TEXAS

The University of Texas at Austin

Emergency Operations Plan

2018

Annex IV - Business Continuity Plan

Version XII

Approvals

This supersedes and rescinds all previous versions of this document.

Approved: _____ Date: 1/24/18 cor 2/23/2018

Dr. Gregory L. Fenves, President
Office of the President
The University of Texas at Austin

Approved: Darrell Bazzell Date: 1/18/18

Darrell Bazzell, Senior Vice President and Chief Financial Officer
Financial and Administrative Services
The University of Texas at Austin

Approved: _____ Date: 1-10-2018

James H. Johnson, Interim Associate Vice President for Campus Safety & Security
Campus Safety and Security
The University of Texas at Austin

Published January 2018

Record of Changes

Description of Change	Entered By	Date Entered
Include Appendix G. Critical Functions & Essential Staff	David Cronk	January 31, 2012
Added Senior Leadership Orders of Succession	Patrick Funari	October 17, 2016
Added Alternate Locations for Senior Leadership	Patrick Funari	October 17, 2016
Formatting and organizational changes throughout; minor language changes throughout to improve clarity and readability	Robin Richards	November 29, 2017

Acknowledgment

The University of Texas at Austin Business Continuity Plan Annex has been developed from the Federal Financial Institutions Examination Council (**FFIEC**) Business Continuity Planning (**BCP**) IT Examination Handbook. Full credit is given to this authority for their detailed plan.

Contents

1. Purpose, Scope, Situation, and Assumptions

2. Concept of Operations

The Business Continuity Plan Annex provides guidance to university colleges, schools, departments, and agencies to ensure financial integrity and continuity of service to the community in the event of a natural or man-made disaster. The Business Continuity Plan (**BCP**) is an annex of the Emergency Management Plan. All emergency planning and response provisions of that document and other annex are in effect. This BCP and unit plans all address the four phases of emergency planning (mitigation, preparedness, response, and recovery) but the BCP has special emphasis on the recovery phase.

Operating disruptions can occur with or without warning, and the results may be predictable or unknown. It is important that the three missions (teaching, research, and service) of the university are sustained during any emergency. First priority is always the safety of the staff, faculty, students, and visitors. The university Emergency Management Plan addresses actions to protect life and property. This annex focuses on business operations and the sustenance of critical functions for the university. Business operations for the university must be resilient and the effects of disruptions in service must be minimized in order to maintain campus trust and confidence. Effective business continuity planning establishes the basis for the university to maintain and recover business processes when operations have been disrupted unexpectedly.

Business continuity planning is the process whereby the university and the subordinate components attempt to ensure the maintenance or recovery of operations, including services, when confronted with adverse events such as natural disasters, technological failures, human error, or terrorism.

The objectives of this BCP are to minimize financial loss to the university or components; continue to appropriately serve students, staff, faculty, and visitors; and mitigate the effects disruptions can have on the university's strategic plans, reputation, operations, and ability to remain in compliance with applicable laws and regulations. Changing business processes (internally to the university and externally to the broader community) and new threat scenarios require the university to maintain updated and viable BCPS at all times.

New business practices, changes in technology, and increased terrorism concerns, have focused even greater attention on the need for effective business continuity planning and have altered the benchmarks of an effective plan. This BCP will take into account the potential for wide-area disasters that effect an entire region and for the resulting loss or inaccessibility of staff. This BCP also considers and addresses the interdependencies of all university units as well as infrastructure. In most cases, recovery time objectives are now much shorter than they were even a few years ago, and for some unit's recovery time objectives are based on hours and even minutes.

Departments and agencies of the university should incorporate business continuity considerations into business process development to mitigate proactively the risk of service disruptions. In creating an effective BCP, university components should not assume a reduced demand for services during the disruption. In fact, demand for some services may increase.

This plan recognized that while technology was the primary basis for concern, an enterprise-wide, process-oriented approach that considers technology, business processes, testing, and communication strategies is critical to building a viable BCP.

Each college, school, department and unit of The University of Texas at Austin is required to participate in the development of a BCP to address disruptions. The unit level at which this plan will be developed will be determined by the provost, responsible dean, or vice president. This plan will include:

- Business Impact Analysis
- Risk Analysis
- Risk Assessment
- Plan Components
- Strategy
- Prevention Measure
- Mitigation Measures
- Emergency Response
- Unit Continuity and Succession of Leadership
- Emergency Communications
- Resource Management and Logistics
- Mutual Aid (Internal and External)
- Training and Awareness
- Exercise and Testing

The university will ensure coordination with the following external agencies:

- The City of Austin Office of Emergency Management
- Governor's Office Division of Emergency Management
- Department of State Health Services
- Other agencies as determined
- Coordination with Strategic Leadership Council (Information Resources) on technology migration plans in order to enhance continuity operations through the acquisition of new technology

2.1. Business Continuity Planning Process

The university BCP planning process reflects the following objectives:

- Business continuity planning is about maintaining, resuming, and recovering the business, not just the recovery of the technology.
- The planning process should be conducted on an enterprise-wide basis.
- A thorough business impact analysis and risk assessment are the foundation of an effective **BCP**.
- The effectiveness of a **BCP** can only be validated through testing or practical application.
- The **BCP** will be updated at least annually to reflect and respond to changes in the financial institution or its service provider(s).

The university will conduct business continuity planning on an enterprise-wide basis. Colleges, schools, departments, and units must consider the critical aspects of its business operations in creating a plan for how it will respond to disruptions. This plan is not limited to the restoration of information technology systems, services, or data maintained in electronic form, as such actions, by themselves, cannot always put a unit back in operation. Without a BCP that considers every critical business function, including personnel, physical workspace, and similar issues, the university may not be able to resume or maintain its teaching, research, and

community service missions at an acceptable level. The university recognizes the systemic impact that service disruptions may have on the integrity of the university.

University colleges, schools, departments, and units must update their BCPs as business processes change. For example, the university is increasingly relying on distributed network solutions to support business processes. This increased reliance can include desktop computers maintaining key applications. While distributed networking provides flexibility in allowing the university to deliver operations to where employees and customers are located, it also means that end-users should keep **BCP** personnel up-to-date on what constitutes current business processes and significant changes. Technological advancements are allowing faster and more efficient processing, thereby reducing acceptable business process recovery periods.

In response to competitive and customer demands, many units are moving toward shorter recovery periods and designing technology recovery solutions into business processes. These technological advancements increase the importance of university-wide business continuity planning. All university BCPs focus on a process-oriented approach to business continuity planning that involves:

- Business Impact Analysis (**BIA**)
- Risk Assessment
- Risk Management
- Risk Monitoring

Business continuity planning should center on all critical business functions that must to be recovered to maintain operations. The BCP must be viewed as one critical aspect of the university-wide process. The review of each critical business function should include the technology that supports it.

2.2. Business Impact Analysis

A business impact analysis (**BIA**) is the first step in developing a BCP. It should include:

- Identification of the potential impact of uncontrolled, non-specific events on the institution's business processes and its customers
- Consideration of all departments and business functions, not just data processing
- Estimation of maximum allowable downtime and acceptable levels of data, operations, and financial losses

The first step for units of the university to develop a BCP is to perform a BIA. The amount of time and resources necessary to complete the BIA will depend on the size and complexity of the unit. At the university, all business functions and units must be included in the planning process, not just data processing.

The **BIA** phase identifies the potential impact of uncontrolled, non-specific events on the university's business processes. The BIA phase also should determine what and how much is at risk by identifying critical business functions and prioritizing them. The **BIA** should estimate the maximum allowable downtime for critical business processes, recovery point objectives and backlogged transactions, and the costs associated with downtime.

University and unit leadership will establish recovery priorities for business processes that identify key and essential personnel, technologies, facilities, communications systems, vital records, and data. The BIA also considers the impact of legal and regulatory requirements such as the privacy and availability of customer data and required notifications.

