activities, ensure communications interoperability, and coordinate continuously with local emergency services personnel.

HAZARD ANALYSIS

Blinn College District campuses and facilities are exposed to hazards, natural and "man-made," that have the potential for disrupting normal working operations, causing casualties and damage to critical infrastructure. Historically, the campuses and facilities of the Blinn College District have suffered localized damage from severe weather events and dealt with the various health and economic impacts of a world-wide pandemic. Lesser incidents impacting the campus community have been limited to food-borne illness and protective responses enacted by Blinn College District law enforcement officials while assisting surrounding jurisdictions with active threats and fleeing suspects. While not an exhaustive list, a summary of major hazards is provided in the table below:

HAZARD TYPE	LIKELIHOOD OF OCCURRENCE	ESTIMATED IMPACT ON HEALTH AND PUBLIC SAFETY	ESTIMATED IMPACT ON PROPERTY
Acts of Violence	LOW	HIGH	MEDIUM
Biological Release	LOW	HIGH	LOW
HazMat Release	LOW	HIGH	LOW
Cyber Threat	HIGH	LOW	LOW
Structural Fire	MEDIUM	MEDIUM	HIGH
Terrorism	LOW	HIGH	MEDIUM
Utility Disruption	MEDIUM	MEDIUM	MEDIUM
Flood	MEDIUM	MEDIUM	MEDIUM
Tornado	LOW	MEDIUM	HIGH
Winter Storm	LOW	LOW	MEDIUM
Infectious Disease	MEDIUM	MEDIUM	LOW
Food Borne Illness	LOW	MEDIUM	LOW

High likelihood indicates hazard occurs frequently, while low likelihood indicates that the hazard rarely or has not occurred.

**High impact indicates significant injury/illness and/or loss of life or damage to assets is probable, while low impact indicates no probable impact on operations, life-safety, or assets.*

***The supporting Hazard Summary for the Washington County EOP can be found on BP-10 of the Washington County EOP.*

CAPABILITIES ASSESSMENT

Primary law enforcement services are provided by the Blinn College District Police Department, unless otherwise noted, and certain critical infrastructure responses can be managed by Blinn College District Facilities Maintenance. The primary and secondary agencies providing emergency services are listed in the table below:

AGENCY TYPE	PRIMARY RESPONDER	SECONDARY RESPONDER
Emergency Medical Service	Washington County: Washington County EMS Brazos County: Brazos County ECD Fayette County: Fayette County EMS Austin County: Austin County EMS	Mutual Aid
Fire Services	Washington County: Brenham FD Brazos County: Bryan FD Fayette County: Schulenburg FD Austin County: Sealy FD	Mutual Aid Mutual Aid Mutual Aid Mutual Aid
Law Enforcement Services	Washington County: Blinn College Dist. PD Brazos County: Blinn College Dist. PD Fayette County: Schulenburg PD Austin County: Sealy PD	Brenham PD Bryan PD Blinn College Dist. PD Blinn College Dist. PD
Public Health Services	Washington County: Washington County HD Brazos County: Brazos County HD Fayette County: Fayette County HD Austin County: Austin County HD	
Emergency Management	Washington County: Washington Co. OEM Brazos County: Brazos Co. OEM Fayette County: Fayette County OEM Austin County: Austin County OEM	Blinn College Dist. EM Blinn College Dist. EM Blinn College Dist. EM Blinn College Dist. EM
Safety and Risk Management	Blinn College District Blinn College District Facilities Maintenance	

Secondary responders may include federal, regional and state response partners as well county-wide law enforcement agencies.

PLANNING ASSUMPTIONS

Established in 1883, the Blinn College District is a muti-campus Texas junior-college system that provides academic and technical education services for more than 15,000 students annually in four counties, including a residential campus located in Brenham, Texas. Additionally, the District employs approximately 1,200 full-time and part-time faculty and staff members.

In addition to the planning assumptions listed in the Washington County EOP, the Blinn College District recognizes the following planning assumptions generalized to all District campuses and facilities:

- The Blinn College District will continue to be exposed to and subject to the impact of those hazards described previously as well as lesser hazards and others that may develop in the future.

- Emergencies may occur at any time and at any place. In many cases, dissemination of warning to the public and implementation of increased readiness measures may be possible. However, some emergency situations occur with little or no warning.

- Although capable of immediate emergency responses on the Brenham, Bryan and RELLIS campuses, the Blinn College District is reliant upon local jurisdictions to provide immediate emergency responses at both the Schulenburg and Sealy Campuses.

- Proper planning and preparedness activities with local emergency services will ensure an effective and coordinated response and, in the case of campuses within Washington County, seamless integration into the EOP, should a critical incident expand beyond the confines and capabilities of the Brenham area campuses.

- Proper mitigation actions, such as floodplain management, timely maintenance of facilities, life safety inspections, and laboratory inspections can prevent or reduce disaster-related losses. Detailed emergency planning, training of emergency responders and other personnel on the activation and deployment of the ERP and conducting periodic emergency drills and exercises can improve readiness to deal with emergency situations.

- Blinn College District officials and representatives must recognize their responsibilities for the safety and well-being of faculty, staff, students and visitors; and assume their responsibilities in the implementation of this ERP.

- Blinn College District officials recognize that students, faculty and staff with disabilities, including access and functional needs, may require additional assistance during emergencies and critical incidents to ensure the nature of the incident is properly and adequately communicated to them, that they are provided assistance in moving to a place of safety or refuge, and that if required, special medical regime(s) are continued for the duration of the incident to the best of the District's capabilities.

- Physical and psychological safety, including trauma-informed care, are necessary for the well-being of students, faculty and staff immediately after an emergency or critical incident. Blinn College District understands that campus-based resources, as well as those available in the greater area, should be made available and readily deployed to assist in the campus community recovery process.

- Proper implementation of the ERP will reduce or possibly prevent disaster related losses to life and property.

The chart below represents the general education service area of the Blinn College District:
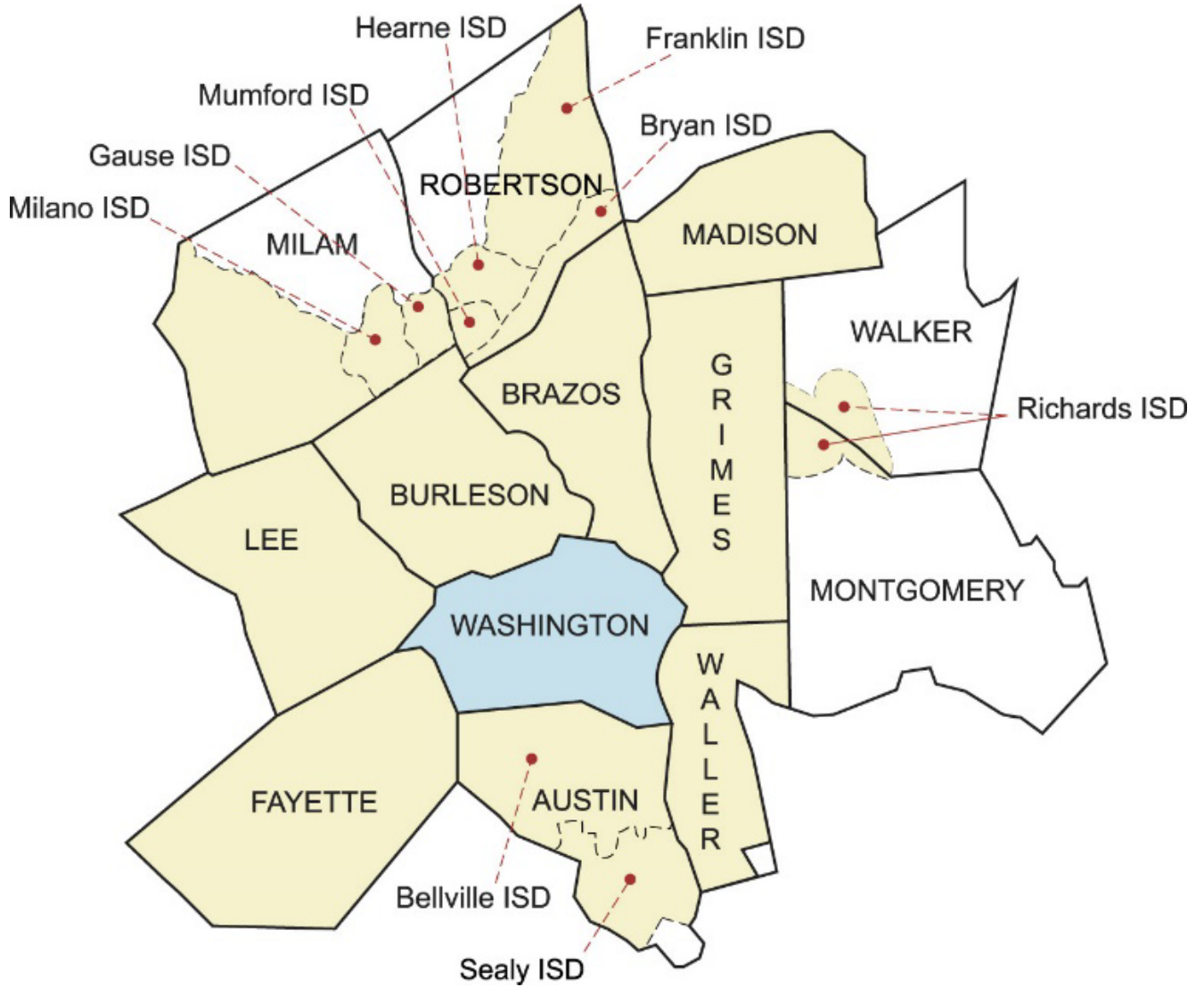
*Blinn College District campuses are located in Brazos (City of Bryan), Washington (City of Brenham), Fayette (City of Schulenburg), and Austin (City of Sealy) Counties, Texas.

OPERATIONAL GUIDANCE - NIMS

The Blinn College District will employ the five components of the NIMS in emergency and critical incident operations:

Preparedness is a continuous cycle of planning, organizing, training, equipping, exercising, evaluating, and taking corrective action. Training and exercising plans are the cornerstone of preparedness which focuses on readiness to respond to all-hazards incidents and emergencies.

Prevention focuses on preventing human hazards, primarily from potential natural disasters or terrorist (both physical and biological) attacks. Preventive measures are designed to provide more permanent protection from disasters; however, not all disasters can be prevented. The risk of loss of life and injury can be limited with good evacuation plans, environmental planning and design standards.

Response is comprised of the coordination and management of resources (including personnel, equipment, and supplies) utilizing the Incident Command System in an all-hazards approach; and measures taken for life/property/environmental safety. The response phase is a reaction to the occurrence of a catastrophic disaster or emergency.

Recovery consists of those activities that continue beyond the emergency period to restore critical community functions and begin to manage stabilization efforts. The recovery phase begins immediately after the threat to human life has subsided. The goal of the recovery phase is to bring the affected area back to some degree of normalcy.

Mitigation is the effort to reduce loss of life and property by lessening the impact of disasters and emergencies. Mitigation involves structural and non-structural measures taken to limit the impact of disasters and emergencies. Structural mitigation actions change the characteristics of buildings or the environment; examples include flood control projects, raising building elevations, and clearing areas around structures. Non-structural mitigation most often entails adopting or changing building codes.

