| Institutional Handbook of Operating Procedures<br>Policy 02.01.04 | |
|---|---|
| Section: General Administration | Responsible Vice President: VP Information Services & CIO |
| Subject: General | Responsible Entity: Information Services & Facilities Risk Management |

## I. Title

*Institutional Resilience Program: Integration of Emergency Management, Business Continuity Management and Disaster Recovery Programs*

## II. Purpose

The primary purpose of the Institutional Resilience Policy is to provide definitive oversight and guidance for UTMB Health's incident planning and response functions; and to provide common response criteria and terminology. The University of Texas Medical Branch (UTMB) institutional preparedness and resilience programs comprise three distinct, yet complementary, risk management disciplines encompassing business continuity, disaster recovery, and emergency management. Together these functions provide the institution the ability to address the potential impacts of: emergency incidents and business interruptions; respond effectively when an incident occurs; continue to deliver a minimum acceptable level of service during and in the immediate aftermath of an incident; and subsequently return conditions to a normal level of operations that is acceptable to the institution.

While the primary focus of business continuity is the reliability of critical business services, it also includes disaster recovery, which addresses resumption of the supporting information technology. Conversely, the focus of emergency management concerns the protection of life and UTMB facilities.

Historically, organizations addressed business continuity, disaster recovery, and emergency management independently. However, these three planning and response functions have clear interdependencies that benefit from a comprehensive resilience program integrating people, processes, procedures, information technology, communications, facilities, and equipment within a common organizational structure.

This integrated approach, an emerging trend, leverages the perspectives, knowledge, and capabilities of related functions within the institution. In addition, unified processes can help avoid segregating risks, better ensure sustainable operations in the event of an incident, and satisfies all applicable compliance requirements., More importantly, the reason to adequately plan and prepare is the realistic possibility that the institution could quickly find itself responding to a major incident with minimal notice. The resilience program incorporates routine maintenance, formal review, feedback, lessons learned, and continuous process improvement to ensure response readiness in adherence with program requirements.

## III. Policy

UTMB will use an integrated approach to Emergency Management, Business Continuity Management, and Disaster Recovery Planning as part of its overall institutional Resilience Program. The Emergency Management component will address the four phases of emergency management:

- Preparedness
- Mitigation
- Response
- Recovery

The Business Continuity Management component will address the continuity of critical business functions. Planning will address critical business functions at the institutional level as well as at departmental, business unit, or campus level.

Disaster Recovery plans will address the Information Technologies that support critical business functions.

Program Maturity: UTMB should use a framework such as the Carnegie Mellon Resilience Management Model to continuously improve its Resilience Program components. Processes should be defined, quantitatively managed, and optimized.

Crisis Communications and Program Awareness: Program Directors responsible for planning under this policy will work with UTMB Marketing and Communications - UTMB's Public Information Officer (PIO) role – to increase awareness of resilience plans among UTMB employees; and to improve mass or targeted notification of emergency incidents, and Crisis Communications capabilities.

Incident Prevention: Program Directors responsible for planning under this policy will work with UT Police and UTMB Information Security to improve information sharing and other activities to help prevent emergency incidents from occurring.

## IV. Procedures

**A.** Annual Program Proposal: A Resilience Program Proposal will be developed each calendar year and presented to the UTMB Institutional Safety and Security Executive Committee for review and approval. Note: The Resilience Program will use a Calendar Year in lieu of the Fiscal Year for program management and planning efforts. Since hurricane damage is likely to remain the highest priority risk for the foreseeable future, the use of a calendar year will allow the entire annual hurricane season to be included in one program year, and will allow sufficient time for analysis of program results and formulation of an Annual Program Proposal in time for the next calendar year.

**1.** The Annual Program Proposal should include:

- Updates on relevant legislation, regulations, accreditation standards, best practices or benchmarks
- Updated Hazard Vulnerability Analysis (Risk Assessment)
- Proposed prioritized list of risks facing UTMB
- Update to the scope or body of the Emergency Operations Plan / Business Continuity Plan / Disaster Recovery Plan
- Priorities for training and staff/student awareness (as appropriate)
- Proposed exercises for the program year
- Analysis of program effectiveness for exercises and real incidents
- Root Cause Analyses for major (real) incidents
- Identification of Program Improvements
- Retesting and validation of any program/plan changes

**2.** The Annual Program Proposal should be presented to the Institutional Safety and Security Executive Committee for approval before the end of the first quarter of the calendar year.