The Emergency Management Plan lists 42 incidents that can impact university operations. The plan also gives a broad university risk assessment of emergency incidents through the probability of occurrence and the estimated impact on public health, safety, property, and the environment. This list is a good starting point for unit **BIA** and risk assessments. If all units start with this document, it will improve the consistency of responses and help personnel involved in the **BIA** phase compare and evaluate business process requirements. This phase may initially prioritize business processes based on their importance to the institution's achievement of strategic goals and maintenance of safe and sound practices. However, this prioritization should be revisited once the business processes are modeled against various threat scenarios so that a **BCP** can be developed.

When determining the university's critical needs, reviews should be conducted for all functions, processes, and personnel within each unit. Each college, school, department, and unit should document the mission critical functions performed. Units should consider the following questions:

- What specialized equipment is required and how it is used?
- How would the department function if mainframe, network, and/or Internet access were not available?
- What single points of failure exist and how significant are those risks?
- What are the critical outsourced relationships and dependencies?
- What is the minimum number of staff and space that would be required at a recovery site?
- What special forms or supplies would be needed at a recovery site?
- What communication devices would be needed at a recovery site?
- What critical operational or security controls require implementation prior to recovery?
- Is there any potential impact from common recovery sites?
- Have employees received cross-training and has the department defined back-up functions/roles employees should perform if key personnel are not available?
- Are emotional support and family care needs adequately considered?

2.3. Risk Assessment

The risk assessment is the second step in developing a BCP. It should include:

- A prioritization of potential business disruptions based upon severity and likelihood of occurrence
- A gap analysis comparing the institution's existing BCP, if any, to what is necessary to achieve recovery time and point objectives
- An analysis of threats based upon the impact on the university as a whole as well as students, staff, faculty, and visitors, not just the nature of the threat

Many units within the university have used the Enterprise Risk Management System to analyze risk. This planning tool is useful in developing the necessary risk information. This risk assessment step is critical and has significant bearing on whether business continuity planning efforts will be successful. If the threat scenarios developed are unreasonably limited, the resulting **BCP** may be inadequate. During the risk assessment step, business processes and the business impact analysis assumptions are stress tested with various threat scenarios. This will result in a range of outcomes, some that require no action for business processes to be successful and others that will require significant **BCP**s to be developed and supported with resources (financial and personnel).

The Office of Campus Safety and Security will work with university units to develop realistic threat scenarios that may potentially disrupt their business processes and ability to meet the expectations of students, staff, faculty, and visitors. Threats can take many forms, including malicious activity as well as natural and technical disasters.

Where possible, units should analyze a threat by focusing on its impact on the entity, not the nature of the threat. For example, the effects of certain threat scenarios can be reduced to business disruptions that affect only specific work areas, systems, facilities (i.e., buildings), or geographic areas. Additionally, the magnitude of the business disruption depends upon a wide variety of threat scenarios based on practical experiences and potential circumstances and events. If threat scenarios are not comprehensive, the BCPs may be too basic and omit reasonable steps that could improve business processes' resiliency to disruptions. Threat scenarios should consider the impact of a disruption and probability of the threat occurring.

Threats that could impact a unit can range from those with a high probability of occurrence and low impact to the unit or university (e.g., brief power interruptions), to those with a low probability of occurrence and high impact on the institution (e.g., hurricane, terrorism).

High probability threats are often supported by very specific BCPs. However, the most difficult threats to address are those that have a high impact on the university but a low probability of occurrence. Using a risk assessment, BCPs may be more flexible and adaptable to specific types of disruptions that may not be initially considered.

It is at this point in the business continuity planning process that university units must perform a gap analysis. In this context, a gap analysis is a methodical comparison of what types of plans the unit needs to maintain, resume, or recover normal business operations in the event of a disruption versus what the existing BCP provides. The difference between the two highlights additional risk exposure that management and the board need to address in BCP development. The risk assessment considers:

- The impact of various business disruption scenarios on both the institution and the students, staff, faculty, and visitors
- The probability of occurrence based, for example, on a rating system of high, medium, and low
- The loss impact on information services, technology, personnel, facilities, and service providers from both internal and external sources
- The safety of critical processing documents and vital records
- A broad range of possible business disruptions, including natural, technical, and human threats

When assessing the probability of a specific event occurring, units should consider the geographic location of facilities and their susceptibility to natural threats (e.g., location in a flood plain) and the proximity to critical infrastructures (e.g., power sources, nuclear power plants, airports, points of interest, major highways, railroads). The risk assessment should include all locations and facilities. Worst-case scenarios, such as destruction of the facilities and loss of life, should be considered. At the conclusion of this phase, the unit will have prioritized business processes and estimated how they may be disrupted under various threat scenarios.

2.4. Risk Management/Business Continuity Plan Development

Risk management is the development of a written, enterprise- wide BCP. The institution should ensure that the BCP is:

- Written and disseminated so that various groups of personnel can implement it in a timely manner
- Specific regarding what conditions should prompt implementation of the plan
- Specific regarding what immediate steps should be taken during a disruption
- Flexible to respond to unanticipated threat scenarios and changing internal conditions

- Focused on how to get the business up and running in the event that a specific facility or function is disrupted, rather than on the precise nature of the disruption
- Effective in minimizing service disruptions and financial loss

After conducting the **BIA** and risk assessment, management should prepare a written BCP. The plan should document strategies and procedures to maintain, resume, and recover critical business functions and processes and should include procedures to execute the plan's priorities for critical versus non-critical functions, services, and processes. The BCP should describe in some detail the types of events that would lead up to the formal declaration of a disruption and the process for invoking the BCP. It should describe the responsibilities and procedures to be followed by each continuity team and contain contact lists of critical personnel. The BCP should describe in detail the procedures to be followed to recover each business function affected by the disruption and should be written in such a way that various groups of personnel can implement it in a timely manner.

As previously discussed, a BCP is more than recovery of the technology, but rather a recovery of all critical business operations. The plan should be flexible to respond to changing internal and external conditions and new threat scenarios. Rather than being developed around specific events (e.g. fire vs. tornado), the plan will be more effective if it is written to adequately address specific types of scenarios and the desired outcomes. A BCP should describe the immediate steps to be taken during an event in order to minimize the damage from a disruption as well as the action necessary to recover. Thus, business continuity planning should be focused on maintaining and resuming. Recovering units would respond if:

- Critical personnel are not available
- Critical buildings, facilities, or geographic regions are not accessible
- Equipment malfunctions (hardware, telecommunications, operational equipment)
- Software and data are not accessible or are corrupted
- Vendor assistance or service provider is not available
- Utilities are not available (power, telecommunications)
- Critical documentation and/or records are not available

Units should carefully consider the assumptions on which the BCP is based. Planners should not assume a disaster will be limited to a single facility or a small geographic area. Units should not assume they will be able to gain access to facilities that have not been damaged or that critical personnel (including senior leadership) will be available immediately after the disruption. Assuming public transportation systems such as airlines, railroads, and subways will be operating may also be incorrect.

The university should not assume the telecommunications system will be operating at normal capacity. The BCP consists of many components that are both internal and external to the university. The activation of a BCP and restoration of business in the event of an emergency is dependent on the successful interaction of various components. The overall strength and effectiveness of a BCP can be decreased by its weakest component. An effective BCP coordinates across its many components, identifies potential process or system dependencies, and mitigates the risks from interdependencies.

Typically, the unit and university business continuity coordinators or teams facilitate the identification of risk and the development of risk mitigation strategies across business areas. Internal causes of interdependencies can include line of business dependencies, telecommunication links, and/or shared resources (i.e., print

operations or e-mail systems). External sources of interdependencies that can negatively impact a BCP can include telecommunication providers, service providers, customers, business partners, and suppliers.

2.5. Other Policies, Standards, and Processes

Other university policies, in addition to the BCP, should incorporate business continuity planning considerations. These include:

- System development life cycles
- Change control policies
- Data synchronization procedures
- Employee training and communication plans
- Insurance policies
- Government, media, and community relations policies
- Security

In addition to documenting **BCP**s, other policies, standards, and practices should address continuity and availability considerations. These include system development life cycles (**SDLC**), change control, and data synchronization

2.5.1. Systems Development Life Cycle (SDLC) and Project Management

As part of the **SDLC** process, units should incorporate business continuity considerations into project plans. Evaluating business continuity needs during the **SDLC** process allows for advance preparation when an institution is acquiring or developing a new system. It also facilitates the development of a more robust system that will permit easier continuation of business in the event of a disruption. During the development and acquisition of new systems, SDLC standards and project plans should address, at a minimum, issues such as:

- Unit requirements for resumption and recovery alternatives
- Information on backup and storage
- Hardware and software requirements at recovery locations
- BCP and documentation maintenance
- Disaster recovery testing
- Staffing and facilities

2.5.2. Change Control

Change management and control policies/procedures should appropriately address and document the business continuity considerations. Change management in computer systems should be included in the change control process and implementation phase.

