

Texas State University Business Continuity Policy

1.0: Policy Statement

It will be the policy of the Texas State University to develop a business continuity plan to cover the administrative and financial operations of the university and each of its departments after a business interruption caused by an unplanned emergency or disaster. We recognize that the prevention of an emergency event or a disaster is impossible and we are not attempting to address those issues. We are making the assumption that an unplanned event and/or disaster will occur at some point in time and it is necessary to take the appropriate steps to minimize the effects of that event and to allow the University to resume its business and service activities in quick and timely manner.

2.0: Texas State University System Policy Statement

The Texas State University System has adopted the following Business Continuity Plan policy for all components of the System:

2.1 Policy:

It will be the policy of the Texas State University System (TSUS) and Component Institutions and this policy shall be in affect to cover the Financial Operations of the System, and each component, during a period of disaster. We recognize that the prevention of a disaster is impossible and we are not attempting to address those issues. We are making the assumption that a disaster will occur sometime and the steps we are taking in this policy are being taken to minimize the effects of that event.

2.2 Scope:

This policy addresses the financial, investment, tax, payroll, accounts payable and financial reporting of the Texas State University System and Component Institutions. Our objective is to have made sufficient preparations and cross training, which will allow us to relocate finance operations to another site if necessary. Reestablish the computer system, restock necessary supplies, and have adequately trained personnel on hand to continue the finance operations.

2.3 Prioritization:

We feel that it is important to define the priorities of the various areas of responsibility of the finance operations. At certain times, these priorities might change because of workloads or at certain times of the year. For example: if a disaster occurs in October, provisions would be needed to handle the preparation of the annual financial report (AFR). During June and July, the preparation of budgets and legislative appropriations (LAR) must continue. If a disaster should occur at the end of the month for payroll, provisions would be needed to handle the payroll process. Accounting records must be available to account for funds available to address the disaster and to give updated expenditure estimates as needed. Proper accounting of disaster expenditures must be maintained to meet requirements of State Auditors, FEMA and insurance carriers.

2.4 Computer System:

The re-establishing of the computer and computer software would be the highest priority. Without the computer and accompanying software none of the following objectives could be met. Every attempt should be made to bring up the web site and post information as soon as possible.

Payroll - our next priority is to our employees and their families. Without them, completing the various missions and goals of the Texas State University System and Component Institutions would not be possible. Our first priority in re-establishing the finance division operations would be the payroll function. Our employees will need to be paid on a regular basis and the system for tax withholding, pension, health insurance coverage, workers' compensation need to be continued with minimal disruptions. Records allowing transfer of funds with banking institutions are necessary to complete this assignment. This priority has to include the ability to move money to accomplish transfer due dates for payroll and other payments due. Manual checks should also be available to provide funds if needed until the regular A/P services are re-established. Internal controls and proper signature sign-offs are necessary for audit purposes. Documentation of special circumstances is imperative.

Accounting and Budget Records - the establishment of the records would be our third priority. Once the computer system is re-established and the backups installed the year to date data should be up to date. These records are needed to produce the AFR, Budgets and LAR. They are also needed to provide estimates of resources available to meet the disaster. The ability to issue purchase orders is necessary to allow contracting of services to prevent further damage and to start repairs of the facilities.

2.5 Disaster Vulnerability:

The types of disasters which the TSUS office and the component institutions are vulnerable to vary due to the widespread nature of the campuses.

The events which could be rated as to probability are as follows:

	TSUS Office	TS at San Marcos	Sam Houston	Angelo State Univ	Lamar, LSC-PA LIT & LSCO	Sul Ross State Univ
Fire	Med	Med	Med	Med	Med	Med
Tornado/ Thunderstorms	High	High	High	High	High	High
Flood	Low	High	Low	Low	High	Low
Hurricane/Related Evacuation activity	Low	Low	Med	Low	High	Low
Terrorist/Chemical Spill/Leak	Med	Med	Med	Med	High	Med

The above list is not exclusive. It serves only as a brief summary of the components of the TSUS system. Each component needs to attach a listing of potential risks in their individual plans.

2.6 Alternate Location:

For events of a short duration, a couple of days or less, the offices would close and re-open as soon as practical. For events of a longer duration, alternate sites would be established to be used on a temporary basis as needed.

If alternate sites are available within the component, then each component would address those needs. A meeting of the CFO's would occur to determine alternative sites if an entire component is affected and it is deemed necessary to establish alternative offices and system office personnel. Items which need to be addressed are: 1) prioritize work and due dates, 2) assignments based on priorities and 3) possible relocations of campus finance/administrative offices.

2.7 Computer Backup Operations:

Routine tape backups are necessary to the file servers in the event of accidental deletion or catastrophic loss. Components are responsible to provide and maintain an off-site location to house back-up financial data and to host web sites.