➢Preparedness
➢Prevention
➢Response
➢Recovery
➢Mitigation

BLINN COLLEGE DISTRICT ICS USE AND STRUCTURE

1. Incident Command System (ICS) Use and Purpose

The District and all associated campuses and facilities have committed to utilizing the ICS as part of NIMS compliance for the response to all emergencies and critical incidents impacting District operations, which would include impacts to the safety and security of all students, faculty and staff as well as District-owned critical infrastructure. The purpose of the ICS is to:

A. Provide an organizational construct than can expand or contract rapidly in response to the requirements of an incident necessitating activation of the ERP;
B. Provide management with the control necessary to direct and coordinate all operations, emergency response services and organizations, and District Emergency Teams responding to incidents;
C. Assign District employees with reasonable expertise and training to perform critical functions expediently;
D. Allow for activation of only those positions needed to effectively manage a particular incident;
E. Promote proper span of control and unity of command.

2. Normal Operations vs. ICS Structures

The organizational structure of the ICS generally does not resemble that of the day-to-day organization of the Blinn College District and associated hierarchies. Assignment to roles within the ICS may necessitate reporting relationships outside of the normal operational hierarchy based upon expertise, skills, and experience in managing critical incidents and emergencies. Furthermore, as the severity of an incident increases, assignments may change in the ICS structure at the direction of the District Chancellor, EMC or IC. The BCD organizational chart for "normal" operations is available in the annex section of this ERP.

3. Use of ICS for Blinn College District Planned Events

The Blinn College District utilizes the ICS structures for all mass- gathering, sensitive, or large "pre-planned" events in the form of Emergency Action Plans (EAPs) developed by the Blinn College Police Department through the direction of the Chief of Police/EMC. Use of EAPs for non-emergency events assists in efficient operation and provide District employees familiarity with the ICS through regular use during non-emergency operations.

## 4. Blinn College District ICS Roles and Responsibilities

The Blinn College District Chancellor has the final authority for all emergency operations in the District. In that role, the Chancellor:

A. Is responsible for ensuring that the Blinn College District EMC promotes the overall development of the ICS and NIMS throughout the District.

B. Is responsible for District-wide emergency declarations in collaboration with the Blinn College District Board of Trustees.

C. Serves as the Area Commander during multiple or concurrent incidents impacting several District campuses or, at their discretion, may designate that responsibility to the EMC.

D. May act as the Blinn College District representative in a Washington County Unified Command.

E. Manage the operations of the Blinn College District Executive Policy Group (EPG) which may include, but is not limited to:
- Chancellor
- Executive Vice Chancellor
- General Legal Counsel
- Vice Chancellor of Human Resources
- Vice Chancellor of Business and Finance
- Vice Chancellor of Academic Affairs
- Vice Chancellor of Student Services
- Assistant Vice Chancellor of Facilities, Planning and Construction
- Campus Executive Deans
- Director of Communications, Media Relations and Marketing (may also staff, or assign staff to ERT and/or ICP)

F. The Executive Policy Group, when established as a component of ERP activation, will:
- Ensure that emergencies and critical incidents are properly managed.
- Work with the EMC in assessing the emergency and/or critical incident and provide policy oversight and support for the District's specific response.
- Ensure that ERP management objectives are met and do not conflict with each other or with District Board policies.
- Allocate critical resources and District assets according to established priorities.

INCIDENT COMMAND SYSTEM GENERAL ROLES SUMMARY
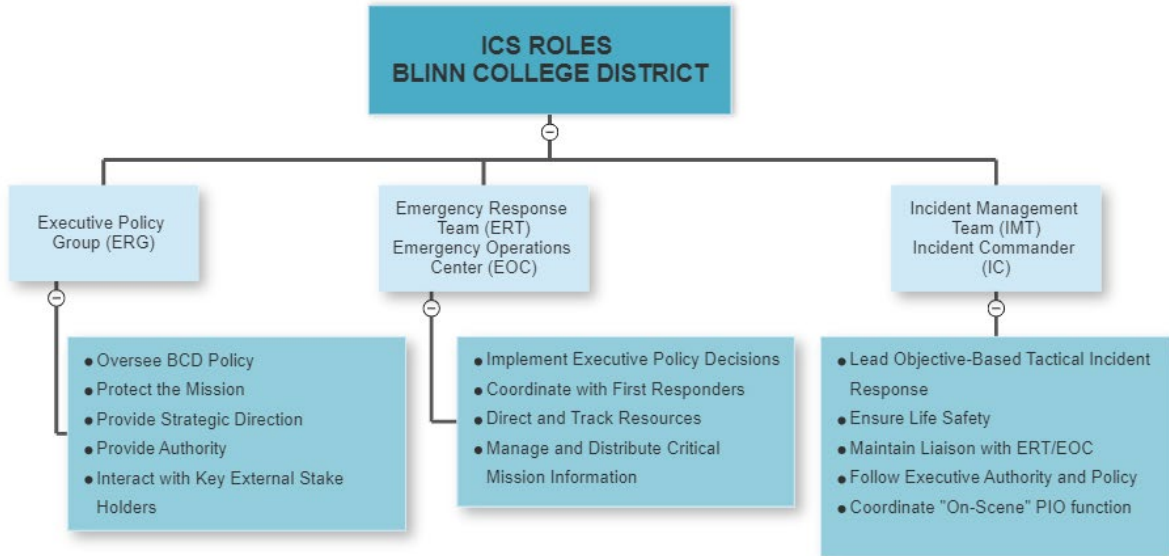
SPECIFIC INCIDENT COMMAND SYSTEM (ICS) ORGANIZATIONAL CHART
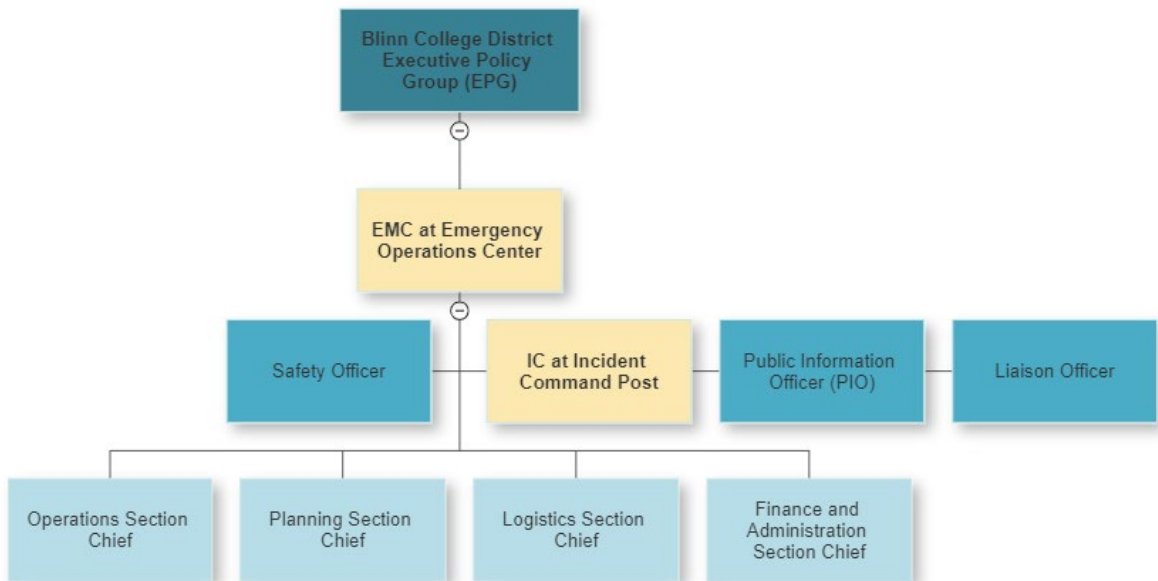
ROLES AND RESPONSIBILITIES WITHIN THE ICS STRUCTURE

1. **Incident Commander (IC) at the Incident Command Post (ICP):**

This position is held by the most capable person at the incident scene, and is usually the BCDPD Assistant Chief of Police, but may also be another first responder (law, fire, EMS) or a trained District authority who can take charge until a first responder arrives to become the new IC. The IC's responsibilities include:

A. Taking immediate actions to preserve life and safety of staff, faculty, students, vendors and visitors.
B. Establishing incident objectives and tactics to address the immediate threat. The IC is directly responsible for ensuring that all functional area activities of the Incident Management Team (IMT) are directed toward accomplishment of the tactical objectives.
C. Initiating contact with the EMC to begin assessment of the incident situation.
D. Activating relevant Command and General Staff to assist in response and recovery of the incident, including requests for additional first responder support.
E. Providing verbal and written communication to the District Executive staff, or their representatives (e.g., the ERT EOC) about the status of the incident and condition of the threat and its impacts, including estimated amount of control of the impacts and estimated time needed to close the incident response.

2. **Emergency Management Coordinator at the EOC (if activated):**

This position is generally held by the BCDPD Chief of Police but may be staffed by Assistant Chief of Police or Director of Safety and Risk Management, and they will report to the designated EOC. The personnel comprising the EOC may be referred to as the Emergency Management Team (EMT). Once at the EOC, the EMC confirms its habitability and begins the process of activation using the checklists provided in the Annex. Once enough staff and communications are available to perform the EOC functions, the EMC informs the Executive Policy Group (EPG) and the IC that the EOC is operational. The EMC's responsibilities will then include:

A. Ensuring emergency communications remain operational.
B. Setting overall organization incident-related priorities.
C. Supporting first responder and Crisis Intervention Response Team (CIRT) immediate actions to preserve life and safety of staff, faculty, students and visitors.
D. Establishing incident objectives and strategies that support the IC to address the immediate threat. The EMC is directly responsible for ensuring that all functional area activities are directed toward accomplishment of the strategic

objectives.

E. Initiating contact with the *first* District Executive available in their line of succession to ensure they are aware and provide policy and oversight support.

F. Activating additional relevant Command and General Staff to assist in response and recovery of incident, including requests for additional position support by Command Staff Officers and Section Chiefs.

G. Providing verbal and written communication to the EPG about the status of the incident and condition of the threat and its impacts, including estimated amount of control of the impacts and estimated time needed to close the incident response.

H. Providing verbal and written communication to the IC about the status of the ICP requested resources and support from the District needed to close the incident response tactical objectives.

3. **Command Staff:**

A. *Public Information Officer (PIO):*

The Public Information Officer (PIO) is responsible for interfacing with the public and media and/or with other agencies with incident-related information requirements. The PIO gathers, verifies, coordinates, and disseminates accurate, accessible, and timely information on the incident's cause, size, and current situation; resources committed; and other matters of general interest for both internal and external audiences. The PIO may also perform a key public information- monitoring and rumor control role. Only one PIO should be designated per incident at the ICP, at the EOC and with the EPG. Assistants may be assigned from other involved agencies, departments, or organizations. The IC, EMC, EPG and the District PIO must collaborate to approve the release of all incident-related information as part of a Joint Information System (JIS) process required by NIMS. In large-scale incidents, or where multiple command posts are established within the District operations, a single designated PIO should lead the Joint Information Center (JIC) in order to ensure consistency in the provision of information to the public.