Whenever a system change is made to an application, operating system, or utility that resides in the production environment, a methodology should exist to ensure all backup copies of those systems are updated to reflect the new environment. In addition, if a new or changed system is implemented and results in new hardware, capacity requirements, or other technology changes, management should ensure the **BCP** is updated and the recovery site can support the new production environment.

2.5.3. Data Synchronization

Data synchronization can become a challenge when dealing with an active/back-up environment. The larger and more complex an institution is (i.e., shorter acceptable operational outage period, greater volume of data,

greater distance between primary and backup location), the more difficult synchronization can become. If backup copies are produced as of the close of a business day and a disruption occurs relatively late the next business day, all the transactions that took place after the backup copies were made would have to be recreated, perhaps manually, in order to synchronize the recovery site with the primary site.

Management and testing of contingency arrangements are critical to ensure the recovery environment is synchronized with the primary work environment. This testing includes ensuring software versions are current, interfaces exist and are tested, and communication equipment is compatible. If the two locations, underlying systems, and interdependent business units are not synchronized, there is the likely possibility that recovery at the backup location could encounter significant problems. Proper change control, information backup, and adequate testing can help avoid this situation. In addition, management should ensure the backup facility has adequate capacity to process transactions in a timely manner in the event of a disruption at the primary location.

2.5.4. Employee Training and Communication Planning

The university will develop enterprise-wide training and exercises. However, all units should provide business continuity training for personnel to ensure all parties are aware of their responsibilities should a disaster occur. Key employees should be involved in the business continuity development process as well as periodic training exercises. The university will incorporate enterprise-wide training as well as specific training for individual business units. Employees should be aware of which conditions call for implementing all or parts of the **BCP**, who is responsible for implementing **BCP**s for business units and the institution, and what to do if these key employees are not available at the time of a disaster. Cross-training should be utilized to anticipate restoring operations in the absence of key employees. Employee training should be regularly scheduled and updated to address changes to the **BCP**.

Communication planning should identify alternate communication channels to utilize during a disaster, such as pagers, cell phones, e-mail, or two-way radios. An emergency telephone number, e-mail address, and physical address list should be provided to employees to assist in communication efforts during a disaster. The list should provide all alternate numbers since one or more telecommunications systems could be unavailable. Additionally, the phone list should provide numbers for vendors, emergency services, transportation, and regulatory agencies. Wallet cards, Internet postings, and calling trees are possible ways to distribute information to employees. Further, units should establish reporting or calling locations to assist them in accounting for all personnel following a disaster.

Units should consider developing an awareness program to inform the university community, service providers, and outside agencies how to contact the institution if normal communication channels are not in operation. The plan should also designate personnel who will communicate with the media, government, vendors, and other companies and provide for the type of information to be communicated.

2.5.5. Insurance (generally, states and state institutions are self-insurers)

Insurance is commonly used to recoup losses from risks that cannot be completely prevented. Generally, insurance coverage is obtained for risks that cannot be entirely controlled yet could represent a significant potential for financial loss or other disastrous consequences. The decision to obtain insurance should be based on the probability and degree of loss identified during the **BIA**. Units of the university must determine potential exposure for various types of disasters and review the insurance options available through the university to ensure appropriate insurance coverage is provided.

University leaders must know the limits and coverage of the university and examine the university insurance policies to make sure coverage is appropriate given the risk profile of the unit. All units must perform an annual insurance review to ensure the level and types of coverage are commercially reasonable and consistent with any legal, management, and board requirements. Also, units must create and retain a comprehensive hardware and software inventory list in a secure off-site location in order to facilitate the claims process.

Units should be aware of the limitations of insurance. Insurance can reimburse for some or all of the financial losses incurred as the result of a disaster or other significant event. However, insurance is by no means a substitute for an effective **BCP**, as its primary objective is not the recovery of the business. For example, insurance cannot reimburse a unit for damage to its reputation.

2.5.6. Government and Community

The university will coordinate with community and government officials and the news media to ensure the successful implementation of the **BCP**. Ideally, these relationships will be established during the planning or testing phases of business continuity planning. The university will develop the proper protocol in case a city-wide or region-wide event impacts the institution's operations. The university will contact state and local authorities during the risk assessment process to inquire about specific risks or exposures for all their geographic locations and special requirements for accessing emergency zones. During the recovery phase, facilities access, power, and telecommunications systems would be coordinated with various entities to ensure timely resumption of operations. Facilities access should be coordinated with the police and fire department and depending on the nature and extent of the disaster, possibly the Travis County Emergency Operations Center, the State of Texas Emergency Operations Center, and the Federal Emergency Management Agency (**FEMA**).

2.6. Risk Monitoring

Risk monitoring is the final step in business continuity planning. It should ensure that the units **BCP** is viable through:

- Testing the BCP at least annually
- Subjecting the BCP to independent audit and review
- Updating the BCP based upon changes to personnel and the internal and external environments

Risk monitoring ensures a **BCP** is viable through testing, independent review, and periodic updating.

3. Direction, Control, Organization, and Coordination

3.1. Senior Leadership Orders of Succession & Responsibilities

The University Orders of Succession (OOS) allow for an orderly and predefined transition of senior leadership during an emergency if any officials are unavailable to execute their legal duties. The designation as a successor enables that individual to act for and exercise the powers of a principal in emergency or continuity situations. The following table presents the University's OOS for senior leadership positions.

Position	Successors
University President	1. Executive Vice President & Provost
	2. Senior Vice President & Chief Financial Officer
	3. Vice President for Student Affairs & Dean of Students
	4. Vice President for Legal Affairs
	5. Vice President for Diversity & Engagement

The university senior leadership to include deans, vice presidents, associate vice presidents, directors, and equivalents are responsible for:

- Allocating sufficient resources and knowledgeable personnel to develop the BCP
- Developing a continuity and succession of leadership
- Setting policy by determining how the institution will manage and control identified risk
- Approving the BCP on an annual basis

Senior leadership, as noted above, are responsible for identifying, assessing, prioritizing, managing, and controlling risks. They must ensure necessary resources are devoted to creating, maintaining, and testing the plan.

These leaders fulfill their business continuity planning responsibilities by setting policy, prioritizing critical business functions, allocating sufficient resources and personnel, providing oversight, approving the BCP, providing training, and ensuring maintenance of a current plan.

The effectiveness of business continuity planning depends on the university's leadership commitment and ability to clearly identify what makes existing business processes work. Each college, school, department, or unit must evaluate its own unique circumstances and environment to develop a comprehensive **BCP**.

At the university, all business continuity planning will be coordinated by the associate vice president of Campus Safety and Security through the Office of Emergency Preparedness. While the planning personnel may recommend certain prioritization, the senior leadership of the university is responsible for understanding critical business processes and subsequently establishing plans to meet business process requirements in a safe and sound manner.

4. Plan Development and Maintenance

The Business Continuity Plan Annex is a component of the Emergency Management Plan. The Business Continuity Plan Annex will be reviewed annually and will be updated and revised as appropriate.

Interim revisions will be made when one of the following occurs:

- A change in university site or facility configuration that materially alters the information contained in the plan or materially affects implementation of the plan
- A material change in response resources
- An incident occurs that requires a review
- Internal assessments, third party reviews, or experience in drills or actual responses identify significant changes that should be made in the plan
- New laws, regulations, or internal policies are implemented that affect the contents or the implementation of the plan
- Other changes deemed significant

Plan changes, updates, and revisions are the responsibility of the Associate Vice President for Campus Safety and Security who will ensure that any plan changes are distributed accordingly.

