Texas Department of Information Resources

Transforming How Texas Government Serves Texans

Texas Framework for Mutual Aid Agreements for Security Incidents

Office of the Chief Information Security Officer

December 2021

Table of Contents

I. Introduction

Texas Government Code Section **2054.0594** requires the Texas Department of Information Resources (DIR) to provide a framework for regional cybersecurity working groups to execute mutual aid agreements. This framework includes the elements of a mutual aid agreement that should be considered, a template mutual aid agreement, and a template non-disclosure agreement. With the framework, state agencies, local governments, regional planning commissions, public and private institutions of higher education, the private sector, and the Texas volunteer incident response team can assist with responding to a security incident in the state. This is a template and should be modified to meet the needs of the participants.

This guideline does not provide legal authority or direction and does not supersede applicable legal authorities and constraints at any jurisdictional level. Entities should consult with applicable legal authorities before entering into a mutual aid agreement or compact. By identifying potential shortfalls and capability gaps through planning and exercises, jurisdictions can work with partners to establish mutual aid agreements as part of their preparedness actions.

II. Key Elements of Mutual Aid Agreements for Security Incidents

Mutual aid agreements can vary considerably based on the needs and resources of the participating parties. When establishing mutual aid agreements, the parties should consider including the following key elements to improve the understanding of the commitment, scope, and general procedures for all parties.

Purpose and Scope

Identify the agreement's conditions, length, and general scope or effect. Present the reason for the agreement and identify the parties, the types of services addressed, and any applicable mutual aid service limitations. Organizations often specify whether the agreement's intent is to provide resources for declared disasters or surge capacity prior to a disaster declaration. Specify if the agreement is limited to incident response or if it also includes recovery efforts. If recovery efforts are included, consider specifying how a duration for the recovery assistance will be determined.

Authorities

Specifically state the legal basis for the parties to enter into the mutual aid agreement in an authority's section. This may include Texas Government Code **2054.0594** and other state laws, local ordinances, tribal resolutions, regulations, or other applicable authorities.

Non-Disclosure and Confidentiality

Identify any requirements for participants to sign a Non-Disclosure Agreement (NDA). Outline the factors for identifying confidential information, and any protections from disclosure under state laws or local ordinances.

Definitions

Define key terms in the agreement to ensure all parties share a common vocabulary, especially any terms that are specific or unique to the circumstances of the contract. Consider including definitions for security incident, incident response plan, and confidential information.

Incident Response Plan

Specify requirements for participants to adopt and maintain an incident response plan. Consider adopting the DIR Incident Response Team Redbook to have a consistent format across participants.

Participant Inventory and Priority List

Specify requirements for participants to maintain an inventory of systems, network diagrams, and a priority level for recovery in the event of an incident. Consider using the Hardware and Software Inventory Form and Services Restoration Priority Worksheet included in the DIR Incident Response Team Redbook.

Resources

Specify the types of assistance included in the agreement. Types of assistance may include services, personnel (employees, contractors, and/or vendors), equipment, supplies, and facilities.

Contact DIR at DIRSecurity@dir.texas.gov to learn what planning and response resources may be available, including the Computer Incident Response Team (CIRT), Regional Network Security Operations Centers, the Texas Volunteer Incident Response Team (VIRT), and Managed Security Services (MSS).

Consider establishing a regional working group to develop a list of available security experts and resources to assist in responding to the security incident and recovery from the incident.

Recognition of Licensure and Certifications

Identify if incident responders will be required to pass a Criminal Justice Information Services (CJIS) background check. Consider whether certain security incidents may require individuals to have a secret security clearance. Outline how individuals will provide proof of required certifications.

Host Organization

Consider identifying a host organization responsible for maintaining a current list of participating entities' contact information and sharing that list with a requesting organization in the event of an incident.

Procedures to Request Assistance

Explain the procedures to request assistance, including who can initiate a request and how it is submitted.

Protocols for Interoperable Communications

Pre-arranged communication frequencies and procedures are critical for effective execution. Identify the overarching requirement for ensuring the necessary level of voice and data communications.

