UCC 027412F
Rescinded by UHDPS

UNIVERSITY of HOUSTON
MANUAL OF ADMINISTRATIVE POLICIES AND PROCEDURES

SECTION: ~~General Information~~Public Safety **Number:** ~~01.03.03~~07.03.02
AREA: ~~University-wide Business Management~~Emergency Preparedness

SUBJECT: Business Continuity Planning

RECEIVED SEP 11 2012

I. PURPOSE AND SCOPE

Business continuity management is ensuring the continuity or uninterrupted provision of critical operations and services for University of Houston's Main Campus. Business continuity management is an ongoing process with several different but complementary elements, addressing the basic requirements of a business continuity plan, including the business impact analysis, security risk assessment, recovery strategy and a disaster recovery plan. The document addresses the basic requirements of a business continuity plan, including those parameters addressed in Texas Administrative Code, Chapter 202.74.~~This document establishes the framework for colleges, divisions and departments for the preparation, updating and monitoring of university business continuity plans. The document will address the basic requirements of a business continuity plan, including those addressed in Texas Administrative Code, Chapter 202.74. Elements of compliance will include the business impact analysis, security risk assessment, recovery strategy, and a disaster recovery plan.~~

It is the policy of University of Houston (UH) to maintain the capability to continue the primary missions of research, teaching, and public service despite potentially disruptive events. In order to achieve this capability, the UH Emergency Management Bureau under the Department of Public Safety directs a comprehensive disaster management program that incorporates elements of safety, security, emergency management, disaster preparedness, mutual aid agreements, administrative, recovery, and communication for all university entities. University departments, offices, and deans of schools must have full knowledge about Business Continuity Planning as they prepare for administrative and academic continuity during potentially disruptive events.

II. ~~POLICY~~DEFINITIONS

A. Business Continuity Planning: The advanced planning and preparations which are necessary to; identify the impact of potential losses; to formulate and implement viable recovery strategies; to develop recovery plan(s) which ensure continuity of organizational services in the event of an emergency or disaster; and to administer a comprehensive training, testing and maintenance program.

B. Business Continuity Program: 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 and recovery plans, and ensure continuity services through personnel training, plan testing and maintenance.

C. Business Impact Analysis: A management level analysis, which identifies the impacts of losing company resources. The Business Impact Analysis (BIA) measures the effect of resource loss and escalating losses over time, in order to provide senior management with reliable data upon which to base decisions on risk mitigation and continuity planning.

Each division of the University of Houston is tasked to assess their areas with regard to the possibility of an incident impacting their area by one of the above critical programs. They determine the strategy for recovery (accept the loss, mitigate toward recovery, or a partial recovery plan), the cost for that recovery and a detailed description for that decision.

1) Critical Space and Facilities are Unavailable
2) Critical Equipment is Damaged or Unavailable
3) Centrally Provided Power is Unavailable
4) Critical Communications are Unavailable
5) Central Information Systems are Not Functional
6) Local Information Systems are Not Functional
7) Critical Staff is Impacted and Unavailable
8) Critical Vendors are Unavailable.

D. Business Recovery Plan: A collection of procedures and information which are developed, compiled, and maintained in readiness for use in the event of an emergency or disaster.

E. Business Resumption: The process of planning for and/or implementing the restarting of defined business processes and operations following a disaster. This process commonly addresses the most critical business functions within BIA specified time frames.

F. Crisis Management: The overall coordination of an organization's response to a crisis, in an effective, timely manner, with the goal of avoiding or minimizing damage to the organization's profitability, reputation, and ability to operate.

G. Disaster Recovery Planning: The approved document by designated management that defines the resources, actions, tasks and data required to manage the technology recovery effort. Usually refers to the technology recovery effort.

H. University of Houston Emergency Management Bureau (UHEMB): University of Houston Emergency Management Bureau is responsible for maintaining and updating plans and policies, training, facilitating exercises and evaluating completed elements.

I. UH PIER System: The web application used to collect and preserve data for business continuity planning.

J. Security Risk Assessment – The administration will assess the Business Impact Analysis to determine the areas needing preventative measures. These preventative measures will be implemented in a timely manner to avoid additional risk to the university. A review will be conducted annually.

K. Recovery Strategy - To ensure a safe and economical recovery, administration will be presented with recovery alternatives and estimates for the university with regard to implementation. The implemented plans will be tested formally and informally on an annual basis.