2.8 Mobile Finance Operations (MFO):

Each component should develop and supply an MFO. It should contain adequate supplies of blank check stock, deposit forms and emergency purchase orders. Supplies of time sheets to record time, equipment and personnel are needed to begin immediately after a disaster for both FEMA and insurance purposes

2.9 Personnel

In order to minimize the effects due to the loss of office staff, each component should actively engage in a program of cross training. This cross training is not designed to make experts out of each employee, but it is intended to familiarize each employee with the general operations of the other positions.

2.10 Disaster Preparedness Testing

Each component is responsible to ensure that proper testing of the plans is performed on an annual basis. This testing should be properly documented and modifications, if necessary, be made to the component plans. This policy shall be subject to review and update on an annual basis in May of each year.

3.0 SCOPE:

This policy's initial focus will be on administrative and financial operations and the facilities that support those operations. Examples include payroll, accounting, financial reporting, auxiliary services, financial aid, student services, academic services, and facilities support and appropriate business functions at Texas State University. Our objective is to have made sufficient preparations and cross training, which will allow us to resume our business functions and to have a plan to relocate our operations to another site if necessary. In addition it may be necessary to reestablish the computer system, restock necessary supplies, and have adequately trained personnel on hand to continue the administrative, finance and business operations. Each of the technology departments in Information Technology (IT) currently has developed a disaster recovery plan in accordance with the Texas Department of Information Resources and conducts annual reviews and updates and upon completion of the latest version of the plan will be linked to the Business Continuity Plan on the Texas State website.

4.0 PROCEDURES FOR DEVELOPING A BUSINESS CONTINUITY PLAN

The process for developing a business continuity plan includes gathering data components which include the following:

- Identify potential business interruptions and/or disasters
- Conducting a Department risk assessment (RA)
- Completing and Business Impact Analysis (BIA)
- Identify Department functions
- Identify Critical Processes and Services
- Identify Priority of Essential Functions
- Identify Critical Data Needs
- Protection of Critical Data
- Identify an alternate work or set up location

5.0: Types of Business Interruptions

The types of business interruptions and disasters which Texas State is vulnerable to include the following:

Environmental Disasters

- Tornado
- Flood
- Ice Storm and freezing conditions
- Electrical storms
- Fire
- Contamination and Environmental Hazards
- Epidemic

Organized and/or Deliberate Disruption

- Act of terrorism
- Act of Sabotage
- Act of war
- Theft
- Arson

Loss of Utilities and Services

- Electrical power failure
- Loss of gas supply
- Loss of water supply
- Petroleum and oil shortage
- Communications services breakdown
- Loss of drainage / waste removal

Equipment or System Failure

- Internal power failure
- Air conditioning failure
- Production line failure
- Cooling plant failure
- Equipment failure (excluding IT hardware)

Serious Information Security Incidents

- Cyber crime
- Loss of records or data
- Disclosure of sensitive information
- IT system failure

Other Emergency Situations

- Workplace violence
- Public transportation disruption
- Neighborhood or city hazard
- Negative publicity
- Legal problems

Although not a complete list, it does give a good idea of the wide variety of potential threats.

6.0 PRIORITIZATION AND COMPONENTS:

We feel that it is important to define the priorities of the various areas of responsibility of the finance operations. **Business Continuity Planning (BCP)** is the standard method by which businesses plan for continuing operations after an emergency. BCP involves several steps, which include performing a **Business Impact Analysis (BIA)** and a **Risk Assessment (RA) (also referred to as Risk Analysis)**. It is impossible to properly plan for a disaster if the likely impacts of various disruptions on an organization are unknown.

A Business Impact Analysis is a means of systematically assessing the potential impacts of various events on operations. It allows an organization to understand the degree of loss that could occur from each potential disruption.

The first step in conducting a BIA is identifying the assets that are required to perform the organization's core mission. The second step involves identifying the potential hazards or threats to these assets. The third step requires determining the susceptibility of the organization to the effects of each hazard or threat. The fourth and final step requires determining the potential impact of each threat. Assessing the impact of an event includes not only estimating the quantitative or economic losses but also the qualitative impact on the organization's ability to operate, i.e., psychological effects on employees and effect on the reputation of the organization.

Although the BIA and RA are two separate inquiries, they are closely related and essential steps in BCP; thus, they are often performed together and the terms are used interchangeably. Often, the RA is performed together with the vulnerability assessment in a BIA.

A critical step in developing a Continuity Plan is identifying the organization's essential functions; their associated key personnel; and supporting critical systems/processes that must be sustained for at least fourteen days following a disruption. Essential functions encompass those critical areas of business that must continue even in the event of an emergency. In other words, they are those functions that must be performed to achieve the organization's mission.

Identifying essential functions requires an intimate understanding of all the organization's operations. Although many functions are important, not every activity the organization performs is an *essential* function that must be sustained in an emergency for fourteen days. Thus, the key to identifying essential functions is the organization's mission.