B. *Safety Officer (SO):*

The Safety Officer (SO) monitors incident operations and advises the IC and the EMC on all matters relating to operational safety, including the health and safety of emergency first responder personnel. The ultimate responsibility for the safe conduct of incident management operations of first responders rests with the IC and supervisors at all levels of incident management. The SO at the EOC is responsible in the same way for District personnel taking response actions to support response operations.

The SO is, in turn, responsible for the systems and procedures necessary to ensure ongoing assessment of hazardous environments, including the incident

Safety Plan, coordination of multiagency safety efforts, and implementation of measures to promote emergency response safety as well as the general safety of incident operations. The SO has immediate authority to stop and/or prevent unsafe acts during incident operations. It is important to note that the agencies, organizations, or jurisdictions that contribute to joint safety management efforts do not lose their individual identities or responsibility for their own programs, policies, and personnel. Rather, each contributes to the overall effort to protect all personnel involved in incident operations.

C. *Liaison Officer (LO):*

The Liaison Officer (LO) is the point of contact for representatives of other governmental agencies, non-government organizations (NGO), and the private sector (with no jurisdiction or legal authority) to provide input on their agency's policies, resource availability, and other incident-related matters. Representatives from assisting or cooperating agencies and organizations coordinate through the Liaison Officer. Agency and organizational representatives assigned to an incident must have the authority to speak for their parent agencies or organizations on all matters, following appropriate consultations with their agency leadership.

Assistants and personnel from other agencies or organizations, public or private, involved in incident management activities may be assigned to the LO to facilitate coordination.

For the initial operations of the District EOC, the LO will coordinate with the IC at the ICP until there are other assisting cooperating agencies involved with the response. For incidents that require multiple operational periods, the EMC and the Operations Section Chief will eventually become the primary contacts with the IC, while the LO takes on other coordination duties.

D. *Other Command Staff, as required:*

During an emergency there may be a need for legal consultation, technical/medical advice, as well as additional security for the EOC. The IC and the EMC may assign representation for these functions. The EMC may make requests for this support from the EPG.

4. **General Staff:**

A. *Operations Section Chief:*

This position is responsible for all tactical activities focused on reducing the immediate hazard, saving lives and property, establishing situational control, and restoring normal operations. Lifesaving and responder safety will always be the highest priorities and the first objectives in the Incident Action Plan (IAP)

developed in coordination with the Planning Section Chief and approved by the EMC.

In catastrophic incidents, the District may request outside support to expand positions in the ICS structure for the Operations Section by activating any or all of the following Branches that report to the Operations Section Chief:

- Search and Rescue
- Emergency Medical Services
- Assembly and Accountability
- Fire
- Law
- Hazardous Materials
- Air Support
- Staging
- Reunification
- Mass Casualty and Temporary Morgue Operations

B. *Planning Section Chief:*

The Planning Section Chief collects, evaluates, and disseminates incident situation information and intelligence to the IC at the ICP, and/or to the EMC and incident management personnel. This Section prepares status reports, displays situation information, maintains an evaluation of resources assigned to the incident, and prepares and documents the IAP, based on Operations Section input and guidance from the IC or the EMC.

In catastrophic incidents, the District may request outside support to expand positions in the ICS structure for the Planning Section by activating any or all the following to report to the Planning Section Chief:

1. Resources Unit:
   Responsible for recording the status of resources committed to the incident. This Unit also evaluates resources committed currently to the incident, the effects additional responding resources will have on the incident, and anticipated resource needs.

2. Situation Unit:
   Responsible for the collection, organization, and analysis of incident status information, and for analysis of the situation as it progresses.

3. Demobilization Unit:
   Responsible for ensuring orderly, safe, and efficient demobilization of incident resources.

4. Documentation Unit:
   Responsible for collecting, recording, and safeguarding all documents relevant to the incident.

5. Technical Specialist(s):
   Personnel with special skills that can be used anywhere within the ICS organization.

C. *Logistics Section Chief:*

The Logistics Section Chief is responsible for all service support requirements needed to facilitate effective and efficient incident management, including ordering resources from off-incident locations. This Section also provides facilities, security (of the incident command facilities and personnel), transportation, supplies, equipment maintenance and fuel, food services, communications and information technology support, and emergency medical services.

In catastrophic incidents, the District may request outside support to expand positions in the ICS structure for the Logistics Section by activating any or all of the following that report to the Logistics Section Chief:

1. Supply Unit:
   Orders, receives, stores, and processes all incident-related resources, personnel, and supplies.

2. Ground Support Unit:
   Provides all ground transportation during an incident. In conjunction with providing transportation, the Unit is also responsible for maintaining and supplying vehicles, keeping usage records, and developing incident Traffic Plans.

3. Facilities Unit:
   Sets up, maintains, and demobilizes all facilities used in support of incident operations. The Unit also provides facility maintenance and security services required to support incident operations.

4. Food Unit:
   Determines food and water requirements, plans menus, orders food, provides cooking facilities, cooks, serves, maintains food service areas, and manages food security and safety concerns.

5. Communications Unit:
   Major responsibilities include effective communications planning as well as acquiring, setting up, maintaining, and accounting for communications equipment.

6. Medical Unit:
   Responsible for the effective and efficient provision of medical services to incident personnel.

D. *Finance/Administration Section Chief:*

A Finance/Administration Section is established when the incident management activities require on-scene or incident-specific finance and other administrative support services. Some of the functions that fall within the scope of this Section are recording personnel time, maintaining vendor contracts, administering compensation and claims, and conducting an overall cost analysis for the incident. If a separate Section is established, close coordination with the Planning Section and Logistics Section is also essential so that operational records can be reconciled with financial documents.

The Finance/Administration Section is a critical part of ICS in large, complex incidents involving significant funding originating from multiple sources. In addition to monitoring multiple sources of funds, the Section Chief must track and report the accrued cost as the incident progresses. This allows the IC and/or the EMC to forecast the need for additional funds before operations are negatively affected.

In catastrophic incidents, the District may request outside support to expand positions in the ICS structure for the Logistics Section by activating any or all of the following to report to the Finance/Administration Section Chief:

1. Compensation/Claims Unit:
   Responsible for financial concerns resulting from property damage, injuries, or fatalities at the incident.

2. Cost Unit:
   Responsible for tracking costs, analyzing cost data, making estimates, and recommending cost savings measures.

3. Procurement Unit:
   Responsible for financial matters concerning vendor contracts.

4. Time Unit:
   Responsible for recording time for incident personnel and hired equipment.

7. **Information Collection, Analysis, and Dissemination:**

Emergency operations succeed or fail based on good intelligence. The first half of providing that intelligence is efficient gathering of information:

- Evaluating raw (unverified) data about the event;
- Compiling facts (verified) about the event; and
- Considering possible future conditions (forecasts) that might impact the event and the response.

Confusion occurs in response and recovery facilities when there is no clear protocol on how to find and manage information critical for emergency operations. The following discussion provides those protocols. ICP, EOC, and

EPG staff must consider the Essential Elements of Intelligence (EEI) as a core element of the District/College's concept of operations.

A. *Gathering the Data*

Gathering the data is a critical process. Effective gathering requires using a well-defined system of collection, sorting and filing so that the Planning Section can perform the task of analysis. The ICP/EOC will use its Planning Section to ensure that documentation and analysis are completed efficiently. The Section Chief will define the sources to be used for gathering data.

B. *Collecting and Defining Sources*

There are hundreds of sources that could be used for gathering information during emergencies. These include, but are not limited to, these potential resources:

- Blinn College District Police Department
- ICP/IC
- District PIO
- Radio stations/programs
- TV stations/programs
- Government agencies (officials contacted directly)
- Private agencies (through the Liaison Officer)
- Warning system (EAS and NOAA Radios)
- Other response/recovery centers at the local and state level

C. *Analyzing the Content*

There are three key measurements needed to transform raw information into intelligence *once* it is gathered from the specified sources of information.

It is important to verify the data for accuracy:

1. Is the information correct?
2. Can the source be identified, contacted, and trusted?
3. Does this information conflict with or contradict other information verified as accurate?

Information must be tested for relevance:

1. Does the information relate to the District's concerns about the emergency or critical incident?
2. How will this information affect the decision-making process for necessary action(s)?
3. What is the age of the information and is it actionable?

Inspect for mission value:

1. Is the content generated clear and readily understandable?

2. Is the content organized in a manner that can assist in clarifying specific mission objectives for taking action(s)?

D. *Categorizing Analyzed Data*

The final step of turning information into intelligence is defining what categories the information should be placed under to classify its best use. This scheme can vary based on the emergency events. For example:

Critical life-safety information for immediate dissemination to the IC and/or EMC:

1. Injuries requiring aid

2. Active gunfire or explosions

3. Approaching "cloud" of hazardous material

4. Individuals trapped in burning or collapsed building(s)

5. Advancing waters approaching occupied area

Information requiring advanced planning:

1. Weather predictions

2. Flooding expectations

3. Potential utilities disruptions

4. Expected resource shortages

5. Uncontrolled fire spread predictions

Discipline-related intelligence:

1. Search and Rescue operations

2. Medical Care and Triage

3. Reunification

4. Facilities condition

5. Debris Removal

6. Law Enforcement

7. Fire Response

Situation Status Reports:

1. Current situation report (SITREP)

2. Summary of deployed District assets and personnel

3. Jurisdictions and agencies actively involved

4. District operations and facilities impacted

5. Injuries, deaths, and financial losses

It is important to remember that all information, documentation, request forms, notes and official correspondence created and/or utilized during the operation period of the emergency or critical incident must be maintained as it will be necessary for federal reimbursement, if applicable, and required for the official After Action Repot (AAR). Archival information includes, but is not limited to:

1. SITREPS

2. Logs and Logbooks

3. E-mail correspondence

4. Photographs of status boards

5. BlinnALERT mass communications

6. Media Releases

7. Captured media reports regarding event

E. *Intelligence Use*

ICS clearly defines intelligence processes as being the role of the Planning Section, unless a specific Intelligence Unit is moved/located in another Section, or under the Command Staff. However, it is every ICP/EOC member's responsibility to recognize critical information. Training should provide all staff with the understanding that life-and-death information needs to be addressed immediately and shared with all IC/EOC staff.

Data that is compiled, analyzed and evaluated does not become actual intelligence until it is available to people who can use it to make decisions and take action. The priorities for distribution of intelligence in the ICP/EOC will be as follows:

1. The IC/EMC has access to all information but depends on the Planning Section Chief to focus on the most important parts of intelligence reports relevant to the concern at the moment, and for critical advance planning.

2. The Safety Officer receives copies of all reports and is immediately informed of any intelligence involving the safety of people involved in the response.

3. The PIO has access to all information generated in the ICP/EOC. Specific, complex issues should be discussed between the Planning Section Chief and the PIO prior to releasing intelligence in news releases or preparing public statements for the District. The PIO will also share any key data with

the Planning Section when that information is acquired from monitoring media sources.