5. Authorities

- Federal

- Homeland Security Presidential Directive/HSPD-5, Management of Domestic Incidents
- NFPA Standard 1600: Standard on Disaster/Emergency Management and Business Continuity Programs
- NFPA 1561 Standard on Emergency Services Incident Management System 2005 Edition
- NFPA72 Annex E Mass Notification Systems

- **State of Texas**
  - Texas Administrative Code Title 1 Part 10 Chapter 202 Subchapter C Rule §202.74
  - Texas Executive Order RP 57
  - Texas Department of Information Resources: business continuity planning Guidelines. December 2004
  - National Response Framework
  - National Incident Management System
  - Joint Commission for Accreditation of Health Organizations: Standard EC1.4

- **The University of Texas System**
  - Memo to Chancellor Yudof dated July 20, 2007: Subject: Survey on Emergency and Incident Response Exercises

Appendices

I. Definitions

Back-up Generations: A methodology for creating and storing backup files whereby the youngest (or most recent file) is referred to as the "son", the prior file is called the "father", and the file two generations older is the "grandfather". This backup methodology is frequently used to refer to master files for financial applications.

Business Continuity: An ongoing process supported by senior management and funded to ensure that the necessary steps are taken to identify the impact of potential losses, maintain viable recovery strategies, recovery plans, and continuity of services (NFPA 1600).

Business Continuity Plan (BCP): A comprehensive written plan to maintain or resume business in the event of a disruption.

Business Impact Analysis (BIA): The process of identifying the potential impact of uncontrolled, non- specific events on an institution's business processes.

Business Resilience: An enterprise-wide state of readiness including people, processes, information, facilities, and third parties as well as technology to cope effectively with potentially disruptive events.

Data Synchronization: The comparison and reconciliation of interdependent data files at the same time so that they contain the same information.

Disaster/Emergency Management: An ongoing process to prevent, mitigate, prepare for, respond to, and recover from an incident that threatens life, property, operations, or the environment (NFPA 1600).

Disaster Recovery Plan: A plan that describes the process to recover from major processing interruptions.

Emergency Management Program: A program that implements the mission, vision, and strategic goals and objectives as well as the management framework of the program and organization (NFPA 1600).

Emergency Plan: The steps to be followed during and immediately after an emergency such as a fire, tornado, bomb threat, etc.

Encryption: The conversion of information into a code or cipher.

FEMA: Acronym for Federal Emergency Management Agency.

Gap Analysis: A comparison that identifies the difference between actual and desired outcomes.

GETS: Acronym for the Government Emergency Telecommunications Service card program. GETS cards provide emergency access and priority processing for voice communications services in emergency situations.

HVAC: Acronym for heating, ventilation, and air conditioning.

Impact Analysis [Business Impact Analysis (BIA)]: A management level analysis that identifies the impacts of losing the entity's resources (NFPA 1600).

Incident Command System: A standardized on-scene emergency management concept specifically designed to allow its user(s) to adopt an integrated organizational structure equal to the complexity and demands of single or multiple incidents without being hindered by jurisdictional boundaries (ICS-010-1).

Incident Management System (IMS): The combination of facilities, equipment, personnel, procedures, and communications operating within a common organizational structure designed to aid in the management of resources during incidents (NFPA 1600).

Media: Physical objects that store data, such as paper, hard disk drives, tapes, and compact disks (CDS).

Mirroring: A process that duplicates data to another location over a computer network in real time or close to real time.

Mitigation: Activities taken to reduce the severity or consequences of an emergency (NFPA 1600).

Mutual Aid/Assistance Agreement: A prearranged agreement between two or more entities to share resources in response to an incident (NFPA 1600).

Object Program: A program that has been translated into machine-language and is ready to be run (i.e., executed) by the computer.

PBX: Acronym for private branch exchange.

Preparedness: Activities, tasks, programs, and systems developed and implemented prior to an emergency that are used to support the prevention of, mitigation of, response to, and recovery from emergencies (NFPA 1600).

Prevention: Activities to avoid an incident or to stop an emergency from occurring (NFPA 1600).

Reciprocal Agreement: An agreement whereby two organizations with similar computer systems agree to provide computer processing time for the other in the event one of the systems is rendered inoperable. Processing time may be provided on a “best effort” or “as time available” basis.

Recovery: Activities and programs designed to return conditions to a level that is acceptable to the entity (NFPA 1600).

Recovery Point Objectives: The amount of data that can be lost without severely impacting the recovery of operations.

Recovery Site: An alternate location for processing information (and possibly conducting business) in an emergency. Usually distinguished as “hot” sites that are fully configured centers with compatible computer equipment and “cold” sites that are operational computer centers without the computer equipment.

Recovery Time Objectives: The period of time that a process can be inoperable.

Recovery Vendors: Organizations that provide recovery sites and support services for a fee.

Resource Management: A system for identifying available resources to enable timely and unimpeded access to resources needed to prevent, mitigate, prepare for, respond to, or recover from an incident (NFPA 1600).

Response: Immediate and ongoing activities, tasks, programs, and systems to manage the effects of an incident that threatens life, property, operations, or the environment (NFPA 1600).

Routing: The process of moving information from its source to a destination.

Server: A computer or other device that manages a network service. An example is a print server, a device that manages network printing.

Situation Analysis: The process of evaluating the severity and consequences of an incident and communicating the results (NFPA 1600).

Source Program: A program written in a programming language (such as C, Pascal, or COBOL). A compiler translates the source code into a machine language object program.

Stakeholder: Any individual, group, or organization that might affect, be affected by, or perceive itself to be affected by the emergency (NFPA 1600).

System Development Life Cycle (SDLC): A written strategy or plan for the development and modification of computer systems, including initial approvals, development documentation, testing plans and results, and approval and documentation of subsequent modifications.

T-1 line: A special type of telephone line for digital communication only.

UPS: Acronym for uninterruptible power supply. Typically, a collection of batteries that provide electrical power for a limited period of time.

Utility Programs: A program used to configure or maintain systems, or to make changes to stored or transmitted data.

UT Institution: The University of Texas System's nine academic teaching institutions and six health centers.

UT System Administration: The central administrative offices that lead and serve the UT Institutions by undertaking certain central responsibilities that result in greater efficiency or higher quality than could be achieved by individual institutions or that fulfill legal requirements.

Vaulting: A process that periodically writes backup information over a computer network directly to the recovery site

II. Functions

In order to preserve and advance the University of Texas at Austin's research, teaching and public service programs, a stable and secure infrastructure of services and administration, is essential. The highest priorities of life, safety, property, and restoration become the interim mission of the University. The overall priorities of the University during an emergency or disaster are the protection of lives, live assets, valuable research processes, property, the community, and the environment. One of the most important aspects of emergency planning and preparedness is determining the essential functions of each university unit that are critical to the operation of the University. Personnel and resources necessary to maintain operations throughout an emergency must be in place with appropriate trained staff in advance. Establishing what is mission critical and essential is a process that must engage unit staff, faculty, unit leaders and senior leaders at the department and college administrative levels. The University of Texas defines these levels of mission tasks: Critical; Essential; Non-Essential. The definitions of these levels are:

- Critical—those operations that are vital to the operation and/or may pose a life safety risk. For each critical activity, mitigation strategies should be implemented and a recovery process developed. For the University of Texas at Austin the following organizations are classified as critical:
    - Campus Safety and Security University
    - Police Department
    - Emergency Preparedness
    - Environmental Health and Safety
    - Fire Prevention Services
    - Parking and Transportation Services
    - University Operations
    - Communications
    - Facilities Service
    - Utilities
    - Information Technology Services
    - Dean of Students Office
    - Division of Housing and Food Service
    - Human Resource Services
    - University Health Services
    - Counseling and Mental Health Center
    - Animal Resource Center
    - Office of the Vice President and Chief Financial Officer

Other organizations may be classified as critical if their function is deemed so. Such organizations must notify the Associate Vice President of Human Resource Services and the Associate Vice President for Campus Safety and Security to ensure inclusion in all emergency communications.

- Essential—Not critical, difficult to operate without, but the organization could function for a period of time. Identify persons who support the critical functions.
- Non-essential—Disruption would merely be an inconvenience. Identify persons who support the critical functions.