There is no one way to identify essential functions. However, the asset identification BIA offers one approach, which focuses on the organization's functions and their criticality. This can be modified for the University context into a four-step approach.

- 1) Identify all functions;
- 2) Identify essential functions;
- 3) Prioritize those functions; and
- 4) Determine essential function resource requirements.

1. Task A: Identify All Organization Functions

Use Worksheet 1, Organization Functions, to complete this task.

The mission statement clearly outlines the basic purpose of the organization and is the first place to look to determine essential functions. Existing Sop's and reports on operations usually offer a good starting point for identifying various functions.

Once all the functions are identified for Business Continuity planning purposes, narrow the list to only the essential functions. This can be accomplished by referring back to the organization's mission and considering the beneficiaries of the function. For example, if other organizations or individuals are dependent on a particular function to continue their operations, then the function is probably an essential function.

2. Task B: Identify Critical Processes and Services

Use Worksheet 2, Resource Requirements for Critical Processes and Services Supporting Essential Functions, in conjunction with Worksheet 1, Organization Functions, to complete this task. After the essential functions are determined, examine the processes and services that support them. Essential functions and their supporting processes and services are intricately connected. Each essential function has unique characteristics and resource requirements, without which the function could not be sustained. Those processes and services described for each function that are necessary to assure continuance of an essential function are considered critical. Often, critical processes and services vary depending upon the emergency or if they have a time or calendar component.

3. Task C: Identify Priority of Essential Functions

Use Worksheet 3, Priority of Essential Functions, to complete this task. Once all essential functions and their supporting critical processes and services have been identified, prioritize the functions according to those activities that are pivotal to resuming operations when a catastrophic event occurs. Prioritization requires determination of the following:

- Time criticality of each essential function; and
- Sequence for recovery of essential functions and their critical processes.

An essential function's time criticality is related to the amount of time that function can be suspended before it adversely affects the organization's core mission. Time criticality can be measured by either recovery time or recovery point objectives. These are terms of art borrowed from Information Technology (IT) disaster recovery planning, but can be used in the broader context of Business Continuity planning. **A recovery time objective (RTO)** is the period of time within which systems, processes, services, or functions must be recovered after an outage. **A recovery point objective (RPO)** is more specific to information systems. It is the amount of data that can be lost measured by a time index. Thus, an RPO of one hour means that the last hour of data before the failure will not be recovered. Not all processes have RPO's, and some processes can have both a RPO and a RTO. During Business Continuity planning, organizations will primarily be focusing on RTO, but it is important to understand RPO and incorporate RPO information into the COOP where necessary.

Recovery Time Objective: The amount of time that is allowable before the system comes back on line.

Recovery Point Objective: The amount of data that can be lost measured by a time index.

Deciding which essential function should be restored first in a crisis would be impossible without also considering its related critical processes and services. Critical processes or services are those that must be resumed soon after a disruption, generally within 24 hours. By contrast, secondary processes or services do not need to be resumed as quickly after a disruption.

4. Task D: Identify Critical Data Needs

Use Worksheet 4, Critical data needs. The protection of vital records, systems, and equipment, including the ability to access and use such records are a central part of planning. Examples of vital records include emergency plans and documents, staffing assignments, and selected program records needed to continue critical operations. In addition, legal and financial records, as well as contractual obligations are vital records that may be maintained. Vital records and systems include any IT applications or systems that are necessary for the Department to perform its minimum essential functions.

5. Task E: Protection of critical data

Use Worksheet 5, Vital Records Protection Methods. The next step after identification of vital records is determination and selection of protection methods. This necessitates first looking at the current methods of protection and preservation. The routine maintenance program for the records in question may be sufficient for the protection of information in the event of a disruption to critical processes and services. However, the effectiveness of the protection method should always be evaluated in light of continuity concerns. Your team should look at the current backup and retention schedules for each vital record and ask if the files should be backed up more often or retained for greater periods. Another measure to consider is the replication of data or of a server in an alternate facility or scanning paper records. The team should also consider storing duplicate files off-site, if they are not currently so stored.

7.0 ALTERNATE LOCATIONS:

For events of a short duration, a couple of days or less, the offices would close and re-open as soon as practical. For events of a longer duration, alternate sites would be established to be used on a temporary basis as needed.

If alternate sites are available within the component, then each component would address those needs. A meeting of the President's Cabinet would occur to determine alternative sites if an entire component is affected and it is deemed necessary to establish alternative offices and system office personnel. Items which need to be addressed are: 1) prioritize work and due dates, 2) assignments based on priorities and 3) possible relocations of campus finance/administrative offices.

8.0 Final Phase

A final phase of a continuity program is the execution of a continuity plan during an actual disruption. This phase will be considered during plan development, because all continuity plans should contain strategies for resumption and recovery of operations that include procedures for emergency response; plan activation; communication; evacuation; and data preservation, salvage, and restoration