

UTMB HANDBOOK OF OPERATING PROCEDURES

Section 2	General Administrative Policies and Services	12/21/07 -Originated
Subject 2.1	General Institutional Policies	-Reviewed w/ changes
		-Reviewed w/o changes
Policy 2.1.5	Business Continuity Planning	Information Services -Author

Business Continuity Planning

Definitions

Business Continuity Coordinator – Person assigned overall responsibility for coordinating a business unit’s Business Continuity program.

Business Continuity Plan – The documentation of a predetermined set of instructions or procedures that describe how an organizations business functions will be sustained during and after a significant disruption.

Business Continuity Planning (BCP) – The process of developing advance arrangements and procedures that enables UTMB to respond to an interruption in such a manner that critical business functions continue with planned levels of interruption or essential change. In simpler terms, BCP is the strategic act of planning a method to prevent, if possible, and to minimize and manage the consequences of an event that interrupts critical business processes.

Business Impact Analysis (BIA) – Involves the identification of critical business functions and workflows, determining the qualitative and quantitative impact of a disruption, and prioritizing recovery objectives.

Emergency Management Plan – The written document describing the process to be implement for managing the consequences of any emergency that could disrupt the organizations’ ability to provide patient care, education, research and other services provided by UTMB.

The plan identifies specific procedures that describe mitigation, preparedness, response, and recovery strategies, actions, and responsibilities.

Information Technology Backup/Failover Plan – Procedures/processes to create and maintain retrievable, exact copies of critical data/information in expectation of a foreseeable business process disruption and in anticipation of unexpected disruption.

Information Technology Disaster Recovery Plan – A Disaster Recovery Plan is the process of recovering Information Technology (IT) systems in the event of a disruption or disaster, including procedures to restore any loss of data.

UTMB HANDBOOK OF OPERATING PROCEDURES

Section 2	General Administrative Policies and Services	12/21/07 -Originated
Subject 2.1	General Institutional Policies	-Reviewed w/ changes
Policy 2.1.5	Business Continuity Planning	-Reviewed w/o changes Information Services -Author

**Definitions,
continued**

Mission Critical Activities – (1) Significant operational and/or business support activities (either provided internally or externally) without which the business or government agency would be unable to achieve its objective(s). (2) Any supported health care delivery activity, which, if interrupted, would result in significant degradation of the health or life of a patient.

Mitigation Activities – Those activities an organization undertakes in attempting to avoid or lessen the severity and impact of a potential emergency.

Risk Assessment (Analysis) - A systematic and analytical approach that identifies and assesses risk to business processes and provides recommendations to avoid or reduce the risk.

Policy

Business Resilience and Continuity Planning (BRCP) is a crucial part of preparing for unforeseen events such as natural and man made disasters, system outages, malfunctions, personnel shortages, etc. It helps departments quickly recover so that essential services can be provided under adverse conditions. This is not the same as a disaster recovery plan which details information technology or a emergency management plan which details emergency preparedness.

All UTMB components must have a business continuity management plan and ensure that all employees are familiar with their individual roles and responsibilities. It is imperative that UTMB is able to resume operations within a reasonable period of time following any disruption to service.

Process

Executive management will assign Business Continuity Coordinators for their departments and/or services within their entity. The coordinator shall ensure that Business Continuity Plans are documented, tested, implemented, maintained, and reviewed annually to ensure they remain relevant and complete.

Each plan will contain the following:

- A business impact analysis to identify and prioritize critical business processes.
 - A risk analysis of critical business processes that describes the events that would disrupt these processes.
 - Identification procedures for downtime, workaround and recovery
-

UTMB HANDBOOK OF OPERATING PROCEDURES

Section 2	General Administrative Policies and Services	12/21/07 -Originated
Subject 2.1	General Institutional Policies	-Reviewed w/ changes -Reviewed w/o changes
Policy 2.1.5	Business Continuity Planning	Information Services -Author

Process, continued

-
- for those mission critical activities in the event of a disruption.
- Disaster recovery procedures and/or downtime procedures for information technology and day to day operations.
 - Disaster recovery procedures for non-electronic, paper documentation kept by department for restoration needs.
 - Location of alternate facilities and a description of staffing and supplies needed at the alternate facility.
 - Identification of critical equipment and identification of process for obtaining the alternate or replacement equipment.
 - Normal and emergency contact information for key staff.
 - Normal, emergency and backup information for critical vendors.
 - Identification of critical supplies and backup process for purchasing critical supplies.
 - All personnel must be familiar with the contents of the plan for their services and processes, and follow its guidance, as appropriate, when there is a disruption.
 - Plans will be tested annually.
 - Plans will be reviewed and updated annually or as critical processes change. These changes will be documented within the plan.

References

-
- Texas Administrative Code: Information Security Standards – Rule §202.74 Business Continuity Planning
 - HIPAA: Security Standards - §164.308 Administrative Safeguards
 - Joint Commission: Management of the Environment of Care (EC 4.10., EC 4.20) and Management of Information (IM 2.30)
-