These protocols may include guidance on interoperability channels, data services, backup systems, and common alerting protocols that are necessary to establish on-the-scene coordination and communications for multijurisdictional or multidisciplinary responses. Identifying common communication protocols in mutual aid agreements is particularly important when integrating mutual aid resources that may not have interoperable systems.

Reciprocity/Reimbursement

Mutual aid agreements should specify how the requesting entity will compensate the responding entity. Compensation options include:
• ***In-kind agreements*** state that the party receiving services will reciprocate by providing the same type of services over time.
• ***Equity agreements*** state that the parties will exchange equitable services, though not of an in-kind nature. The value of the services exchanged under an equity agreement is equal.
• ***Reimbursable agreements*** provide the terms of the exchange of services for payment. Contracts specify the costs of various types of services and the payment mechanisms parties will use. In some incidents, responding parties cannot afford to lend their services and resources for extended periods of time without reimbursement.

Mutual aid agreements that involve direct payment often include the following provisions:

- Conditions that would trigger the start of reimbursable time for resources provided through mutual aid.
- Eligibility and documentation requirements for expenses that are reimbursable (e.g., a travel reimbursement policy).
- Jurisdictional or organizational policies related to specific reimbursable costs. Examples of such costs may include personnel compensation and travel.
- Equipment Rates: reimbursement costs for equipment utilization.
- Commodities: expendable and durable commodities that often include office supplies.
- Other: these are costs that do not fall into one of the above categories.

Operational Plan and Procedures Requirements

Specify any requirements concerning the development of a mutual aid operational plan, including procedures, the timeline for completion, and the process for approving and implementing the plan. Typically, this includes procedures for how mutual aid resources and personnel who were mobilized to support an incident continue under the operational control of their day-to-day leaders. It often also includes details on how the requesting entity's existing Incident Command System structure integrates resources and personnel. Additionally, it may specify how the requesting entity maintains control over the incident, makes organizational and strategic goals and objectives, and assigns tasks to the mutual aid resources through the chain of command.

Supplemental Information Based on Declaration Status

Include supplemental information on authorities and procedures that are triggered under governor-declared disasters, such as provisions to:

- Implement intergovernmental agreements, memoranda of agreement/understanding, intrastate legislation, or gubernatorial executive orders to deploy tribal personnel, private resources, and volunteers;
- Incorporate resources that provide form and structure to interstate mutual aid during governor-declared states of emergency; and/or
- Request and receive assistance from other member states quickly and efficiently.

III. Key Elements of Mutual Aid Operational Plans

Mutual aid operational plans support mutual aid agreements and guide the responding and requesting parties in managing and providing effective mutual aid. Though not required, these plans are essential to identify specific resources, tasks, personnel, asset allocations, roles, responsibilities, integration, and actions that mutual aid participants execute respective to their assignments. Regional councils in Texas should establish working groups to facilitate the creation of mutual aid agreements between entities in their region for security incident support when the need arises.

Mutual aid operational plans:
• Supplement mutual aid agreements, either as an appendix to the agreement or as a separate document;
• Identify specific resources, tasks, personnel, asset allocations, roles, responsibilities, integration, and actions that mutual aid participants execute respective to their assignments; and
• Help requesting or requesting parties manage mutual aid assets during or following an incident.

The following subsections present key characteristics and components of effective mutual aid operational plans.

Implementation, Schedule, Training, and Exercises

The mutual aid operational plan should include a schedule of training and exercises to validate its concepts and actions. Mutual aid-based exercises provide responders the opportunity to practice their procedures and responsibilities. Exercises test operational plan design, concept, and implementation, in addition to testing the communications, logistics, and administrative structure needed to support the plan.

Sound operational plans, coupled with training and opportunities to exercise plan components, help build a solid foundation for implementing mutual aid. Listing scheduled training or exercises, as well as learning objectives for each, in an operational plan is a best practice. In addition, the operational plan should list any requirement for minimum training standards between the parties.
This section should include an implementation schedule for individual and joint training and validation exercises.

