Section	2	General Administrative Policies and Services	12/21/07 -Originated
Subject	2.1	General Institutional Policies	07/12/12 -Reviewed w/ changes -Reviewed w/o changes
Policy	**2.1.5**	**Business Continuity Planning**	08/06/12 - Effective Information Services -Author

Business Continuity Planning

Definitions

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, identifies critical information resources, determining the qualitative and quantitative impact of a disruption, and prioritizing recovery objectives.

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 a life safety event.

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

To ensure that UTMB is able to resume operations within a reasonable period of time following any adverse event or operational disruption, all departments and business units will have a business continuity plan (BCP). This plan may be department specific or may be part of a larger entity-level plan.

For mission critical activities, particularly those relying heavily on information technology, the BCP must contain both a business impact analysis and a risk assessment.

Policy, continued

BCP's will be updated annually or as critical processes change and will be approved by appropriate entity management. Executive Leadership will have final accountability for entity plans and stewardship of resources. All BCP's will be stored in a central repository to ensure they are available to institutional leadership during an event.

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)