The President of the University or his/her designated representative will make the decision concerning closure or any emergency condition. Each university vice president, dean and director/department chair will establish a

"Leadership Succession" list of who can make operational decisions if the head of the unit leader is absent. Additionally, each vice president, dean and director/department chair is responsible for updating and publishing each year a list of essential personnel that must remain on file with the Assistant Vice President for Human Resources and the Associate Vice President for Campus Safety and Security.

All university organizations will determine and state their essential functions in their Business Continuity Plan and persons responsible to perform those essential functions. Supervisors of essential personnel are responsible for ensuring that personnel designated as "essential" understand their assignments and report to work whenever this policy is in effect. Employees whose responsibilities and duties are vital to the continuity of university operations are required to report to work during an authorized closing. Essential personnel are required to be notified of their status in writing by their supervisors.

The Emergency Management Plan and each unit Business Continuity Plan are a supplement to the University's administrative policies and procedures. Under emergency activation and implementation, these plans set forth the authority to direct operations, direct staff assignments, procure and allocate resources, and take measures to restore normal services and operations. Ultimately, trust must be developed through all levels of the public and private sector. After obtaining top level support, the process must involve the people who will respond to and manage the critical incident.

III. Internal and External Threats

While a BCP should be focused on restoring the university's ability to do business, regardless of the nature of the disruption, different types of disruptions may require a variety of responses in order to resume business. Many types of disasters impact not only the university but also the surrounding community. The human element can be unpredictable in a crisis situation and should not be overlooked when developing a BCP. Employees and their families could be affected as significantly as, or more significantly than, the university. Therefore, university leadership must consider the impact such a disruption would have on personnel the institution would rely on during such a disaster. For example, providing accommodations and services to family members of employees or ensuring that alternate work facilities are in close proximity to employee residences may make it easier for employees to implement the institution's BCP. Also, cross-training of personnel and succession planning may be just as essential as backup procedures addressing equipment, data, operating systems, and application software.

This Appendix discusses three primary categories of internal and external threats: malicious activity, natural disasters, and technical disasters.

A. Malicious Activity

- **Fraud, Theft, Or Blackmail**

  Since fraud, theft, or blackmail may be perpetrated more easily by insiders, implementation of employee awareness programs and computer security policies is essential. These threats can cause the loss, corruption, or unavailability of information, resulting in a disruption of service to customers. Restricting access to information that may be altered or misappropriated reduces exposure. The institution may be held liable for release of sensitive or confidential information pertaining to its customers; therefore, appropriate procedures to safeguard information are warranted.

- **Sabotage**

  Personnel should know how to handle intruders, bomb threats, and other disturbances. The locations of critical operation centers should not be publicized and the facilities should be inconspicuous. A disgruntled employee may try to sabotage facilities, equipment, or files. Therefore, personnel policies should require the immediate removal from the premise of any employee reasonably considered a threat, and the immediate revocation of their computer and facility access privileges.

- **Terrorism**

  The risk of terrorism is real and adequate business continuity planning is critical for a university in the event a terrorist attack occurs. Some forms of terrorism (e.g., chemical or biological contamination) may leave facilities intact but inaccessible for extended periods of time. The earlier an attack is detected the better the opportunity for successful treatment and recovery. Active monitoring of federal and state emergency warning systems, such as local, state and FEMA, and the Center for Disease Control (CDC) should be considered. Terrorism is not new, but the magnitude of disruption and destruction continues to increase. The loss of life, total destruction of facilities and equipment, and emotional and psychological trauma to employees can be devastating. Collateral damage can result in the loss of communications, power, and access to a geographic area not directly affected. Terrorist attacks can range from bombings of facilities to cyber-attacks on the communication, power, or financial infrastructures. The goal of cyber-terrorism is to disrupt the functioning of information and communications systems. Unconventional attacks could also include the use of chemical, biological, or

nuclear material. Bioterrorists may employ bacterial or viral agents with effects that are delayed, making prevention, response, and recovery problematic. While the probability of a full-scale nuclear attack is remote, it is necessary to address the readiness to deal with attacks on nuclear power plants and industries using nuclear materials and for attacks initiated by means of “dirty” nuclear devices, weapons combining traditional explosives with radioactive materials.

B. Natural Disasters

- **Fire**

  A fire can result in loss of life, equipment, and data. Data center personnel must know what to do in the event of a fire to minimize these risks. Instructions and evacuation plans should be posted in prominent locations and should include the designation of an outside meeting place so personnel can be accounted for in an emergency and should include guidelines for securing or removing media if time permits. Fire drills should be periodically conducted to ensure personnel understand their responsibilities. Fire alarm boxes and emergency power switches should be clearly visible and unobstructed. All primary and backup facilities should be equipped with heat or smoke detectors. Ideally, these detectors should be located in the ceiling, in exhaust ducts, and under raised flooring. Detectors situated near air conditioning or intake ducts that hinder the build-up of smoke may not trigger the alarm. The emergency power shutdown should deactivate the air conditioning system. Walls, doors, partitions, and floors should be fire-resistant. Also, the building and equipment should be grounded correctly to protect against electrical hazards. Lightning can cause building fires, so lightning rods should be installed as appropriate. Local fire inspections can help in preparation and training. Additionally, dry pipe sprinkler systems should be used, which activate upon detection of a fire and fill the pipe with water only when required, thereby minimizing the risk of water damage from busted pipes. These systems should be the staged type, where the action triggered by a fire detector permits time for operator intervention before it shuts down the power or releases fire suppressants. Personnel should know how to respond to these automatic suppression systems as well as the location and operation of power and other shut-off valves. Waterproof covers should be located near sensitive equipment in the event that the sprinklers are activated. Hand extinguishers and floor tile pullers should be placed in easily accessible and clearly marked locations. The extent of fire protection required depends on the degree of risk an institution is willing to accept and local fire codes or regulations.

- **Floods and Other Water Damage**

  Facilities located in or near a flood plain expose units to increased risk. Units should take the necessary actions to manage that level of exposure. As water seeks the lowest level, critical records and equipment should be located on upper floors, if possible, to mitigate this risk. Raised flooring or elevating the wiring and servers several inches off the floor can prevent or limit the amount of water damage. In addition, institutions should be aware that water damage could occur from other sources such as broken water mains, windows, or sprinkler systems. If there is a floor above the computer or equipment room, the ceiling should be sealed to prevent water damage. Water detectors should be considered as a way to provide notification of a problem.

- **Severe Weather**

  A disaster resulting from an earthquake, hurricane, tornado, or other severe weather typically would have its probability of occurrence defined by geographic location. Given the random nature of these

natural disasters, institutions located in an area that experiences any of these events should consider including appropriate scenarios in their business continuity planning process. In instances where early warning systems are available, management should provide procedures to be implemented prior to the disaster to minimize losses.

- **Air Contaminants**

  Some disasters produce a secondary problem by polluting the air for a wide geographic area. Natural disasters such as flooding can also result in significant mold or other contamination after the water has receded. The severity of these contaminants can impact air quality at an institution and even result in evacuation for an extended period of time. Business continuity planning should consider the possibility of air contamination and provide for evacuation plans and the shutdown of HVAC systems to minimize the risks caused by the contamination. Additionally, consideration should be given to the length of time the affected facility could be inoperable or inaccessible.

C. Technical Disasters

- **Hazardous Chemical Spill**

  The university is located near a major interstate highway, US highways, and rail lines. The risk of a chemical spill is real and must be factored into all BCPS. A leak or spill can result in air contamination, as described above, and chemical fires as well as other health risks. Institutions should make reasonable efforts to determine the types of chemicals being produced or transported nearby, obtain information about the risks each may pose, and take steps to mitigate such risks.