Organizing Mutual Aid Resources

Entities use various mechanisms to organize, develop, train, and exercise certain response and recovery resources prior to an emergency or disaster. These mechanisms are developed by mutual aid system managers ahead of time for anticipated mission requirements, as well as on an ad hoc basis. Managers assemble existing teams and organize them based on a mission's specific requirements.

Inventorying Resources

A variety of sources can provide resource requirements, depending on the nature of the emergency and the public and private sector entities operating in the affected areas. Appropriate planning requires that jurisdictions communicate potential resource needs in advance of any incident to prospective resource providers. To assist in this process, maintaining an inventory of resources "owned" by parties in the agreement is a best practice. This inventory should include specifics on capabilities, maintenance requirements, operational status, and deployment information. Include procedures to identify the immediate and future resource needs and priorities of the incident, including what and how much is needed, where and when it is needed, and who will be receiving or using it, based on incident response experience and specific damage assessments.

Specific details may include the following:

- ***Name***: The unique name of the resource.
- ***Resource Typing Definition or Job Title***: The resource typing definition or job title that applies to the resource. This can be job title/position qualification or a local, state, or tribal definition.
- ***Status***: The status of the resource (available, assigned, or out of service).
- ***Mutual Aid Readiness***: Whether the resource is ready for deployment under mutual aid.
- ***Point of Contact***: Individuals and relevant information for those who are points of contact for communication related to the resource and their relevant information.
- ***Owner***: The agency, tribe, company, person, or other entity that owns the resource.
- ***Manufacturer/Model***: The manufacturer, model name, and serial number for equipment.
- ***Contracts***: Purchase, lease, rental, or maintenance agreements or other financial agreements associated with the resource.
- ***Certifications***: Documentation that validates the official qualifications, certifications, or licenses associated with the resource.
- ***Deployment Information***: The information needed to request a resource, which includes:
    - Minimum Lead Time (in hours): The minimum time a resource needs to prepare for deployment.
    - Maximum Deployment Time (in days): The maximum time a resource can be deployed or involved in a response before its owner needs to pull it back for maintenance, recovery, or resupply.
    - Restrictions: Any restrictions placed on the resource use, capabilities, etc.
    - Reimbursement Process: Any special information regarding the reimbursement process.
    - Release and Return Instructions: Any information regarding the release and return of the resource.
    - Sustainability Needs: Any information regarding resources or criteria for maintaining a capability during a deployment.

Management and Coordination

Provide a protocol for integrating mutual aid resources into the management and coordination structure. This protocol should include specifics on who assumes operational control of mutual aid resources and how the responding entity integrates mutual aid resources into the requesting entity's command and control structure.

Health and Safety

The dangers and environmental hazards that responders may encounter during the incident dictate protocols for health and safety. Provide or reference the types and levels of personal protective equipment, respiratory equipment, or other protection, as well as associated training on that equipment, which are necessary to ensure responder and patient health and safety.

Documentation and Reporting

Include standardized protocols for documenting and reporting procedures to help parties maintain situational awareness and give personnel access to critical information.

Demobilizing Resources

A best practice is to include demobilization guidance in mutual aid operational plans to detail the process for demobilizing resources.