4. The Planning Section is responsible for gathering and compiling, analyzing and verifying, and evaluating all data. The Section develops Advance Plans and Situation Status Reports from all available intelligence. The Planning Section Chief is responsible for ensuring all intelligence is provided in a timely manner to the correct ICP/EOC staff. All ICP/EOC staff should have copies of the Situation Status Reports and be able to see the status boards, which are updated with time-sensitive intelligence. The Planning Section also provides all ICP/EOC participants with copies of the Incident Action Plan, which has all the operational objectives for the Operational Period.

5. The Operations Section receives fast-breaking intelligence and intelligence related to specific disciplines, such as search and rescue or medical operations. The Operations Section also receives the Advanced Planning reports from the Planning Section. The Operations Section Chief is responsible for providing reports to the Planning Section for use in Situation Status Reports.

6. The Liaison Officer and Technical Representatives from other organizations receive copies of all reports relevant to their roles.

7. The Logistics Section should receive a copy of all reports generated in the ICP/EOC. Logistics obtains much of its intelligence directly from the Operations Section and from EOC status boards and reports. They should also report relevant, critical data from their Section to the Planning Section Chief, especially regarding resource use and allocation.

8. The Finance/Administration Section should receive a copy of all reports generated in the IC/EOC, but their focus is on data, not necessarily intelligence. Time reporting, costs, etc., are not considered intelligence unless they have relevance to operations decisions. This may occur in the case of ramping up operations or reductions during demobilization. At those times, the data from Finance/Administration should go through the intelligence process before it is provided to the IC/EMC. This is the responsibility of the Planning Section in coordination with the Finance/Administration Section Chief.

CONCEPT OF OPERATIONS UNDER ICS FRAMEWORK

The overall strategies for designing, preparing, implementing and maintaining the entire emergency program arise from the NIMS concept of operations. These are intended to address the Core Capabilities required for District operations. FEMA/DHS "Core capabilities" relevant to the District's mission are included as an annex to this ERP.

The District's emergency management program must include, at a minimum, the following elements:

- Standardized organization structures, processes and procedures;
- Standards for planning, training and exercising personnel;
- Equipment acquisition and certification;
- Interoperable communications processes, procedures and systems;
- Information management systems; and
- Supporting technologies for voice and data communications, information, data display and specialized technologies.

A. Preparedness

Preparedness involves the readiness of plans and procedures, personnel, supplies and equipment, facilities and agreements with external organizations. Readiness is based on meeting the needs to address the primary threats identified in the risk assessment for the District.

B. Plans and Procedures

The District, through the Director of Safety and Risk Management, in collaboration with the Emergency Management function, develops the ERP and SOPs for the Unified Campus Safety Program (UCSP), and assists BCD Departments to develop their own internal plans and procedures, as necessary, The Director of Safety and Risk Management also works in collaboration with Executive staff to develop other supporting documents that affect emergency readiness, including:

1. Critical Incident Response Team (CIRT) SOPs

2. Blinn College District General Safety Manual

3. Emergency Action Plans (EAPs) for Specific Events

4. Continuity of Operations Plan (COOP)

5. Behavior Intervention Team (BIT)

6. Fire Safety Inspections Protocols and Procedures

7. Laboratory Safety and Chemical Hygiene Plans

During this process, the Director of Safety and Risk Management is responsible for ensuring documents meet District expectations to comply with all federal, state and local laws and regulations, as well as reflecting best practices for effective and safe emergency operations. The overall process for scheduling and managing training is described in the Maintenance section of this ERP.

C. Continuity of Operations Plan (COOP) - Concept

The District or Continuity of Operations Plan (COOP) ensures a process to continue operations no matter what incident may cause interruptions. The following discussion summarizes the process for the District to follow to maintain essential functions throughout all emergencies. Specific directions and D tactics are found in the official COOP.

D. Vital Records Retention

Vital records include financial data, licenses, legal agreements, contracts, databases, and any written communications critical to the essential functions of operations. The District has an Information Technology (IT) emergency policy that directs preservation of District vital records and ensures they are duplicated and secured at an alternate, safe location on a regular basis. The critical operations records are secured daily. These include primary financial and individual records for staff, faculty and students.

A test of the backup system is completed regularly to verify that the recovery system works. The tests also establish the time expected for data retrieval from storage. This is summarized in the IT COOP.

E. Essential Facility and Infrastructure Protection

The District has considered how to continue operations when there is damage or loss of essential facilities or other infrastructure. To prevent interruption of service, the District established alternate locations to continue business until the normal operating location is restored. This would only be done when there is major structural damage or long-term threats to the health and safety of people at the District offices and/or campuses.

These sites should have nearly the same operating capacity and resources as the primary locations. Test should be complete through, at least, a tabletop drill to evaluate the ability of moving and working from an alternate site. Additional infrastructure protection includes security measures, mitigation from major threats, and standard maintenance.

F. Special Legal Emergency Planning Considerations: Clery Act, FERPA, HIPAA, ADA, PFA

A series of laws affect emergency protocols included in District plans and procedures, especially regarding the access to student, staff and faculty personal records, which can become critical for public health and safety, the treatment and care of emergency victims, and for reunification with families. The District must take these laws into consideration during preparation of their concepts of operations.

1. Jeanne Clery Disclosure of Campus Security Policy and Campus Crime Statistics Act **(Clery Act)**

The Clery Act requires clear communications and notifications about criminal activity on or near District properties as well as timely emergency notifications to those on District properties when emergency conditions arise. The District follows the requirements of the Clery Act for criminal notifications through operations of the BCDPD. Criminal activities that are not generally considered emergency conditions are managed separately from the District ERP. There are special considerations for dormitory occupants as the District operates on-campus housing at the Brenham Campus.

Emergency notification processes, including criminal behavior that does qualify as an emergency incident (active shooter, violent protest, bomb threat, etc.) are collaboratively managed with BCDPD, District Communications, and District Executive staff. A pre-defined message system with protocols known as BlinnALERT is in place to speed the process for limited and full-District notifications. It is evaluated after drills, exercises and actual emergencies. It is effective and timely and meets best practices found for colleges and universities. The emergency notification system is used frequently throughout the year for drills, exercises and actual incidents. The effectiveness of emergency notifications is evaluated in NIMS-required After-Action Reports (AARs).

The District uses BlinnALERTs for a wide range of emergency notifications to staff, faculty and students. However, it is not currently mandatory for students to participate. The BCDPD also has a select listing of key contacts who receive emergency e-mail, text and phone call notifications directly from the BCDPD personnel involved in any emergency or critical incident. Each campus also has the ability to activates it's CIRT to perform protective actions for buildings at risk during emergency incidents, including evacuations, shelter-in-place and lockdowns.

These systems are used for general threat notifications, specific emergency warning and notifications, and for post-event information such as reunification directions and campus closure/reopening messages.

Emergency public information (EPI) for the general public is provided appropriately through the news media, through social media sites and contacts, and through media briefings in accordance with the District Crisis Communications Plan.

2. Family Educational Rights and Privacy Act **(FERPA)**

Access to student records (academic, health, criminal) that are held by the District must be handled under the strict legal constraints of the Family Educational Rights and Privacy Act (FERPA). FERPA is primarily a legal concern for daily operations of District programs. However, it does have a bearing during emergency incidents when student information is critical for the

public health and safety. There is a specific exception in that case for disclosure of personal identifiable information (PII).

District officials may disclose PII from education records without consent to appropriate parties only when there is an actual, impending, or imminent emergency, such as an articulable and significant threat (an emergency event where the information is clearly necessary for the protection of public health and safety). Information may be disclosed only to protect the health or safety of students or other individuals. In applying the health and safety exception the District must:

- Determine what constitutes a health or safety emergency.

- Define who "appropriate parties" includes, such as law enforcement officials, first responders, public health officials, trained medical personnel, and parents (including parents of an eligible student).

- Recognize that this FERPA exception is temporally limited to the period of the emergency and does not allow for a blanket release of PII. It does not allow disclosures to address emergencies that might occur, such as would be the case in emergency preparedness activities.

- Ensure that information that may be disclosed is limited to only PII from an education record that is needed based on the type of emergency.

- Ensure that disclosures based on this exception must be documented in the student's education records to memorialize the Emergency that formed the basis for the disclosure; and

- Record the parties with whom the District/College shared the PII.

3. Health Insurance Portability and Accountability Act **(HIPAA)**

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is implemented through two parts called Titles. Title I protects health insurance coverage. Title II requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers. Title II has specific restrictions on the sharing of health information that is relevant to District operations, especially when minors are enrolled participants in District activities and are present during an emergency. This act gives the right to privacy to individuals from age 12 through 18. Under most circumstances the District must have a signed disclosure from the affected minor before giving out any information on provided health care to anyone, including parents. Title II also addresses the security and privacy of health data for minors and adults to other parts of the healthcare system and defined appropriate authorities. When this information becomes part of a student record it is also connected to FERPA. District staff and faculty information are also protected under Title II.

The most important exception to these restrictions is when public health and safety is threatened. This is relevant to a disease outbreak emergency, e.g., a pandemic disease. Under the health or safety emergency exception, school officials may, without consent, disclose PII from education records to appropriate parties in connection with an emergency. In the case of an influenza outbreak, for instance, if District officials determine that an emergency exists, they may share immunization records with parties, such as state and local public health officials, whose knowledge of the information is necessary to protect the health or safety of students or others in the campus community. Under this exception, the District may share information only during the limited period of time connected with the emergency. A blanket release of information is not allowed. The District must instead determine what information to disclose on a case-by-case basis depending on the particular threat.

4. **Americans with Disabilities Act (ADA)**

The District works diligently to comply with the Americans with Disabilities Act (ADA) through its District Human Resources Department. Title II of the ADA prohibits discrimination on the basis of disability, and generally would prohibit unnecessary disclosures of disability status, or information related to that disability, to third parties. Disclosures may be necessary when the student presents a significant, articulable threat to others, including before, during, or after emergency declarations. This would include records on services and accommodations provided to students under Section 504 of the Rehabilitation Act of 1973, and Title II and Title III of the ADA.

5. **Psychological First Aid (PFA)**

Psychological First Aid (PFA) is an evidence-informed modular approach used by mental health and disaster response workers to help individuals of all ages in the immediate aftermath of disaster and terrorism. PFA is designed to reduce the initial distress caused by traumatic events and to foster short- and long-term adaptive functioning and coping. PFA does not assume that all survivors will develop mental health problems or long-term difficulties in recovery.

Instead, it is based on an understanding that disaster survivors and others affected by such events will experience a broad range of early reactions (e.g., physical, psychological, behavioral, spiritual). Some of these reactions will cause enough distress to interfere with adaptive coping and recovery. This can be reduced by support from compassionate and caring disaster responders. The District supports early and continual application of PFA through Human Resources programs. For more information on PFA see the Psychological First Aid – Field Operations Guide:

http://www.nctsn.org/content/psychological-first-aid

G. Blinn College District Emergency Teams

The Director of Safety and Risk Management provides guidance for the selection of emergency support teams throughout the District so the daily skills and interests of the team members are a close match to assigned roles and responsibilities on response and recovery teams. The Director of Safety and Risk Management works closely with District Executives, College Safety Committees and Emergency Planning Committees to define the team size, membership, training and equipment needs for the following teams:

- **Incident Management Team (IMT)**

- **Emergency Response Team (ERT)**

- **Critical Incident Response Team (CIRT)**

- **Behavior Intervention Team (BIT)**

- **Emergency Policy Group (EPG)**

Team membership is typically voluntary except for team membership specifically defined within this District ERP. District personnel may, as appropriate, be required to perform in a team as part of their job description.