- **Communications Failure**

  The distributed processing environment has resulted in an increased reliance on telecommunications networks for both voice and data communications to customers, third parties, and backup sites. Units lacking diversity in their telecommunications infrastructures may be susceptible to single points of failure in the event a disaster affects one or more of these critical systems. The university will make the effort to identify and document potential single points of failure within their internal and external communications systems. If arrangements are made with multiple telecommunications providers for diverse routing to achieve redundant systems in an attempt to mitigate this risk, management should, to the extent possible, identify common points of failure within these systems. One technique is to perform an end-to-end trace of all critical or sensitive circuits to search for single points of failure such as a common switch, router, PBX, or telephone central office. In addition to restoring data communication lines with affiliates and vendors, restoration of communications with employees will be critical to any BCP. As an alternative to voice landlines, institutions should consider cell phones, two-way radios, text-based pagers, corporate and public e-mail systems, and Internet- based instant messaging. Another alternative would be to register and establish a standby World Wide Web home page that is activated during a disaster and is used to communicate information and individual requirements. Satellite phones may also be useful for communicating with key personnel.

- **Power Failure**

  The loss of power can occur for a variety of reasons, including storms, fires, malicious acts, brownouts, and blackouts. A power failure could result in the loss of computer systems, lighting, heating and cooling systems, and security and protection systems. Additionally, power surges can occur as power is

restored, and without proper planning, can cause damage to equipment. As a means to control this risk, voltage entering the computer room should be monitored by a recording voltmeter and regulated to prevent power fluctuations. In the event of power failure, institutions should use an alternative power source, such as uninterruptible power supplies (**UPS**), or gasoline, kerosene, natural gas, or diesel generators. A **UPS** is essentially a collection of standby batteries that provide power for a short period of time. When selecting a **UPS**, an institution should make sure that it has sufficient capacity to provide ample time to shut down the system in an orderly fashion to ensure no data is lost or corrupted. Some UPS equipment can initiate the automated shut down of systems without human intervention. If processing time is more critical, an organization may arrange for a generator, which will provide power to at least the mission critical equipment during extended power outages. Management should maintain an ample supply of fuel on hand and have arrangements for replenishment. One potential advantage of natural gas is that it is supplied by pipeline, avoiding the need to truck it in and maintain it on site. It is important to note that if a disruption is significant enough, it may result in the inability to obtain additional fuel. Further, fuel pumps and delivery systems may not be operable. It is also important to ensure alternative power supplies receive periodic maintenance and testing to maintain operability. The university will coordinate with local authorities on ordinances pertaining to the location of generators and the storage and delivery of fuel if such systems are determined to be needed.

- **Equipment and Software Failure**

  Equipment and software failures may result in extended processing delays and/or implementation of BCPS for various business units depending on the severity of the failure. The performance of preventive maintenance enhances system reliability and should be extended to all supporting equipment such as temperature and humidity control systems and alarm or detecting devices.

- **Transportation System Disruptions**

  Units should not assume regional or national transportation systems will continue to operate normally during a disruption. Air traffic and/or trains may be halted by natural or technical disasters, malicious activity, work stoppages, or accidents. This can adversely impact cashier operations and other business operations. Units should investigate the option of using private entities to mitigate disruptions.

IV. Interdependencies and Telecommunications Infrastructure

Voice and data communication BCP specifics are stored in "Restarting Texas", the official BCP service for the university. Due to the security sensitive nature of this information, general approaches recommended for any institution are included below.

Voice and data communications are essential for conducting business and connecting critical elements of units such as business areas, customers, and service providers/vendors. The advancement in network technologies allows greater geographic separation between people and system resources and/or primary and alternate processing locations. Network technologies have played a key role in enabling distributed processing environments, which reflect an increased reliance on telecommunications networks for both voice and data communications. Given their critical nature and importance, it is necessary for institutions to design high levels of redundancy and resiliency into their voice and data communication infrastructures. In addition, as critical as it is to have effective business continuity arrangements for a data center, it is equally important to have effective backup arrangements for voice and data telecommunications links. Since voice and data infrastructures are typically a shared resource across the different business areas of a unit, the dependency and criticality of these resources are further heightened.

The telecommunications infrastructure contains single points of failure that represent vulnerabilities and risks for financial institutions. Elements of risk reside within the public telecommunications network infrastructure and are outside the control of a single institution. This necessitates the need for units to be proactive in establishing robust processes to ensure telecommunication resiliency and diversity. The university will develop risk management practices to identify and eliminate single points of failure across their network infrastructures. Risk management strategies need to be incorporated into the design, acquisition, implementation, and maintenance processes related to communication networks and should address single points of failure or points of commonality relating to:

- Primary and backup network infrastructures
- Telecommunication carriers
- Points of entry into facilities
- Telecommunication routing through central offices
- PBXs within an institution

The university will actively manage our service relationship with telecommunication providers in order to manage risk more effectively. In management strategies:

- Establish service level agreements that address contingency measures and change management for services provided
- Establish processes to inventory and validate telecommunication circuits and routing paths
- Include a framework to periodically verify telecommunication routing paths

In addition to robust risk management practices, the units must have viable business continuity arrangements for voice and data services. At a minimum, telecommunications plans should address skilled human resources, internal and external connectivity, communications media, network equipment, and telecommunication management systems. The BCP should establish priorities and identify critical network components. Original plan components such as reliability, flexibility, and compatibility must also be considered in formulating the

backup plan. For example, a modem used for backup may not provide the level of service required, or a line may satisfactorily transmit voice, but be insufficient in quality and speed for data transmission. The costs of various backup alternatives should be weighed against the level of risk protection provided by the alternatives. This assessment also should address costs associated with testing, since all components of a plan should be tested periodically, including the communications media.

The **BCP** should address the practicality of each component. Selected alternatives should be able to accommodate the anticipated volumes or capacities at the necessary speeds to meet the established priorities. For example, several dial-up lines may not be a practical replacement for a T-1 line. Also, the backup plan should recognize availability and lead times required to employ certain components, such as installing additional lines or modems and multiplexers/concentrators at a recovery site.

The university will play a key role in the maintenance of financial systems. Units should be aware of certain government programs and offices that work to coordinate and expedite the restoration or procurement of telecommunication services during an emergency. The Office of Priority Telecommunications (**OPT**) under the National Communications System (**NCS**) administers the Telecommunications Service Priority System (**TSP**) which ensures priority treatment of the nation's most important telecommunication services supporting national security and emergency preparedness missions. This means that tsp designated circuits will be the first to be repaired in an emergency. All non-federal users requesting **TSP** provisioning or restoration are required federal regulator for information on the **TSP** program and whether they qualify for a TSP designation.

The university may qualify for sponsorship in the Government Emergency Telecommunications Service (**GETS**) card program. This program is also administered by **NCS** and provides emergency access and priority processing for voice communications services in emergency situations. Units that perform national security or emergency preparedness functions essential to the maintenance of the nation's economic posture during any national or regional emergency will qualify for program sponsorship.

The unit BCP should consider the security of alternative components to ensure data integrity. Switching from fiber optics to wire pairs, dedicated to switched, or digital to analog may make the line more susceptible to a wiretap or to line noise, which can result in errors. Using dial-up lines could facilitate access by the public. Additionally, where warranted, alternate equipment selected should be checked to determine if it permits encryption. The relative importance of the applications processed and the extent to which an institution depends on its telecommunications system will determine the degree of backup required. Leadership should make a careful appraisal of its backup telecommunications requirements, decide on an effective plan, detail the procedures, and test its effectiveness periodically.

V. Third-party Providers, Key suppliers, and Business Partners

Reliance on third-party providers, key suppliers, or business partners may expose the university to points of failure that may prevent resumption of operations in a timely manner. The risks in outsourcing information, transaction processing, and settlement activities include threats to the security, availability, and integrity of systems and resources, to the confidentiality of information, and to regulatory compliance. In addition, when a third party performs services on behalf of the institution, increased levels of credit, liquidity, transaction, and reputation risk can result. Institutions should review and understand service providers' **BCPS** and ensure critical services can be restored within acceptable timeframes based upon the needs of the institution. The contract should address the service provider's responsibility for maintenance and testing results and review audits to determine the adequacy of plans and the effectiveness of the testing process.

If possible, the university may consider participating in their service provider's testing process. Contracts should include detailed business recovery timeframes that meet the business continuity planning needs of the institution. The university's business continuity planning process will include developing call lists necessary for contacting key individuals at the service provider's primary and recovery locations. The unit's BCP should also address how it will be exchanging information with its service providers should the institution be operating from an alternative location, e.g., transmission via a branch facility that has redundant telecommunications links with the service provider.