Definitions

Agency: A government element with a specific function offering a particular kind of assistance.
Compact: A contract between parties, which creates obligations and rights capable of being enforced, and contemplated as such between the parties, in their distinct and independent characters.
Confidential Information: Information that must be protected from unauthorized disclosure or public release based on state or federal law or other legal agreement.
Demobilization: The orderly, safe, and efficient return of an incident resource to its original location and status.
Emergency: Any incident, whether natural, technological, or human-caused, that necessitates responsive action to protect life or property.
Entity: A state agency, local government, regional planning commission, public and private institution of higher education, the private sector, and the Texas Volunteer Incident Response Team. When entities enter into a mutual aid agreement, they become parties to the agreement.
Incident Response Plan: The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyber attack against an organization's information system(s).
Interoperability: The ability of systems, personnel, and equipment to provide and receive functionality, data, information, and/or services to and from other systems, personnel, and equipment, between both public and private agencies, departments, and other organizations, in a manner enabling them to operate effectively together. Interoperability allows emergency management/response personnel and their affiliated organizations to communicate within and across agencies and jurisdictions via voice, data, or video-on-demand in real time, when needed, and when authorized.
Mutual Aid: The timely and efficient sharing of capabilities in the form of resources and services upon request.
Mutual Aid Agreement: A written or oral agreement between and among agencies/organizations and/or jurisdictions that provides a mechanism to quickly obtain assistance in the form of personnel, equipment, materials, and other associated services. The primary objective is to facilitate the rapid, short-term deployment of emergency support prior to, during, and/or after an incident.
Party: A person or entity involved in an agreement.
Protocol: A set of established guidelines for actions (designated by individuals, teams, functions, or capabilities) under various specified conditions.
Reimbursement: A mechanism to recoup funds expended for incident-specific activities.
Requesting Entity: The party in the mutual aid agreement that receives resources.
Resource Typing: Defining and categorizing incident resources by capability.
Resources: Personnel, equipment, teams, supplies, and facilities available or potentially available for assignment to incident operations and for which status is maintained. Resources are described by kind and type and may be used in operational support or supervisory capacities at an incident or at an emergency operations center.
Responding Entity: The party in the mutual aid agreement that provides resources.
Security Incident: An event which results in the accidental or deliberate unauthorized access, loss, disclosure, modification, disruption, or destruction of information or information resources.
Type: A resource classification that refers to capability of a specific kind of resource that applies a metric to designate it as a specific numbered class.

Resources

DIR Incident Response Team Redbook

The Texas DIR Incident Response Team Redbook provides policy guidance and includes helpful templates for creating incident response capability.

Template Mutual Aid Agreement

MUTUAL AID AGREEMENT (MAA) FOR SECURITY INCIDENTS

This Mutual Aid Agreement ("MAA") is by, between, and among _____ (the "Host Entity") and the undersigned Participating Entities of the State of Texas (each a "Participating Entity"), acting by and through their respective authorized representatives (referred to individually as a "Party" and collectively as the "Parties").

RECITALS:

WHEREAS, this Agreement is authorized by Texas Government Code Section 2054.0594 and Chapter 791; and

WHEREAS, each Participating Entity may experience a cyber incident, natural disaster, or other emergency capable of degrading or disrupting information technology services ("Security Incident") beyond the capabilities of the Participating Entity; and

WHEREAS, each Participating Entity acknowledges the importance of prompt restoration of IT Services to allow local governments to function and operate; and

WHEREAS, each Participating Entity has agreed to adopt a formal or informal cyber response plan in the event of a significant cyber incident; and

WHEREAS, each Participating Entity has agreed to adopt a formal or informal response plan in the event of a natural disaster or other emergency; and

WHEREAS, a Participating Entity requesting IT Services (hereinafter referred to as a "Requesting Entity") receives benefit from a responding Participating Entity (hereinafter referred to as a "Responding Entity") through the provision of supplemental IT Services personnel or computer hardware for the period of support; and

WHEREAS, the Responding Entity receives the benefit of its IT Services personnel gaining knowledge through the experience of aiding in the restoration of IT Services during a crisis; and

WHEREAS, the Parties desire to enter a MAA to offer time and expertise of IT Services personnel to assist in the detection, response, and short-term remediation of the cyber incident or assist in the repair and restoration of IT Services due to a natural disaster or other emergency.

NOW THEREFORE, in exchange for the mutual covenants set forth herein and other valuable consideration, the sufficiency and receipt of which are hereby acknowledged, the Parties agree as follows:

ARTICLE I
DEFINITIONS

Unless the context clearly indicates otherwise, the following words and phrases used in this Agreement shall have the following meaning:

"Host Entity" shall mean the Participating Entity that is responsible for maintaining a current list of participating entities and contact information and sharing with a requesting organization in the event of an incident.

"Security Incident" shall mean an event which results in the accidental or deliberate unauthorized access, loss, disclosure, modification, disruption, or destruction of information or information resources.