1. *Training Qualifications*

Training is the key to the success of the ERP at the District. Teams and Executive Officers will be required to participate in regular training. The table on the following page summarizes the types of training for each team. The table reflects minimum classroom training. However, the BCD Chancellor and/or the BCD EMC may mandate additional training at any time in order to meet the evolving needs of the District and changes to laws, guidelines, best practices and BCD Board of Trustee policies concerning emergency response protocols. Team members may choose to independently complete any additional training that specifically compliments or improves a team's performance. All formal training should be recorded and tracked by the Director of Safety and Risk Management.

BLINN COLLEGE DISTRICT EMERGENCY TEAMS

DISTRICT EMERGENCY TEAM	Incident Command System (ICS)	Basic Protective Actions for Building Occupants	EOC Operations	Crisis Management Techniques	Continuity of Operation Plan (COOP)	1st Aid, CPR, AED, Bleed Control
Incident Management Team (IMT)	◉	◉	◉	◉		◉
Emergency Response Team (ERT)	◉		◉	◉		◉
Critical Incident Response Team (CIRT)	◉	◉		◉		◉
Emergency Policy Group (EPG)	◉			◉	◉	
Behavior Intervention Team (BIT)				◉		

ICS Courses 100 HE (or equivalent), 200, 700, 800 are required of ERT members. BCDPD staff have additional training to include 300, 400.

In addition to formal classroom and online training, all team members and Executive staff in the Emergency Policy Group must participate in at least one planned drill or exercise each year. Participation in response to a real incident satisfies this requirement.

All formal training and drill/exercise participation requires proof of involvement through sign-in sheets used at the time of the incident, or through certificates from providing organizations.

If participants do not complete their training as required within a calendar year the District administrator managing a non-compliant team member will be asked by the Director of Safety and Risk Management to provide a written explanation of why compliance was not met, including action steps to be taken by the administrator of that team member to ensure the team meets compliance as soon as possible. Failure to maintain training qualifications places the District at risk of not meeting federal NIMS requirements.

2. *Supplies, Equipment and Facilities*

The EPG, CIRT and BIT do not require unique facilities, equipment or supplies. Their tools are their plans, procedures, and laptop computers. They can meet in any facility that provides adequate communication tools in a safe and secure environment.

The ERT, however, requires an Emergency Operation Center (EOC) (primary and secondary) with the capacity to be secure, habitable and meet all the operational needs

as designated in the checklist in the Annex to this Plan. The EOC must have supplies at the ready for operability 24/7. The facility need not be solely dedicated as an EOC, but others using the site must understand that during an incident requiring ERT activation that any other activities are secondary to the incident response.

The CIRT requires plans and procedures, as well, but they also need to have kits personally assigned and available, as well as pre-identified Assembly Areas that allow appropriate distance from the building at risk in various directions which allow safe movement of evacuees in a direction away from the threat, depending on the incident.

Other Blinn College District personnel are expected to take a role in an incident. BCDPD officers have some equipment appropriate for unique incidents, including limited personal protection equipment (PPE) for hazardous materials. BCDPD is also responsible for ensuring their officers, who often become the initial Incident Commander (IC), have the supplies and equipment to establish and operate an Incident Command Post (ICP) near the threat location. District Facilities and Maintenance personnel maintain floor maps and utility maps of the District sites for reference, if needed, by first responders or the ERT. All of this equipment, the supplies and the facilities must be standardized and maintained for deployment as needed.

3. *Formal Agreements with External Organizations for Emergency Support*

The Chancellor shall appoint the BCDPD Chief of Police, who serves as the EMC, as the coordinator for all District Department of Homeland Security (DHS) issues, including external agreements. Any District location contacted or in communication with an outside organization regarding homeland security request(s) or issue(s) shall provide notification and regular updates to the EMC. All District formal, written emergency agreements with external organizations must be approved by the Chancellor and may have to be approved by the Board of Trustees.

4. *Response Capabilities of the District/Colleges*

The planning and preparedness process should ensure that the District has defined and developed the appropriate core capabilities for response required under the NIMS guidance. The response capabilities currently noted as appropriate for the District/Colleges are found in the appendices of this ERP.

H. Response

Response is comprised of activities that address the short-term, direct effects of an incident. These may include:

- Immediate actions to save lives, protect property and meet basic human needs;

- Declaration of a District-wide or emergency;

- Activation of the District ERP/SOPs and response teams;

- Initial threat and damage assessments;

- Coordination with supporting agencies and organizations to control the threat;

- Continual evaluation of the threat to develop objectives to protect lives, property and the environment;

- Application of intelligence and other information to lessen the effects or consequences of the threat;

- Increasing security and law enforcement operations to protect people, property and the environment;

- Increased health surveillance and testing (physical and mental) as needed, depending on exposures to vectors, agents and trauma during the incident.

Incidents often follow a pattern that allows effective management of the impacts from the threat. Response processes can be categorized as pre-response, initial response and continuing response activities.

1. *Pre-Response Readiness*

The following actions are typically completed when there is a 24 to 36-hour lead time before an emergency incident occurs (severe weather, violent protest, disease outbreak, etc.). These actions cannot be taken in a timely manner in fast-breaking events (active shooter, hazardous materials spill, bomb threat, fire alarm, etc.)

A. Situational Awareness

1. District Executive and Department Management personnel are responsible for situational awareness of threats that may rise to create an emergency situation.

2. Threats may be easily recognized based on seasonal, geographic and historical reference points.

3. Information should be monitored through the media, from warning services (like NOAA all-hazards radios), daily briefings and BCDPD updates.

4. District Executives are responsible for maintaining a Common Operational Picture (COP) for the District that includes recognizing major threat potentials and ensuring the readiness to address them.

B. Plans and Procedures

District authorities responsible for coordinating and maintaining emergency plans and procedures should verify that the documents are sound and ready for use if there is an impending threat. This includes ensuring that teams have the latest copy of approved documents, especially checklists and required forms.

2. *Equipment, Supplies and Facilities*

District authorities responsible for coordinating and maintaining emergency readiness should verify that emergency equipment, supplies and supporting facilities (like the

EOC) are complete, available and that facilities are habitable if needed for use if there is an impending threat. This includes ensuring that teams have checked their kits and materials, communications, and know that either a primary or secondary facility has been designated for use.

3. Team and Key Personnel Readiness

When teams are advised that they may be activated, their responsibility is to ensure they are capable of fulfilling their role (which could be comprised by health, family conditions, or other compelling issues); that they have their documents, equipment and supplies in readiness; and that they know who they would report to and where if the threat requires an emergency activation. At this stage they should also provide current contact information to their supervisor so they can be notified quickly.

4. Emergency Communications

a. The District must maintain emergency communications equipment, systems, software and personnel training.

b. Pre-incident tests of key notification and warning systems are to be completed when the likelihood of an emergency incident is likely within a day of a threat's arrival.

c. Emergency pre-scripted messages should correlate with the standards set by the Integrated Public Alerts and Warning System (IPAWS) and the Commercial Mobile Alert System (CMAS) established at the Federal Emergency Management Agency (FEMA), when they are to be released through local government to the general public.

d. Response teams should ensure batteries for their radios are charged and that their radios are operational on no less than a monthly basis.

e. BCDPD should ensure that it is capable of meeting the Clery Act requirements for timely notification of a criminal act that may qualify as an emergency incident.

f. All District response teams should be briefed, if possible, prior to an emergency to remind them of restrictions on handling and transmitting sensitive personal information under the Clery Act, FERPA, HIPAA and ADA laws.

g. BlinnALERT notifications shall be used to alert CIRT and key staff per procedure for immediate life-threatening incidents.

5. Initial Response and Threat Identification

The recognition of the threat and the classification of its type (natural, technological, human caused) should be based on the hazard/threat evaluation chart in this ERP. The final decision on the threat identification can be made by:

a. The Chancellor and/or Executive Vice Chancellor, or their designee for a District-wide incident

b. The EMC

c. An offsite emergency responder acting as the IC

d. An offsite emergency management authority (City/County or Governor) for local, regional or statewide incidents.

6. *District/College Emergency Declaration and "Trigger Chart"*

The initial activation of the District ERP and the response teams and resources should occur quickly, in accordance with the pre-agreed upon conditions in a declaration trigger chart (or based on the seriousness of the kind of incident threat when it is not listed specifically in the emergency declaration trigger chart). The District emergency activation chart is provided as an annex to this ERP.

Declarations may be more conservative than the guidance in the activation trigger chart, but never less conservative.

A. <u>District Emergency Declaration Authority and Process</u>

The authority to declare a District emergency rests with the Chancellor or their designee if conditions allow. A District emergency declaration gives the District immediate authority to take protective actions and to activate teams and resources to protect the health and safety of students, faculty, staff and visitors.

1. The authority to declare a District-wide emergency declaration rests with the Chancellor, Executive Vice Chancellor, or their designees (in line of succession) when there is:

2. An incident that severely impacts District campuses;

3. An incident that has caused multiple fatalities on District property;

4. An incident which caused the District Chancellor (or their designee) to declare an emergency and the college has activated their ERP;

5. An incident that directly impacts two or more campuses;

6. A threat is moving toward the any facility/campus of the District, which may cause major damage and injuries/deaths if immediate actions are not taken (e.g., massive flooding predicted, wildfire approaching, tornado on the ground, civil unrest, etc.).

B. <u>Incident Level Identification</u>

1. Incident complexity determines the numbers and types of emergency and incident response personnel and resources needed to respond effectively.

2. As defined below, it is unlikely that this Emergency Plan would be activated for any incident defined by NIMS as level 4 or 5. Most District incidents that require initial protective actions are at the 4 or 5 level of complexity. They are usually completed, with an 'All Clear' given, within an hour or less. BCDPD (or someone with the most experience at the incident scene) would establish an

initial Incident Command Post (ICP), but there would not be enough time to establish a formal ICS structure like the Emergency Response Team. The CIRTs throughout the District would work within this limited time frame, but they are not part of an ICS structural framework. They are strictly a response team for protective actions that support ICS and NIMS concepts. It is also doubtful that a District-wide emergency declaration would occur for anything other than a 1-or-2 level incident. The five levels of emergencies are defined in NIMS as the following:

TYPE 1

- This type of incident is the most complex, requiring national resources for safe and effective management and operation.

- All command and general staff positions are filled.

- Operations personnel often exceed 500 per operational period and total personnel will usually exceed 1,000.

- Branches need to be established.

- A written incident action plan (IAP) is required for each operational period.

- The agency administrator will have briefings and ensure that the complexity analysis and delegation of authority are updated.

- Use of resource advisors at the incident base is recommended.

- There is a high impact on the local jurisdiction, requiring additional staff for office administrative and support functions.

TYPE 2

- This type of incident extends beyond the capabilities for local control and is expected to go into multiple operational periods. A Type 2 incident may require the response of resources out of area, including regional and/or national resources, to effectively manage the operations, command, and general staffing.

- Most or all the command and general staff positions are filled.

- A written IAP is required for each operational period.

- Many of the functional units are needed and staffed.