A. Contracts

The university contracts with third-party service providers and other vendors for disaster recovery assistance. These arrangements can be cost-effective since the cost of maintaining a dedicated recovery site can be substantial. When contracting with third-party providers for recovery services, institutions should consider:

- **Staffing**: What kinds of technical support personnel is the service provider obligated to make available on site to assist institution employees in getting the recovery site operating?
- **Processing Time Availability**: Assuming other clients are also using the same recovery site, how much processing time is the institution entitled to on a particular computer system? Is the institution guaranteed a sufficient amount of processing time to handle the volume of work that will need to be done at the site?
- **Access Rights**: Since most backup sites can be used by numerous clients, does the institution have a guaranteed right to use the site in case of an emergency? Alternatively, does the service provider accept clients on a first- come, first-serve basis until the recovery site is at full capacity?
- **Hardware and Software**: Is the recovery site equipped with the precise computer hardware and software that the institution needs to continue operations? Will the institution be notified of changes in the equipment at the recovery site?
- **Security Controls**: Does the recovery site have sufficient physical and logical security to adequately protect the institution's information assets?
- **Testing:** Does the contract with the service provider permit the institution to perform at least one full-scale test of the recovery site annually? Does the service provider perform tests of its own BCP and submit test reports to the unit?
- **Confidentiality of Data**: In the event other businesses are also using the recovery site, what steps will the service provider take to ensure the security and confidentiality of institution data? Has the service provider entered into an appropriate contract with the customer that addresses the requirements of the Interagency Guidelines Establishing Standards for Safeguarding Customer Information?
- **Telecommunications:** Has the service provider taken appropriate steps to ensure the recovery site will have adequate telecommunications services (both voice and data) for the number of personnel that will be working at that site and the volume of data transmissions that are anticipated?
- **Reciprocal Agreements**: In the event the unit's recovery site is another university with whom there is a reciprocal agreement, does the other institution have sufficient excess computer capacity? Are the

hardware and software at the recovery site compatible with the affected institution's systems? Will the unit be notified of changes in equipment at the recovery site?

- **Space:** Does the recovery site have adequate space and related services to accommodate the affected institution's staff and enable them to conduct business? This may also include consideration of the space at the service provider or in the local community to provide food, toilets, medical supplies, family care, counseling, news, housing, and diversions to personnel.
- **Paper Files and Forms:** Does the recovery site maintain a sufficient inventory of paper- based files and forms that are necessary to the conduct of the affected institution's business?
- **Printing Capacity/Capability:** Does the recovery site maintain adequate printing capacity to meet the demand of the affected institution?
- **Contacts:** Who in the unit is authorized to initiate use of the backup site? Who does the unit contact at the backup site?

VI. Technology Components

Technology component BCP specifics are stored in "Restarting Texas", the official BCP service for the university. Due to the security sensitive nature of this information, general approaches recommended for any institution are included below.

The technology components that should be addressed in an effective **BCP** include:

- Hardware—mainframe, network, end-user
- Software—applications, operating systems, utilities
- Communications (network and telecommunications)
- Data files and vital records
- Operations processing equipment
- Office equipment

Comprehensive inventories will assist with the business resumption and recovery efforts and ensure all components are considered during plan development. Planning should include identifying critical business unit data that may only reside on individual workstations, which may or may not adhere to proper backup schedules. Additionally, the plan should address vital records, necessary backup methods, and appropriate backup schedules for these records. Units should exercise caution when identifying non-critical assets. A unit's telephone banking, Internet banking, credit authorization, or ATM systems may not seem mission critical when systems are operating normally. However, these systems may play a critical role in the **BCP** and be a primary delivery channel to service customers during a disruption. Similarly, a unit's electronic mail system may not appear to be mission critical, but may be the only system available for employee or external communication in the event of a disruption.

A. Data Center Recovery Alternatives

The university will make formal arrangements for alternate processing capability in the event their data processing site becomes inoperable or inaccessible. The type of recovery alternative selected will vary depending on the criticality of the processes being recovered and the recovery time objectives. Recovery plan alternatives may take several forms and involve the use of another data center or installation, such as a third-party service provider. A legal contract or agreement should evidence recovery arrangements with a third-party

vendor. The following are acceptable alternatives for data center recovery. However, institutions will be expected to describe their reasons for choosing a particular alternative and why it is adequate based on their size and complexity.

- **Hot Site (traditional "active/backup" model**): A hot site is fully configured with compatible computer equipment and typically can be operational within several hours. The university may rely on the services of a third party to provide backup facilities. The traditional active/backup model requires relocating, at a minimum, core employees to the alternative site. This model also requires backup media to be transferred off-site on at least a daily basis. Large units that operate critical real-time processing operations or critical high- volume processing activities should consider mirroring or vaulting. If a unit is relying on a third party to provide the hot site, there remains a risk that the capacity at the service provider may not be able to support their operations in the event of a regional or large-scale event. Smaller offices may contract for a "mobile hot site", i.e., a trailer outfitted with the necessary computer hardware that is towed to a predetermined location in the event of a disruption and connected to a power source.

- **Duplicate Facilities/Split Operations ("active/active" model):** Under this scenario, two or more separate, active sites provide inherent backup to one another. Each site has the capacity to absorb some or all of the work of the other site for an extended period of time. This strategy can provide almost immediate resumption capacity depending on the systems used to support the operations and the operating capacity at each site. The maintenance of excess capacity at each site and added operating complexity can have significant costs. Even using the active/active model, current technological limitations preclude wide geographic diversity of data centers that use real-time, synchronous data mirroring backup technologies. However, other alternatives beyond synchronous mirroring may be available to allow for greater distance separation.

- **Cold Site:** Cold sites are locations that are part of a longer-term recovery strategy. A cold site provides a backup location without equipment, but with power, air conditioning, heat, electrical, network and telephone wiring, and raised flooring. An example of a situation when a cold site can be a viable alternative is when the unit has recovered at another location, such as a hot site, but needs a longer term location while their data center is being rebuilt. Cold sites typically can take up to several weeks to activate. Institutions may rely on the services of a third party to provide cold site facilities or may house such a facility at another location, such as a branch or other operations center.

- **Tertiary Location**: Some units have identified the need to have a third location or a "backup to the backup." These tertiary locations provide an extra level of protection in the event neither the primary location nor the secondary location is available. Moreover, a tertiary location becomes the primary backup location in the event the institution has declared a disaster and is operating out of contingency or secondary site.

The university may enter into agreements, commonly referred to as "Reciprocal Agreements", with other institutions to provide equipment backup. This arrangement is usually made on a best-effort basis, whereby institution "A" promises to back up institution "B" as long as institution "A" has time available and vice versa. In the vast majority of cases, reciprocal agreements are unacceptable because the institution agreeing to provide backup has insufficient excess capacity to enable the affected institution to process its transactions in a timely manner. If an institution chooses to enter into a reciprocal agreement and can establish that such an

arrangement will provide an acceptable level of backup, the agencies expect such an agreement to be in writing and to obligate unit "A" to make available sufficient processing capacity and time. The agreement should also specify that each unit will be notified of equipment and software changes at the other units.

B. Backup Recovery Facilities

The recovery site should be tested at least annually and when equipment or application software is changed to ensure continued compatibility. Additionally, the recovery facility should exhibit a greater level of security protection than the primary operations site since the people and systems controlling access to the recovery site will not be as familiar with the relocated personnel using it. This security should include physical and logical access controls to the site as well as the computer systems. Further, the BCP and recovery procedures should be maintained at the alternative and off-site storage locations. Regardless of which recovery strategy is utilized, the recovery plan should address how any backlog of activity and/or lost transactions will be recovered. The plan should identify how transaction records will be brought current from the time of the disaster and the expected recovery time frames. Alternative workspace capacity is just as important as alternative data processing capabilities. Management should arrange for workspace facilities and equipment for employees to conduct ongoing business functions.