"Mutual Aid" shall mean, but is not limited to, such IT Service resources as facilities, equipment, services, supplies, and personnel.

"Participating Entity" shall mean a participating state agency, local government, regional planning commission, public and private institution of higher education, private sector, or the Texas Volunteer Incident Response Team that executes this Agreement and includes the "Host Entity". All private sector entities will serve as "Responding Entities" only.

"Requesting Entity" shall mean the Participating Entity that requests Mutual Aid under this Agreement as result of a Security Incident under the terms of this Agreement.

"Responding Entity" shall mean the Participating Entity providing Mutual Aid to a Requesting Entity in response to a Security Incident.

ARTICLE II
PURPOSE

The purpose of this Agreement is to establish a MAA between and among the Parties, which will allow each Participating Entity to provide Mutual Aid to a Requesting Entity as a result of, in response to, or during a Security Incident.

ARTICLE III
TERM; TERMINATION

3.1 The term of this MAA shall be for a period of one (1) year commencing on the last date of execution by the Participating Entity ("Effective Date"). Thereafter, this MAA shall automatically renew for successive periods of one (1) year each under the terms and conditions stated herein, not to exceed four (4) additional one (1) year terms, unless sooner terminated as provided herein.

3.2 A Participating Entity may terminate its participation in this MAA by providing thirty (30) days prior written notice to terminate its participation in this MAA to the Host Entity. The Host Entity shall provide written notice of any such termination to the designated representative of each Participating Entity.

3.3 A Participating Entity's participation in this MAA may be terminated by the Host Entity for cause, including, but not limited to, failure to comply with the terms or conditions of this Agreement upon thirty (30) days prior written notice to such Participating Entity.

3.4 Termination by one or more Parties to this Agreement does not affect the Agreement as it applies to the remaining Parties.

ARTICLE IV
RESPONSIBILITY OF PARTIES

4.1 Requesting Assistance. The Chief Information Officer ("CIO"), Information Technology Director ("IT Director"), or designee of the Participating Entity that has experienced a Security Incident may request Mutual Aid from the CIO, IT Director, or designee of another Participating Entity verbally or in writing. The determination as to what Mutual Aid may be made available to the Requesting Entity without unduly interfering with the IT Services of the Responding Entity shall be made at the sole discretion of the head of the Responding Entity, or designee. Each Participating Entity agrees to assess available resources to determine availability of Mutual Aid based on current or anticipated needs of the Responding Entity. Requests for Mutual Aid shall not be requested by a Party unless it is directly related to the Security Incident and resources available from the Requesting Party are inadequate.

4.2 Provision of Aid At Entity's Discretion. Each Participating Entity recognizes that it may be requested to provide aid and assistance at a time when it is necessary to provide aid and assistance to the Participating Entity's own constituents. This MAA shall not be construed to impose any obligation on any Participating Entity to provide Mutual Aid to Requesting Entity. Each Participating Entity may choose not to render Mutual Aid at any time for any reason, or to recall such Mutual Aid that has been provided at any time.

4.3 Procurement of Equipment, Software and Services. The Requesting Entity shall be responsible for any incidental costs, equipment, software, or services related to the Mutual Aid response to the Security Incident. If the Responding Entity indicates a need for the acquisition or purchase of equipment, software, or services, the Requesting Entity shall decide if such acquisition or purchase is necessary and will make any required acquisition or purchase subject to all limitations and requirements under law, including laws governing appropriations or the availability of funds.

4.4 Use of Computer Hardware. A Requesting Entity in need of computer hardware (e.g. personal computers, laptops, servers, network equipment, etc.), will compile a written list of such computer hardware and the estimated length of time that such equipment is needed which may be sent to the Participating Entities. Any Participating Entity may choose to respond in whole or in part and is under no obligation to provide computer hardware to the Requesting Entity. A Responding Entity which chooses to loan computer hardware will respond back to the Requesting Entity to affirm that such computer hardware or portion thereof is available for temporary use. The Responding Entity makes no claim of the currency or operational use of the computer hardware nor is the Responding Entity liable for any damages resulting from the Requesting Entity's use of any computer hardware so provided. The transportation and delivery of such computer hardware or charges related thereto shall be the responsibility of the Requesting Entity unless otherwise agreed by those Parties. The Requesting Entity shall be responsible for, and pay the Responding Entity for any damages, loss, or destruction of such computer hardware while in the use and possession of the Requesting Entity, including the transport thereof, to the greatest extent permitted by law. Any ongoing

maintenance, lease or other fees related to such computer hardware shall continue to be paid by the Responding Entity.