L. Disaster Recovery Plan – University Information Technology (UIT) will ensure that a proper Disaster Recovery Plan has been implemented and tested annually.

III. POLICY

A. Rationale - Business continuity plans play a vital role in the UH all-hazards disaster preparedness approach. It is through business continuity management and planning that UH mission-critical entities develop the necessary understanding of their core business processes and interdependencies required for effective prevention of and response to operational disruptions.

B. Scope - This policy applies to UH mission-critical departments, offices, centers, services, etc., as defined by the Emergency Management Team (e.g., Executive Vice President for Administration and Finance, Executive Associate Vice President for Academic Affairs, Associate Vice President for Student Affairs, Associate Vice President for University Relations, Assistant Vice President for Public Safety and Security, Emergency Management Director, Chief Information Officer, Executive Director of Facilities, Student Government Association President, Staff Council President, Faculty Senate President, Executive Director for Residential Life and Housing, and Executive Director for Research Services) and located in UH-owned properties, jointly-owned facilities, and UH-leased spaces that are under the control of UH operations and staff. This policy applies to missioncritical UH entities under contractual obligation with affiliated institutions or in any location where a UH entity has a contractual obligation to fulfill university business.

C. Forms and Tools/Online Processes

1. To assist UH units with completing a business impact analysis and a business continuity plan, the UHEMB utilizes the UH BCP program. The application resides on a UH PIER Systems server and is secured by the network. All users will be able to access their continuity plans through the UH PIER System network.

2. Access to the UH BCP system requires the user to request authorization from the UHEMB. The employees' password will be used to log into the UH BCP PIER System. The web site location is http://www.piersystem.com.

D. Responsibilities

1. Business continuity management responsibilities apply to all units which are mission-critical to the campus, organizational units, and departments.

a. All University mission-critical units are required to have a completed plan that includes procedures for operational continuity to ensure UH is able to provide critical services.

b. **Administrative** units include both centralized as well as distributed organizations, departments, and divisions that support the UH research, academic, and public service functions.

c. **Academic** units include all colleges, schools, departments, research programs, programs and centers that serve UH's primary mission of teaching/instruction, research, and public service activities.

2. UH Emergency Management Bureau (UHEMB)

a. The UHEMB provides expertise and oversight for the development and maintenance of the UH business continuity program and creates a back-up centralized location for documentation of all business continuity plans, training, and exercises. All UH business continuity plans will be created, stored, and updated utilizing the UH PIER System.

Note: The Office of University Information Technology is the only department that will be the exception to the rule. UIT will also have a plan stored in another location. Their plan will be integrated into the UH PIER System process as they are a critical function to all departments.

The primary location of plans and documentation is in the respective units. Business continuity management training, orientation, and support is available to UH units annually.

b. UHEMB has the primary responsibility of coordinating the identification of risks and to assist in determining what impact these risks have to overall business operations. The UHEMB develops and maintains an overarching business continuity plan based on these identified risks and documents recovery strategies and procedures that are reviewed, approved, and updated on an annual basis. The determination of risk, strategies and procedures will be based on identifying critical functions necessary to continuing University service delivery.

c. The Office of University Information Technology and the UHEMB ensure that the business impact analysis coordinates with the business continuity tool with regards to terminology of functional delays (i.e., critical, essential, delayed, and suspended).

d. The UHEMB is responsible for the development of the over-arching business continuity plan which contains the following elements:

- Authority
- Purpose and Scope
- Risk Assessment
- Business Impact Analysis
- Explanation of Terms
- Situation and Assumptions
- Concept of Operations
- Organization and Assignment of Responsibilities
- Direction and Control

- Readiness Levels
- Administration and Support
- Plan Development and Maintenance
- Support Documentation

IV. PROCEDURE

A. Each Vice President/Provost, Dean, Director, Department Chair, or Supervisor is required to assume responsibility for the operational continuity in their respective units. Procedures of the development of a BCP include but are not limited to:

1. Identify and prioritize critical business processes.
2. Assess the potential impact of various types of events/disasters on a regular basis.
3. Define departmental responsibilities and emergency arrangements.
4. Document all procedures and responsibilities.
5. Communicate business continuity and recovery plans to all necessary individuals.
6. Participate in an annual business continuity exercise of their continuity and recovery plans.
7. Identify gaps, best practices and updates within their plan after an exercise and share findings with UHEMB for implementation into the After Action Report (ARR). Findings reported in the AAR should have a timeline for correction/implementation and identification of who is responsible for the corrective action.
8. Direct an annual review of business continuity and recovery plans to ensure they are complete and up-to-date.