- Operations personnel normally do not exceed 200 per operational period and total incident personnel do not exceed 500 (guidelines only).

- The agency administrator is responsible for the incident complexity analysis, agency administration briefings, and the written delegation of authority.

TYPE 3

- When incident needs exceed capabilities, the appropriate ICS positions should be added to match the complexity of the incident.

- Some or all the command and general staff positions may be activated, as well as division/group supervisor and/or unit leader level positions.

- A Type 3 IMT or incident command organization manages initial action incidents with a significant number of resources, an extended attack incident until containment/control is achieved, or an expanding incident until transition to a Type 1 or 2 IMT.

- The incident may extend into multiple operational periods.

- A written IAP may be required for each operational period.

TYPE 4

- Command staff and general staff functions are activated only if needed.

- Several resources are required to mitigate the incident, including a task force or strike team.

- The incident is usually limited to one operational period in the control phase.

- The agency administrator may have briefings and ensure the complexity analysis and delegation of authority is updated.

- No written IAP is required but a documented operational briefing will be completed for all incoming resources.

- The role of the agency administrator includes operational plans including objectives and priorities.

TYPE 5

- The incident can be handled with one or two single resources with up to six personnel.

- Command and general staff positions (other than the incident commander) are not activated.

- No written IAP is required.

- The incident is contained within the first operational period and often within an hour to a few hours after resources arrive on scene.

- Examples include a vehicle fire, an injured person, or a police traffic stop.

I. **Activation of the District ICS Operations**

Once a threat is recognized and the conditions reach an emergency declaration trigger, the District/College will take immediate actions to activate resources and take protective actions to protect the health and safety of staff, faculty, students and visitors. Initial actions may occur even before Executive staff have declared an emergency, especially if first response personnel are at the scene of an incident in progress and immediate life-protection actions must be taken. First responders have the duty and authority to make those decisions without prior approval or declarations.

1. *Incident Command Post Establishment*

In the case of a major incident (1 through 3), the Incident Commander (IC) (usually an BCDPD officer on scene) shall immediately establish an Incident Command Post (ICP) location and activate the appropriate protective actions necessary to safeguard individuals, property, and maintain normal operations for educational facilities. The Incident Commander shall immediately consult with the EMC and Campus Dean if the incident is on a campus, or the Chancellor (or their designee in line of succession)

when the incident is primarily on other District properties. The IC will brief the Executives regarding the emergency and the need for a declaration and activation of teams and taking of protective actions, including notifications.

In level 4 incidents, the ICP will be established, if only for a brief time, in order to coordinate with District Executives and multiple emergency response disciplines (law, fire, EMS, public works, health, etc.). The EMC can prepare the ERT for additional activation if the threat worsens.

Appropriate warning notifications should be sent to the appropriate target audiences about the safety of the area and if an 'All Clear' has been issued.

In level 5 incidents, the responder in charge still becomes the IC, but no other formal ICS command structures are usually needed for a minor operation that can be managed in several hours or less, including any protective actions. District Executives are still informed, but no formal actions are needed, outside of general notifications about the incident and whether it is now safe in the area where it occurred.

2. *Protected Entry Access After a Declaration*

   a. Once an emergency declaration is made, only registered employees, administration, registered students, and affiliates (i.e. persons required by employment) are authorized to enter onto District properties. Individuals without proper ID shall be asked to leave. Unauthorized individuals attempting to enter District properties that are under emergency declarations may be subject to arrest in accordance with the Texas Penal Code.

   b. Media may have access to the District properties during an emergency but may not in any way impede or interfere with protective actions, emergency team operations or first responder activities, or infringe on the privacy of staff, faculty, students or visitors. Failure to follow the directions of first responders in a disaster may make media members subject to arrest in accordance with the Texas Penal Code.

3. *Activation of Emergency Teams*

   a. The District Executive level will not typically initiate the use of emergency teams (ERT or CIRT) at a level 5 or 4 incident, unless there are compelling reasons to provide support from an ERT or provide protective actions from a CIRT.

   b. At level 3, 2 and 1, District and College ERT and BATs will be activated. They may be activated by:

   c. Direct notification by phone from an Executive in the line of succession for the District

   d. Notification by BlinnALERT

   e. Alarms activating in a building

f. First responder directions (e.g., BCDPD requesting assistance to evacuate a building or shelter-in-place)

g. Self-activation from general awareness of the incident threat (e.g., see fire or smoke, hear about incident from other reliable staff/faculty, news announcements such as NOAA weather alert of a warning to take immediate action)

h. Additional organizational elements such as BCDPD, Safety and Risk Management, Facilities Maintenance, Public Relations etc., that support each campus and satellite locations, will be mobilized to provide the degree of support commensurate with the requirements of an incident at the individual campuses.

i. If the District ERT is activated, the EMC will provide a written list of people with authorized access to the EOC who serve on the ERT, to an BCDPD officer on scene to ensure control at the EOC, and access through any law enforcement control points restricting access to the area.

4. *Initial Response Capabilities*

    a. <u>Immediate Protective Actions</u>

    First responders at any incident scene have the authority and responsibility to take whatever immediate actions are needed to protect human life and safety. They can take this action without approval from any other authority.

    If, and when, a CIRT leader is present and functional they will work in coordination with the BCDPD or other first responders to take any and all protective actions to address public health and safety. Actions may include:

    - Evacuation to an outside designated Assembly Area

    - Reverse Evacuation (relocating back inside another building when the conditions outside further threaten people)

    - Lockdown

    - Shelter-in-Place

    b. *<u>Direction and Control</u>*

        1. Upon determination that a District-wide emergency exists, (through coordination with any existing Incident Commander at the scene, BCDPD, and Safety and Risk Management) the Chancellor (or their designee in line of succession) shall activate the Incident Command System (ICS) for the District and the District ERP.

        2. The person with the most experience and authority at the incident scene shall assume responsibility as the Incident Commander (IC). During an incident, decisions directing and/or controlling first responder resources will

be the responsibility of the IC. The Incident Commander will have full authority over first responder actions during the incident.

3. During a District-wide emergency, the Chancellor (or the first available person in their line of succession) should provide formal notification to the IC that they are acting within their authority on District property.

4. An Incident Command Post (ICP) should be located near enough to the incident site to provide ready support and observation, but far enough away to ensure the safety of first responders from any threat (e.g., explosion, inhalation, flooding, etc.).

5. Facilities Maintenance will assist the IC to establish a nearby but safe marshaling area for external emergency response agencies' vehicles, teams and other resources needed for coordination of operations for combined on-site emergency response.

6. The IC will continue to exercise management authority over first responders and will activate elements of the Incident Command Post (ICP) as necessary, following the ICS.

7. If the person acting as the IC is not a first responder, they will be in charge until a first responder can take the IC position during a turnover, with the new IC clearly announcing that they are now in charge as the new IC.

8. If the emergency involves only one building or a small part of a District campus, BCDPD shall secure the emergency scene in cooperation with the CIRT, and as the IC, request support from other BCDPD officers, Dispatch for external first responder support (law enforcement, fire, EMS, etc.) and further request support from the Executives of the Blinn College District (using their line of succession), Facilities Maintenance staff for that campus, Public Relations, and Safety and Risk Management until the emergency is closed and there is an 'All Clear.'

9. The IC and ICP personnel will continue to develop objectives to address the threat in accordance with the priorities of this Plan.

10. Communications will be established with District Executives as soon as possible.

11. If an incident escalates to the point an ERT at the College District level is required, the IC will coordinate with the ERT Liaison Officer in the EOC, or directly with the EMC and Operations Section Chief, depending on the conditions at hand. The IC would continue to lead tactical operations while the EOC ERT would provide resources and strategic support through its coordination with District Executives in the Executive Policy Group (EPG), which would operate separately from the EOC.

12. For District-wide incidents, the Chancellor (or the next available person in the order of succession) should form an Area Command that provides joint resource management at the Chancellor's Level, while tactical initiatives for first responders remain at the ICP.

13. All ICS operations will follow the standard Planning "P" per NIMS standards to organize and operate during response.

14. An Area Command will be established when the complexity of an incident and incident management span-of- control considerations so dictate. Area commands are relevant to incidents such as public health emergencies, given that these events are typically not site specific, and not immediately identifiable, may be geographically dispersed, and evolve over time ranging from days to weeks. It is important to note that an Area Command does not have operational responsibilities.

15. If Washington County forms a Unified Command (after a Local Emergency Declaration occurs), the Chancellor, or their designee, may need to become part of the Unified Command process, especially regarding allocation of strategic resources needed to support District operations. The District maintains its operational authority while supporting a Unified Command structure with the County.

J. Continuing Response

1. *Emergency Response Teams*

a. If an ERT is activated, it will continue to operate in collaboration with the Executive Policy Group (EPG) and with the IC, until such time as it is agreed that the ERT is no longer needed, through a collaborative decision with the EMC, the EPG and the IC (if the IC and ICP is still operational). The ERT will function within the scope of its duties defined within ICS and using the checklists found for its operation in the EOP Annex.

b. The CIRTs will be activated, or self-activated, as previously defined. They will complete their efforts to perform protective actions to protect the health and safety of all staff, faculty, students, vendors and visitors until there is an 'All Clear' provided by the appropriate District authority.

c. The Continuity of Operations Plan (COOP) may be activated during this period to begin the processes of reestablishing normal District operations as the incident moves into the recovery stage.

2. *Facility Operations*

a. If an ERT is activated, it will operate from a primary or alternate EOC.

b. If an EPG is activated, it will work typically from an office near the District Chancellor's Office (if habitable), or for District-wide emergencies, from a space or building near the Chancellor's Office.

    c. The CIRTs will work initially from their assigned floors and buildings, and then move to the selected Assembly Area(s).

    d. All other personnel and/or ad-hoc teams will utilize appropriate and available space to carry out their assigned duties.

3. *Resource Management*

    a. All teams and ICS participants will coordinate resources within the protocols defined in the ICS and the NIMS processes. Critical resources may be withheld from the District depending on a greater need in the surrounding community. Private sector resources may also become scarce during major regional disasters.

    b. In a local or state of emergency, elected officials may choose to extract resources from the District to assist greater needs for others within Washington County or the State of Texas at large. In a federal declaration, federal authorities may also reallocate any public or private resources defined as critical for life safety operations.

    c. In all cases, the District will manage the selection, allocation, use, cost and return of its resources for any declared emergency such that resources are used effectively, efficiently and in a safe manner. Costs for external use of District resources may be allowed, so resources allocated by outside agencies will be tracked for future reimbursements if available.

4. *Communications and Information Management*

    a. All teams and ICS participants will provide timely and effective communications to all the primary participants responding to the incident, and with internal and external stakeholders in accordance with protocols defined in the ICS and the NIMS processes.

    b. Interoperability will be supported by all District and first responder organizations so that methods of communication are identified and shared between all responding organizations.

    c. Communication messages must remain accurate, brief and timely to ensure effective decisions are made and for a Common Operating Picture (COP) to be maintained throughout all operations.

    d. Information will be verified and validated before it is distributed.

    e. The ICS standard forms will be the preferred means for distributing critical emergency information on a regular basis to organizations external to the District (as provided in the Annex to this Plan).