C. Geographic Diversity

When determining the physical location of an alternate processing site, management should consider geographic diversity. Units should consider the geographic scope of disruptions and the implications of a citywide disruption or even a regional disruption. The distance between primary and backup locations should consider recovery time objectives and business unit requirements. Locating a backup site too close to the primary site may not insulate it sufficiently from a regional disaster. Alternatively, locating the backup site too far away may make it difficult to relocate the staff necessary to operate the site. If relocation of staff is necessary to resume business operations at the alternate site, consideration should be given to their willingness to travel due to the events, the modes of transportation available, and if applicable, lodging and living expenses for employees that relocate. When evaluating the locations of alternate processing sites, it is also important to subject the secondary sites to a threat scenario analysis.

D. Backup and Storage Strategies

Institution management should base decisions on software and data file backup and on the criticality of the software and data files to the financial institution's operations. In establishing backup priorities, management should consider all types of information and the potential impact from loss of such files. This includes financial, regulatory, and administrative information, and operating, application, and security software. In assigning backup priority, management should perform a risk assessment that addresses whether:

- The loss of these files would significantly impair the unit's operations
- The files are being used to manage university assets or to make decisions regarding their use
- The files contain updated security and operating system configurations that would be necessary to resume operations in a secure manner
- The loss of the files would result in lost revenue, critical information, or vital research
- Any inaccuracy or data loss would result in significant impact on the institution (including reputation) or its customers

The frequency of file backup also depends on the criticality of the application and data. Critical data should be backed up using the multiple generation (i.e., "grandfather- father-son," etc.) method and rotated to an off-site

location at least daily. Online/real-time or high-volume systems may necessitate more aggressive backup methods such as mirroring or electronic vaulting at a separate processing facility to ensure appropriate backup of operations, as an alternative to backup tape storage. Backup tape storage remains a viable solution for many units. However, when a unit's primary backup media is tape storage, backup tapes should be sent to the off-site storage as soon as possible and should not reside at their original location overnight. Backup media, especially tapes, should be periodically tested to ensure they are still readable. Tapes repeatedly used or subjected to extreme variations in temperature or humidity may become unreadable, in whole or part, over time. Remote journaling is the process of recording transaction logs or journals at a remote location. These logs and journals are used to recover transaction and database changes since the most recent backup. Backup of operating system software and application programs must be performed whenever they are modified, updated, or changed.

E. Data File Backup

One of the most critical components of the backup process involves the university's data files, regardless of the platform on which the data is located. Units must be able to generate a current master file that reflects transactions up to the point in time of the disruption. Data files should be backed up both on-site and off-site to provide recovery capability. Retention of current data files, or older master files and the transaction files necessary to bring them current, is important so that processing can continue in the event of a disaster or other disruption. The creation and rotation of core processing data file backup should occur at least daily, more frequently if the volume of processing or online transaction activity warrants. Less critical data files may not need to off-site in a timely manner and not be returned until new backup files are off-site.

F. Software Backup

Software backup for all hardware platforms consists of three basic areas: operating system software, application software, and utility software. All software and related documentation should have adequate off-premises storage. Even when using a standard software package from one vendor, the software can vary from one location to another. Differences may include parameter settings and modifications, security profiles, reporting options, account information, or other options chosen by the institution during or subsequent to system implementation. Therefore, comprehensive backup of all critical software is essential. The operating system software should be backed up with at least two copies of the current version. One copy should be stored in the tape and disk library for immediate availability in the event the original is impaired; the other copy should be stored in a secure, off-premises location. Duplicate copies should be tested periodically and recreated whenever there is a change to the operating system. Application software, which includes both source (if the institution has it in its possession) and object versions of all application programs, should be maintained in the same manner as the operating system software. Backup copies of the programs should be updated as program changes are made. Given the increased reliance on the distributed processing environment, the importance of adequate backup resources and procedures for local area networks and wide area networks is important. Management should ensure that all appropriate programs and information are backed up. Depending on the size of the unit and the nature of anticipated risks and exposures, the time spent backing up data is minimal compared with the time and effort necessary for restoration. Files that can be backed up within a short period of time may require days, weeks, or months to recreate from hardcopy records, assuming hardcopy records are available. Comprehensive and clear procedures are necessary to recover critical networks and systems. Procedures should, at a minimum, include:

- Frequency of update and retention cycles for backup software and data

- Periodic review of software and hardware for compatibility with backup resources
- Periodic testing of backup procedures for effectiveness in restoring normal operations
- Guidelines for the labeling, listing, transportation, and storage of media
- Maintenance of data file listings, their contents, and locations
- Hardware, software, and network configuration documentation
- Controls to minimize the risks involved in the transfer of backup data, whether by electronic link or through the physical transportation of diskettes and tapes to and from the storage site
- Controls to ensure data integrity, client confidentiality, and the physical security of hardcopy output, media, and hardware

G. Off-site Storage

The off-site storage location should be environmentally controlled and secure with procedures for restricting physical access to authorized personnel. Moreover, the off- site premises should be an adequate distance from the computer operations location so that both locations will not be impacted by the same event. Beyond a copy of

the **BCP**, duplicate copies of all necessary procedures including end of day, end of month, end of quarter and procedures covering relatively rare and unique issues should be stored at the off-site locations. Another alternative to consider would be to place the critical information on a secure shared network drive with the data backed up during regularly scheduled network backup. However, this shared drive should be in a different physical location that would not be affected by the same disruption. Management needs to maintain a certain level of non-networked (e.g., hardcopy) material in the event that the network environment is not available for a period of time. Reserve supplies, such as forms, manuals, letterhead, etc., should also be maintained in appropriate quantities at an off-site location and management should maintain a current inventory of what is held in the reserve supply.

VII. Identification of Continuity Personnel

Based on the **BIA**, the **BCP** should assign responsibilities to management, specific personnel, teams, and service providers. The plan should identify integral personnel that are needed for successful implementation of the plan and develop contingencies to be implemented should those employees not be available. Additionally, vendor support should be identified. The **BCP** should address:

- How will decision making succession be determined in the event of the loss of management personnel?
- Who will be responsible for leading the various **BCP** Teams (e.g., Crisis/ Emergency, Recovery, Technology, Communications, Facilities, Human Resources, Business Units and Processes, Customer Service)?
- Who will be the primary contact with critical vendors, suppliers, and service providers?
- Who will be responsible for security (information and physical)?

Planning should also consider personnel resources necessary for decision making and staffing at alternate facilities under various scenarios. Key personnel should be identified to make decisions regarding efforts to provide for renovating or rebuilding the primary facility. This could require personnel beyond what is necessary for ongoing business continuity efforts.

Finally, the business continuity planning coordinator and/or planning committee should be given responsibility for regularly updating the BCP on at least an annual basis and after significant changes to the operations and environment.

VIII. Continuity Facilities

The **BCP** should address site relocation for short-, medium- and long-term disaster and disruption scenarios. Continuity planning for recovery facilities should consider location, size, capacity (computer and telecommunications), and required amenities necessary to recover the level of service required by the critical business functions. This includes planning for workspace, telephones, workstations, network connectivity, etc. When determining an alternate processing site, management should consider scalability in the event a long-term disaster becomes a reality. Additionally, during the recovery period, the BCP should be reassessed to determine if tertiary plans are warranted. Procedures to utilize at the recovery location should be developed. In addition, any files, input work, or specific forms, etc., needed at the backup site should be specified in the written plan. The plan should include logistical procedures for moving personnel to the recovery location in addition to steps to obtain the materials (media, documentation, supplies, etc.) from the off-site storage location. Plans for lodging, meals, and family considerations may be necessary.

In the event the Main Building is not available for an extended period of time, University Senior Leadership may be relocated to the Flawn Activity Center on campus. If the entire campus is impacted, other alternate locations may be considered to include the Pickle Research Center and the UT Golf Club.

IX. Communication

Communication is a critical aspect of a BCP and should include communication with emergency personnel, employees, directors, regulators, vendors/suppliers (detailed contact information), customers (notification procedures), and the media (designated media spokesperson). Alternate communication channels should be considered such as cellular telephones, pagers, satellite telephones, and Internet-based communications such as e-mail or instant messaging.

X. Other Considerations

Each unit is different and processes will vary. However, management should consider how to accomplish the following:

- Prevention, mitigation, and preparedness
- Reconciling recovery times with business unit requirements
- Disaster declaration and plan implementation processes
- Recovery progress reporting
- Training of personnel and testing of the plan