B. UHEMB assists and consults with departments on campus to ensure that department business continuity plans are completed. UHEMB provides guidance, direction and support as part of a cooperative effort for planning.

C. All planning will rely on the input from the staff and faculty of each department to ensure a proper level of consideration is given to all aspects of those unit's critical operations. The actual plan will be written by a member of the department as designated by the unit leader.

~~The Administration and Finance Division is charged with the following roles and responsibilities related to the preparation, updating and monitoring of university business continuity plans.~~

~~1. Providing a business continuity plan template to use when creating business continuity plans which can be found at www.piersystem.com, Business Continuity Plan section.~~

~~2. Enacting an annual monitoring mechanism to ensure timely completion of updates to university business continuity plans.~~

3. Providing an annual status report to be approved by the President or designee on the implementation of business continuity plans.

B. The divisions are responsible for collecting the plans within their area and completing an executive summary that highlights the key areas of risk within their division, and how these risks are addressed in the business continuity plan. These summaries should be included in the annual status report that is presented in the annual report provided to the President or designee.

C. The Division of Administration and Finance is responsible for ensuring that the following are in accordance with the Texas Administrative Code, Chapter 202.74:

1. Business Impact Analysis - This analysis will include the potential impact of loss of business to the campus community. The analysis will be reviewed and evaluated each year along with the business continuity plans. A report will be prepared and posted annually.

2. Security Risk Assessment – The administration will assess the Business Impact Analysis to determine the areas needing preventative measures. These preventative measures will be implemented in a timely manner to avoid additional risk to the university.

3. Recovery Strategy - To ensure a safe and economical recovery, administration will be presented with recovery alternatives and estimates for the university with regard to implementation. The implemented plans will be tested formally and informally on an annual basis.

4. Disaster Recovery Plan – Information Technology will ensure that a proper Disaster Recovery Plan has been implemented and tested.

IIIV. REVIEW AND RESPONSIBILITY

Responsible Party: Assistant Vice President for Public Safety and Security

Review: Every three years, on or before September 1March 31

IVVI. APPROVAL

Carl P. Carlucci
Executive Vice President for Administration and Finance

Renu Khator
President

Date of President's Approval: December 1, 2010

VII. REFERENCES

A. *Texas Administrative Code §202.70:*

The Code establishes the Security Standards Policy and states that it is the policy of the State of Texas that Information Resources residing in the various agencies of state government are strategic and vital assets belonging to the people of Texas. Assets of the UH System must be available and protected commensurate with their value and must be administered in conformance with federal and state law and UH System Regents' Rules and Regulations. Information resources are available when needed. Continuity of information resources supporting critical governmental services are ensured in the event of a disaster or business disruption.

B. *Texas Administrative Code §202.74:*

Business Continuity Planning, part of the Security Standards for Institutions of Higher Education issued by the Department of Information Resources (DIR), covers all business functions of an institution of higher education and it is a business management responsibility. Institutions of higher education maintain written Business Continuity Plans so that the effects of a disaster will be minimized, and the institution of higher education will be able to either maintain or quickly resume mission-critical functions.

The institution of higher education head or his or her designated representative(s) approve the Plan. The Plan is distributed to key personnel and a copy is stored offsite. Elements of the department/unit plan should include the following:

- Departmental Information
- Critical Functions
- Information Technology
- Faculty Preparedness if applicable
- Key Resources
- Action Items
- List of Key Documents if applicable

REVISION LOG

Revision Number	Approved Date	Description of Changes
1	11/29/2000	Initial edition
2	04/15/2003	Addendums were removed from policy and inserted as web links where appropriate. Applied revised MAPP template to meet current documentation standards
3	06/01/2008	Contents rewritten to reflect current process
4	10/07/2010	In Section IX.B, the applicable authority cycle for notification changed from Treasurer and Associate Vice Chancellor for Finance to Treasurer and Executive Vice Chancellor for Administration and Finance

Revision Number	Approved Date	Description of Changes
5	TBD	Added revised MAPP template and new Revision Log. Renumbered the MAPP from 01.03.03 to 07.03.02. Rewrote procedure to reflect current operating requirements, adding definitions and references. Changed the review period from every three years on or before September 1st to every three years on or before March 31st