5. *Threat Assessment and Damage Assessment*

a. Threat Assessment

The EMC will work with the Planning Section Chief and the Operations Section Chief to evaluate the threat based on the best intelligence available including:

- • Status of vulnerable populations and facilities still at risk

- • Movement of the threat

- • Growing or diminishing impact of the threat

- • Collateral damages and issues related to the threat that were not   identified in the initial response

This assessment will shape the ERT objectives in support of the IC in addressing the ongoing threat(s) until the threat is controlled or removed.

b. Damage Assessment

The EMC will work with the Operations Section Chief to complete an Initial Damage Assessment (IDA) form (as provided in the Annex to this Plan) in order to share this information with the IC, the City/County Emergency Operations Center (if activated), and as the basis for setting strategic goals for recovery.

6. *Reunification*

In major incidents, especially those with multiple casualties, accountability is crucial for eventual reunification of staff, faculty, students and visitors with their family and friends. The District will work diligently during continued response operations to implement effective reunification processes (especially in the case of minors who are located on any District property). The ERT personnel in the EOC can accomplish this by:

a. identifying a safe location separate from distractions and/or media and the general public, but close enough to allow family members to feel connected in proximity to their children/loved ones;

b. Scheduling periodic updates even if no additional information is available;

c. Preparing to speak with family members about what to expect during unification with their child/loved ones (including security measures to ensure the child can be released to the adult); and

d. Providing effective communication with those that have language barriers or need other accommodations, such as sign language interpreters for deaf family members.

e. If reunification is not possible because an individual is missing, injured or killed, how and when this information is provided to families is critical.

f.   The District must determine how, when, and by whom people will be informed if their loved one is missing or has been injured or killed. Law enforcement typically takes the lead on death notifications.

7. *Transition into Recovery*

Recovery begins early in the continued response stage, as soon as life-saving protective actions are completed, and casualties have been treated and/or removed from the incident site. Each incident is unique in its demands for coordination and resource support. However, the leaders in the incident response can measure the need to move out of the response phase and into full recovery mode by noting that the following circumstances are met:

a.   Threat conditions may persist, but are stable and no longer increasing;

b.   Vulnerable people, the District infrastructure, and the environment are no longer in any immediate danger from the threat;

c.   Utilities and communications are restored and stable; and

d.   No additional emergency resources are needed or requested.

When these conditions are all met, the response leaders and teams can be confident that it is appropriate to consider demobilizing staff and deactivating teams and facilities in an orderly process.

8. *Demobilization and Deactivation*

A basic tenet of ICS is that the structure of an organization should match the needs of the incident. When the incident threat no longer requires current ICS structures, leaders of emergency teams and organizations can reduce the size and components of the response structure. This is performed in collaboration with other response organizations so that all parties are aware of the reduction in capacity.

Demobilization of staff for response during a declared emergency typically follows a priority pattern from the bottom up:

a.   At the ICP, positions no longer needed to address the threat or public interests;

b.   At the EOC, ERT support positions below Section Chief, and finally the Section Chiefs. The EMC and the Safety Officer will always be the last two positions to demobilize;

c.   At the JIC, any District PIO representatives;

d.   At the EPG, all members if they are no longer needed for executive policy support; and

e.   At Unified Command for Washington County, as District representatives.

K. RECOVERY

1. *Recovery Goals*

The goal of recovery is to return to operational normalcy and to restore as quickly as possible the infrastructure required to accomplish the District's mission. The ERT EMC and Section Chiefs typically provide direction and overall management of the District recovery effort. The EOC provides the overall operational support necessary to accomplish recovery objectives.

Recovery may take an extended period of time and should be anticipated and planned in all District emergency plans.

The first priority of recovery is the welfare of staff, faculty and students and restoration of the physical site. Support will require a caring and supportive environment sensitive to the physical and mental health needs of people.

The District will assess the emotional needs of all staff, faculty and students to attempt to best determine those who need intervention by a counselor, social worker, psychologist or other mental health professional. The District will arrange as needed, and whenever possible, the appropriate interventions by District Human Resources or by community-based service providers. The District realizes that appropriate group intervention may be beneficial to staff, faculty and students experiencing severe reactions to the incident.

The EOC staff will follow the chain of command as outlined in the EOP when providing information about recovery activities for an incident. All information is to be disseminated through the PIO position in the EOC or other official representatives of the District. It is important to have a single and accurate message being sent out to staff, students, the community and the media. The District staff will make every effort to consider cultural differences when preparing these materials, as well as needs of the ADA community.

Financial recovery and protection of District assets is also crucial to the overall restoration of the District mission to ensure resumption to normal activities. One of the major goals of recovery is to provide for the continuity of operations. This is addressed through District/College Continuity of Operations Plans (COOP). The implementation of the recovery goals will fall initially to the Emergency Response Team (ERT) at the District or impacted campus(s) Emergency Operations Center, and then transferred, as needed, to individual District departments as incident response efforts diminish.

2. *Continuity of Operations Considerations*

The continuity of operations for the District must be considered during the initial response phase and again after the response phase has concluded and the District begins its long-term recovery phase.

The District will use its COOP to define the critical functions and services of the District. Contingency plans must be developed in advance as part of the COOP to ensure that

the essential services/functions can continue during and after a major incident. The COOP contains procedures describing how the District will continue or recover its minimum essential functions.

Essential functions are generally understood to mean those activities that must be performed to achieve the District's critical missions. The District must inventory and prioritize all its functions and determine which ones are truly essential. Specific contingency plans must then be developed, and resources allocated to ensure continuity of each essential function identified as mission critical. District and Senior Executives, as well as Department managers and supervisors, will use these COOP plans to ensure there is minimal disruption to their mission critical services.

The Blinn College District Continuity of Operations Plan (COOP) is available as an annex to the ERP.

3. *Transitioning from full response to initial recovery*

a. Personnel

The first order of business during recovery is to return the organization to normal operations as quickly as possible. The District may need to help staff and their families cope with separations from one another during the long hours required for reopening of the campuses and District offices after a major emergency or disaster.

A substantial effort should be made immediately to support personnel and students who have been traumatized by the incident. This may require paid leave time for counseling for staff and faculty. This may also mean allowing staff time off to repair their own homes and deal with personal loss and grief. Temporary staffing may be required from other campuses outside the disaster area, or from temporary hiring firms. Do not expect personnel to work at their pre-disaster levels of skill until they have had time to process the trauma. This includes management. Ignoring this supportiveness may cause a loss of employee productivity, affect health and behavior, and even the permanent loss of key staff.

b. Infrastructure

During the first hours and days after a major incident (Short-term Recovery Stage), the principal objectives will be to restore the necessary structural elements [facilities, HVAC systems, roadways and grounds] and non-structural functions and resources (power, water, sanitation, telecommunications) to any impacted District site.

c. Mid-term Recovery

In the first days or weeks following a major incident (Mid-term Recovery Stage), the BCD Facilities Maintenance will establish the principal objectives of recovery to ensure the restoration of all pre-identified essential business functions at the District that are considered to be critical to normal business operations, typically defined in the COOP.

d. Roles and Responsibilities

Divisions and Departments normally responsible for performing the critical business functions of the District will be responsible for recovering those functions after a disaster. Mid-term operations may occur concurrently in the EOC and decisions should be made at this stage whether Facilities Maintenance will continue to use the EOC facilities after EOC deactivation or move to another site, or even use a virtual structure.

e. Documentation

It is critical that careful cost documentation is performed early and continuously during response and throughout recovery. District Finance and Administration Section Chiefs should use recovery checklists for recovery operations to ensure this accountability is maintained. This will be required for insurance reimbursement.

Records of actual costs should be filed for auditing and reference for at least three years after recovery is complete. This is required for reimbursements when a federal disaster declaration allows reimbursement, and typically if a State of Emergency provides compensation for response and recovery from the State of Texas.

4. *Long-term Recovery*

During Long-term Recovery, the District's principal objective is to resume normal operations. The EOC will be deactivated and based on the size and nature of the incident, the timeline to resume normal operations depends on the extent of disrupted critical services on campuses or in District offices. Recovery involves restoration of critical infrastructure necessary for normal District operations such as facilities, grounds, water, power, sanitation, HVAC, network services and telecommunications. Ongoing external government emergency operations may hamper recovery activities within the District if resources become scarce in major emergencies. Local, regional and even State–level priorities for resources may reduce access to critical recovery equipment, supplies, tools and expertise.

In addition, the timeline to resume normal operations will be greatly dependent on damage to District sites (structural) and to computer and data management facilities (systems, communications, and non-structural) and non-duplicated vital records.

In a major incident, the recovery efforts may take several weeks, months or even years to complete. The Assistant Vice Chancellor of Facilities, Planning and Construction will collaborate with the Chancellor and Board of Trustees, to define an appropriate facilities recovery timeline.

The District should officially inform its internal stakeholders and then the community at large when the District is recovered and fully operational.

a. Infrastructure Recovery

In smaller events there is typically little challenge to acquiring the kinds of services and materials needed to recover District critical infrastructure. However, in larger events, especially regional catastrophes, necessary resources may be scarce and costly. The

District should prepare a list of the most important resources it will need for long-term recovery. It is in the best interests of the District to make formal agreements beforehand with the providers of these resources and services so there is no question the District will be served if the vendor has access to the needed resources. Setting fixed prices for certain goods and services each year can also reduce "add-ons" when a vendor wants to pass along their own disaster losses to clients. For the most critical recovery elements (e.g., emergency power, food and water, etc.), the District should consider having multiple vendor agreements in case a primary vendor is lost because of the disaster. Having a local, regional, and then out of state vendor for the most critical infrastructure recovery elements is a sound practice.

b. Disaster Assistance

District Executive Management may reach a limit to recovery actions based on available financial assistance. Early recognition helps plan for the next level of support requests. Recovery disaster assistance processes should be tested through tabletop exercises with local, state and federal stakeholders to ensure all parties understand current standards and practices for recovery funding.

c. Documentation

The District is responsible for preparing a system for capturing all costs associated with disaster operations, both for response and recovery. These records will be used for insurance reimbursement.

They may also be used to justify application for state and federal disaster funding applications. If a local or state government has used a District resource (e.g., refrigeration units, facilities for sheltering, food service support, etc.), documentation is critical for reimbursement from the State or federal government for the use/maintenance/repair costs encumbered by the District. The records should be kept at least three years after the recovery is complete.

5. *After Action Report (AAR)*

The District should coordinate with the Director of Safety and Risk Management to produce an After-Action Report (AAR) for the event after response is complete and recovery is the primary activity. The AAR should include:

a. A timeline of major events that involved the District from the beginning of the incident through the stage of recovery at the time of the AAR. This includes major decisions by the District.

b. Losses to the District, including injuries and death, infrastructure damage, loss of funding due to cancellation of classes, loss of other valuable assets.

c. Impacts on the community from interruption or loss of the District, including lost wages, taxes, educational opportunity, and any chemical releases that affected the environment.

d. Total estimated financial losses, including losses of enrollment, staff income, and inability to complete graduations.

e. Actions District management and staff took through their ICS structure with or without the ERT/EOC activation.

f. Support received by government, non-profits, other organizations to assist the District.

g. Lessons learned in the event (what worked well and what needs improvement).

h. Gaps that occurred in the capability to respond and recover—these should be very specific regarding resources, planning, training, communications, coordination with other organizations, etc.

i. Course of Action—what the District plans to do in the future, including updating plans and procedures, training, prevention, mitigation, and any final recovery efforts, and proposed resolutions of identified gaps should be included.

j. Photos of the damage, and the recovery, as well as names of people and agencies who supported the AAR critique.