4.5 Criminal Justice Information System ("CJIS"). The Requesting Entity shall be responsible for restricting the Responding Entity personnel from access to CJIS information unless the Responding Entity personnel have completed all CJIS background checks and is in current compliance with CJIS training requirements.

4.6 List of Participating Entities. The Host Entity shall maintain a current list of Participating Entities and provide such list to a Participating Entity upon request

ARTICLE V
INSURANCE

5.1 Worker's Compensation Coverage. To the extent permitted by Texas law, each Party shall be responsible for its own actions and those of its employees and is responsible for complying with the Texas Worker's Compensation Act.

5.2 Automobile Liability Coverage. To the extent permitted or required by Texas law, each Party shall be responsible for its own actions and is responsible for complying with the Texas motor vehicle financial responsibility laws.

5.3 General Liability Insurance. Each Party agrees to obtain general liability and public official's liability insurance, if applicable, or maintain a comparable self-insurance program.

ARTICLE VI
MISCELLANEOUS

6.1 Expending Funds. Each Party that furnishes Mutual Aid pursuant to this MAA shall do so with funds available from current revenues of such Party. No Party shall have any liability for the failure to expend funds to provide Mutual Aid.

6.2 Severability. If a provision contained in this Agreement is held invalid for any reason, the invalidity does not affect other provisions of the Agreement that can be given effect without the invalid provision, and to this end, the provisions of this Agreement are severable.

6.3 Legal Construction. In the event any one or more of the provisions contained in this Agreement shall for any reason be held to be invalid, illegal, or unenforceable in any respect, such invalidity, illegality, or unenforceability shall not affect other provisions, and it is the intention of the Parties to this Agreement that in lieu of each provision that is found to be illegal, invalid, or unenforceable, a provision shall be added to this Agreement which is legal, valid and enforceable and is as similar in terms as possible to the provision found to be illegal, invalid or unenforceable.

6.4 Amendment. This Agreement may be amended only by the mutual written consent of the Parties.

6.5 Third Parties. This Agreement is intended to inure only to the benefit of the Parties hereto. This Agreement is not intended to create, nor shall be deemed or construed to create any rights, to third parties.

6.6 Authorization. Each Party represents that it has full capacity and authority to grant all rights and assume all obligations that are granted and assumed under this Agreement. By execution of this Agreement the Participating Entity consents to be a Party to this Agreement and acknowledges that it is not necessary to receive copies of the Agreement from other local governments that are, or which become, Parties to this Agreement. Each Party is solely responsible for its actions and those of its agents, employees, or subcontractors, and agrees that neither Party nor any of the foregoing has any authority to act or speak on behalf of DIR or the State.

6.7 Entire Agreement. This Agreement is the entire agreement between and among the Parties with respect to the subject matter covered in this Agreement. There is no other collateral oral or written Agreement between and among the Parties that in any manner relates to the subject matter of this Agreement.

6.8 Governing Law. This Agreement shall be governed by the laws of the State of Texas.

6.9 Recitals. The recitals to this Agreement are incorporated herein.

6.10 Counterparts. This Agreement may be executed in counterparts. Each of the counterparts shall be deemed an original instrument, but all the counterparts shall constitute one and the same instrument.

6.11 Survival of Covenants. Any of the representations, warranties, covenants, and obligations of the Parties, as well as any rights and benefits of the Parties, pertaining to a period following the termination of this Agreement shall survive termination.