The AAR shall be retained, indefinitely, by the District and Emergency Management Coordinator.

L. Mitigation

Mitigation is any action of a long-term, permanent nature that reduces the actual or potential risk of loss of life or property from a hazard that is a known threat. An example would be installation of automatic doors for wheelchair access or updating stairwells for emergency evacuation. Mitigation can also involve security actions such as installing shock- resistant glass for offices that handle cash. Mitigation projects sometimes take substantial planning, funding, and sometimes collaboration with community organizations.

Mitigation is an important part of the emergency management process. Mitigation provides value by creating a safer environment and impeding the cycle of disaster damage, reconstruction, and repeated damage. The process of mitigation is considered a two-part process in NIMS. First, there is risk management through prevention. Second, there is an improved sense of situational awareness of threats and collaboration through outreach.

M. Prevention

Risk management and its strategies help reduce the dangers of operating in the all-hazards environment when threats can impact District vulnerabilities.

These strategies include avoidance (e.g., not building structures in floodplains), reduction of impacts when avoidance cannot be completely implemented (e.g., installation of fire sprinkler systems in structures), and acceptance of some or all of the consequences of a particular risk while providing response tools to address the losses (e.g., insurance, mutual aid, response teams.)

Prevention is also accomplished by District Management taking actions to avoid an incident or to intervene to stop an incident from escalating. Prevention is typically an applied process of ongoing activities. For District operations, prevention involves actions to protect lives and property. It involves applying intelligence and other information to a range of activities that may include such countermeasures as:

- Deterrence operations;

- Heightened inspections;

- Improved surveillance and security operations;

- Investigations to determine the full nature and source of the threat;

- Safety enforcement;

- Immunizations of District personnel; and

- Assisting law enforcement operations aimed at deterring, preempting, interdicting, or disrupting illegal activity when such activities relate to District business.

- Identify past losses during incidents and try to identify the root cause for those losses;

- Evaluate neighboring operations to identify new or changing threats that might impact District operations.

Some of the prevention efforts employed by the District include:

- Complying with or exceeding floodplain management and environmental regulations;

- Enforcing building codes for new construction, or repairing or retrofitting existing buildings;

- Identifying and utilizing shelters and safe rooms to help protect people in tornado-prone areas;

- Implementing a vital records program to prevent loss of crucial documents and records;

- Conducting site specific hazard vulnerability assessments of all District locations;

- Management of data regarding historical incidents to support strategic planning and analysis; and

- Development of hazard-specific evacuation routes.

Sometimes prevention can be accomplished through coordinated efforts with the general community. A good example is providing personal safety instructions for students to take home to their families and friends off campus. Other examples include providing guidance for constructing portable emergency kits or supporting vaccinations for influenza before flu season while providing hand-cleansing sites for students, staff, faculty and visitors on campus. All of this is outreach that helps reduce threats not just at the District, but within the community it serves.

The District/College enhances prevention by outreach activities, including:

- Releasing updates of interest regarding seasonal threats or new threats of interest in order to increase situational awareness

- Providing emergency guidance and tools on for District personnel

- Placing posters for specific threats throughout District

- Supporting placement of programmed weather radios in several key locations through the District

- Training staff to recognize the meaning of local public warning systems

- Updating emergency contact phone numbers

- Providing First-aid, CPR, AED and fire extinguisher training to appropriate target audiences

- Developing MOUs and other agreements for resource shortages, response, and recovery

- Following guidance on prevention from local and state government response agencies, FEMA, and DHS.

N. Program Maintenance

The District has the responsibility for maintaining and supporting the Emergency Management Program. The ERP is the basis for the Emergency Management Program. There are other plans related to the EOP that are also used for addressing other types of incidents that may not rise to the level of an emergency, such as those that affect business systems, injuries, the handling of general safety concerns, etc. This ERP is not meant to replace any of those specific plans already in use by the District, but rather to ensure there is clear policy for emergency events from the all-hazards environment.

The Emergency Management Coordinator (EMC) is responsible for preparation and implementation of the District ERP by ensuring regular ERP updates, staff training, placement and readiness of response equipment, agreements as needed with external organizations, and sufficient coordination with other external organizations such as the Washington County Office of Emergency Management.

The EMC is responsible for providing appropriate guidance for acquiring and maintaining the correct tools, supplies and facilities for the various emergency teams throughout the District. Such tools include the ERP, fact sheets and updates provided throughout the year, opportunities to attend training courses in person or online, and briefings when critical new information becomes available, such as legislation or directives regarding how the District will prepare and respond to emergencies.

The EMC will use a basic five-year schedule to plan and implement the various elements of the Emergency Management Program, as described below:

1. *Emergency Response Plan Development*

The EMC works directly with the Director of Safety and Risk Management and District leadership to continually update emergency operations. The EMC is responsible for ensuring the regular review and update of the ERP throughout the District.

The ERP is reviewed on an annual basis for thoroughness and compliance. The emergency team membership and design is reviewed each year for both correctness and completion. Review of the ERP and emergency team structures ensures that District emergency actions result in the best possible outcomes. Items that may require revision are:

- Major changes in laws and regulations
- New compliance guidance for emergency management operations
- Changes in organizations such as the District ERT
- Changes in supporting government organizations or vendors
- Emerging threats that require creation of new or revised plans
- Input from staff, faculty, or other stakeholders for specific changes

2. *Plan Maintenance*

Although the ERP is reviewed annually, The District will perform a complete revision of the ERP, through the EMC, as necessary to ensure the documents are relevant and compliant with current laws and regulations, as well as best practices.

3. *Plan Distribution*

The Director of Safety and Risk Management is responsible for identifying who receives original copies of the ERP, as well as all later revisions. The District may make the full ERP available through a controlled access locations and/or through direct distribution of hard copies when it is appropriate. Printed copies of ERP should be created and distributed, along with electronic copies, to primary offsite emergency response organizations within the county/city of operation, or other agencies as appropriate. Distribution dates and tracking of those receiving the ERP are to be noted on the Distribution Record. The entire ERP should not be shared outside of the District

unless an emergency response organization makes a specific request in writing that is approved by the BCD Chancellor upon advice from the EMC.

Emergency tactics should be handled as sensitive information. As such, a "public facing" electronic copy of the ERP shall be made available on the Blinn College District website, located on the Emergency Management webpage, that does not contain specific annexes that discuss procedures, protocols, and policies concerning law enforcement response to active threats including, but not limited to, active shooters, terrorism, bombings, and information extortion.

4. *Training*

The EMC, through the Director of Safety and Risk Management, is responsible for the formal training of District employees based on the contents of the ERP and any other procedures the District uses to respond to emergencies.

External training is often available through Washington County and the Brazos Valley Council of Governments (BVCOG). Other training is also available for related topic areas, like ICS, through the Texas Division of Emergency Management (TDEM), Texas Engineering Extension Service (TEEX), Federal Emergency Management Agency (FEMA), and Department of Homeland Security (DHS).

Training records will be kept for each person who completed any official training related to the ERP. Those records should be maintained as verification of the District's preparedness and its level of readiness. These training records should be managed by the EMC whenever they are not maintained by the Blinn College District's Human Resources Learning Management System (LMS).

5. *Drills and Exercises*

Drills are small practice sessions of specific elements in emergencies. Testing the emergency lighting, holding fire drills, practicing CPR, and testing back-up generators are all drill applications.

Exercises are larger events that may be low key discussions using a scenario around a table of key policy makers (tabletop exercise), a functional exercise (where the ERT actually meets and plays out a realistic scenario with the ICS structure activated in their EOC), or a field exercise where actual events are played out with movement within and outside the District, sometimes including outside agencies.

Drills and exercises require various levels of performance, but the capabilities of District personnel will improve during actual response and recovery when personnel have had both training and exercise experiences.

RECORD OF DISTRIBUTION

VERSION NUMBER	DATE OF DISTRIBUTION	DISTRIBUTION GROUPS	DISTRIBUTED BY
V.1	October 3, 2022	BCDPD, EPG, ERT, IMT, CIRT, Washington County EMC, RELLIS EMC	A.B. Carlisle
V.1.1	October 2, 2023	BCDPD, EPG, ERT, IMT, CIRT, Washington County EMC, RELLIS EMC	A.B. Carlisle
V.1 (PUBLIC)	October 3, 2022	BCD Webpage – Emergency Management	A.B. Carlisle R. Bray
V.1.1(PUBLIC)	October 2, 2023	BCD Webpage – Emergency Management	A.B. Carlisle R. Bray
V.1.2	August 27, 2024	BCDPD, EPG, ERT, IMT, CIRT, Washington County EMC, RELLIS EMC	A.B. Carlisle
V.1.2 (PUBLIC)	August 27, 2024	BCD Webpage – Emergency Management	A.B. Carlisle R. Bray

PLAN DEVELOPMENT AND MAINTENACE

The Blinn College District Emergency Management Coordinator (EMC) shall be responsible for directing the revision and review process of the Blinn College District Emergency Response Plan (ERP) at least annually and/or under the following circumstances:

• An After-Action Review (AAR) of an emergency or critical incident indicates that changes, revisions or updates to the ERP are necessary,

• Legislative changes and/or new legislation is enacted having bearing on the emergency response protocols of junior colleges which mandate compliance,

• At the request of the Blinn College District Chancellor and/or through formal request of the Blinn College District Board of Trustees.

Any change(s) to the existing ERP, including annual review - even if no change(s) have been made, will be noted in the "Record of Change" section of the plan along with a brief description of the change(s). Additionally, the month, year and version number of the plan shall be updated as well as the record of distribution, indicating that the ERP has been appropriately distributed to key stakeholders.

RECORD OF CHANGE

CHANGE NUMBER	DATE OF CHANGE	DESCRIPTION OF CHANGE	CHANGE MADE BY:
1	September 27, 2022	Creation of new Emergency Response Plan to satisfy requirements of TEC 37.108 and TSSC guidance. This ERP replaces both the BCD ERP of 11/4/14 and BCD EPM of 10/21/14.	A.B. Carlisle
2	September 28, 2023	BCD ERP Reviewed by EMC, Asst. EMC, and Dir. S-RM. Existing Annex 9 (AS9) – FEMA/DHS Core Capabilities replaced by new Annex 9 – Hazardous Materials and Train Derailment Response. Table of Contents updated. No additional changes recommended during annual review process	A.B. Carlisle
3	August 27, 2024	BCD ERP Reviewed by EMC, Asst. EMC, and Dir. S-RM. Existing Annex 12 (AS12) Texas Education Code replaced by new Annex 12 – Cybersecurity Response. Table of Contents updated. Function Emergency Management Exercise (EM-X	

		24) conducted at TAMU RELLIS Campus on 7/26/24.	

END OF BLINN COLLEGE DISTRICT EMERGENCY RESPONSE PLAN

PAGE INTENTIONALLY LEFT BLANK