6.12 Notice. All notices pertaining to this Agreement shall be in writing and shall be deemed delivered (i) when received at a Party's address if hand delivered or sent via overnight delivery service by way of USPS, UPS, FedEx, or similar carrier, or (ii) on the third (3rd) business day after being deposited in the United States mail, postage prepaid, certified mail, addressed to Participating Entity at the address set forth below the signature of the Party

6.13 Severability. In the event any one or more of the provisions contained in this Agreement shall for any reason be held to be invalid, illegal, or unenforceable in any respect, such invalidity, illegality, or unenforceability shall not affect the other provisions, and the Agreement shall be construed as if such invalid, illegal, or unenforceable provision had never been contained in this Agreement.

6.14 Nondiscrimination. In their execution of this agreement, the Parties and others acting by or through them shall comply with all federal and state laws prohibiting discrimination, harassment, and sexual misconduct. Any breach of this covenant may result in termination of this agreement.

6.15 Cybersecurity Training Program. Pursuant to Section 2054.5192, all parties to this agreement will ensure all employees designated to respond to a requesting agency are in compliance with all current

State of Texas law(s) regarding required cyber security training. The cybersecurity training program must be completed during the term and any renewal period of this Agreement. Failure to comply with the requirements of this section are grounds for termination of this Agreement.

6.16 Sovereign Immunity. Notwithstanding any provision of this Agreement, nothing herein shall be construed as a waiver by any Party of its constitutional, statutory, or common law rights, privileges, immunities, or defenses. To the extent the terms of this paragraph conflicts with any other provision in this Agreement, the terms of this paragraph shall control.

[Signature Pages to Follow]

EXECUTED this _____ day of _____ 2021.

_____,
Host Entity

By:

ATTEST:

By:

APPROVED AS TO FORM:

By:

EXECUTED this _____ day of _____, 2021.

PARTICIPATING ENTITY:

_____

By:
Name:
Title:

Address:

ATTEST:

By:

APPROVED AS TO FORM:

By:

Template Non-Disclosure Agreement

Non-Disclosure Agreement

Mutual Aid Agreement (MAA)

The MAA is established in accordance with TGC Section **2054.0594 to allow state agencies, local governments, regional planning commissions, public and private institutions of higher education, the private sector, and the incident response team** to assist with responding to the cybersecurity event of a state agency, including an institution of higher education, or a local government (hereafter referred to as "participating entity").

I,_____, the undersigned hereby certify that I understand and agree to be bound by the commitments with regard to participating as a MAA Participant to provide response assistance as detailed herein.

I understand there may be eligibility criteria for my participation as a MAA Participant, including but not limited to a requirement that I have expertise in addressing cybersecurity events.

I agree that as a MAA Participant I will be required to:

(1) acknowledge the confidentiality of information required by Section 2054.52010, as applicable;

(2) protect all confidential information from a conflict of interest as a Participant under this agreement;

(3) comply with all applicable security policies and procedures regarding information resources technologies;

(4) consent to any required background screening; and

(5) attest to my satisfaction of any eligibility criteria.

Confidential Information is information written, produced, collected, assembled, or maintained by a MAA Participant if the information:

(1) identifies or provides a means of identifying a person who may, as a result of disclosure of the information, become a victim of a cybersecurity event;

(2) consists of a Participant's cybersecurity plans or cybersecurity-related practices; or

(3) is obtained from a Participant or from a Participant's computer system in the course of providing assistance under this agreement.

I agree to perform any and all duties in an unbiased manner, to the best of my ability, and with the best interest of the State of Texas paramount in all decisions.

I acknowledge as a MAA Participant, I am not an agent, employee, or independent contractor of this state for any purpose and have no authority to obligate this state to a third party. The state is not liable to a MAA Participant for personal injury or property damage sustained by the volunteer that arises from participation in the incident response team.

I will immediately inform both my management and the Host Entity if, at any time during the MAA participation, any of these statements are no longer true and correct.

I have been given the opportunity to review this statement prior to signing. If I have questions or concerns about this statement, I am to contact my management or the Host Entity.

_____(Signature) _____(Date)

_____ (Printed name)