**B.** Annual Business Continuity Review: UTMB will follow the Disaster Recovery Institute International (DRII) Business Continuity Professional Practices in conducting its annual review of Business Continuity Plans. The Business Continuity Review will be completed by June 1 each year. At a minimum the review will include:

- An updated risk assessment
- A Business Impact Analysis (BIA) to identify critical business functions. For each critical business function identified, the BIA will include a Recovery Time Objective (RTO) (see Definitions below); Recovery Point Objectives (RPO) for information systems; Continuity Strategies to assure that RTOs and RPOs can be met for the highest priority risks
- The BIA may include a Maximum Tolerable Period of Disruption (at the discretion of the Business Continuity Coordinator)
- A Continuity Exercise (that may be combined with an Emergency Management Recovery Exercise and/or an information technology Disaster Recovery Exercise)

**C.** Disaster Recovery will be incorporated into the Annual Business Continuity Review. Disaster Recovery Plan updates and exercises will be completed prior to June 1 for each year. The number of critical information system DR plans tested within the year will be reported as a percentage of the total number of critical systems – to the Institutional Safety and Security Executive Committee as part of the annual review process.

## V. Definitions

Business Continuity Management: A management process that identifies risk, threats and vulnerabilities that could impact an entity's **continued operations** and provides a framework for building organizational resilience and the capability for an effective response (DRII)
https://drii.org/certification/professionalprac.php?lang=EN

Business Continuity Strategies: The data that was collected during the BIA and Risk Evaluation is used in this professional practice to identify available continuity and recovery strategies for the entity's operations and technology. Recommended strategies must be approved and funded and must meet both the recovery time and recovery point objectives identified in the BIA. A cost benefit analysis is performed on the recommended strategies to align the cost of implementing the strategy against the assets at risk. https://drii.org/certification/professionalprac.php?lang=EN

Business Impact Analysis: Identification of the likely and potential impacts from events on the entity or its processes and the criteria that will be used to quantify and qualify such impacts. The criteria to measure and assess the financial, customer, regulatory and/or reputational impacts must be defined and accepted and then used consistently throughout the entity to define the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for each of the entity's processes. The result of this analysis is to identify time sensitive processes and the requirements to recover them in the timeframe that is acceptable to the entity. (DRII) https://drii.org/certification/professionalprac.php?lang=EN
A Business impact analysis (BIA) differentiates critical (urgent) and non-critical (non-urgent) organization functions/activities. Critical functions are those whose disruption is regarded as unacceptable. Perceptions of acceptability are affected by the cost of recovery solutions.

Crisis Communications: Framework to identify, develop, communicate, and exercise a crisis communications plan. A Crisis Communications plan addresses the need for effective and timely communication between the entity and all the stakeholders impacted or involved during the response and recovery efforts (DRII) https://drii.org/certification/professionalprac.php?lang=EN

Disaster Recovery: (DR) involves a set of policies and procedures to enable the recovery or continuation of vital technology infrastructure and systems following a natural or human-induced disaster. Disaster recovery focuses on the IT or technology systems supporting critical business functions, as opposed to business continuity, which involves keeping all essential aspects of a business functioning despite significant disruptive events. Disaster recovery is therefore a subset of business continuity

Emergency Management: The development and implementation of UTMB's plan for response to emergency situations that may impact safety of the entity's employees, visitors or other assets. The emergency response plan documents how the entity will respond to emergencies in a coordinated, timely and effective manner to address life safety and stabilization of emergency situations until the arrival of trained or external first responders (DRII - https://drii.org/certification/professionalprac.php?lang=EN) Emergency Management (FEMA)

Emergency Management – Preparedness: Actions that involve a combination of planning, resources, training, exercising, and organizing to build, sustain, and improve operational capabilities. Preparedness is the process of identifying the personnel, training, and equipment needed for a wide range of potential incidents, and developing jurisdiction-specific plans for delivering capabilities when needed for an incident. http://www.fema.gov/media-library-data/20130726-1828-25045-0014/cpg_101_comprehensive_preparedness_guide_developing_and_maintaining_emergency_operations_plans_2010.pdf

Emergency Management – Mitigation: Activities providing a critical foundation in the effort to reduce the loss of life and property from natural and/or human-caused disasters by avoiding or lessening the impact of a disaster and providing value to the public by creating safer communities. Mitigation seeks to fix the cycle of disaster damage, reconstruction, and repeated damage. These activities or actions, in most cases, will have a long-term sustained effect. http://www.fema.gov/media-library-data/20130726-1828-25045-0014/cpg_101_comprehensive_preparedness_guide_developing_and_maintaining_emergency_operations_plans_2010.pdf

Emergency Management – Response: Immediate actions to save and sustain lives, protect property and the environment, and meet basic human needs. Response also includes the execution of plans and actions to support short-term recovery. http://www.fema.gov/media-library-data/20130726-1828-25045-0014/cpg_101_comprehensive_preparedness_guide_developing_and_maintaining_emergency_operations_plans_2010.pdf

Emergency Management – Recovery: The development, coordination, and execution of service and site restoration plans; the reconstitution of operations and services; evaluation of the incident to identify lessons learned; post-incident reporting; and development of initiatives to mitigate the effects of future incidents. http://www.fema.gov/media-library-data/20130726-1828-25045-0014/cpg_101_comprehensive_preparedness_guide_developing_and_maintaining_emergency_operations_plans_2010.pdf

Emergency Management – Prevention: Actions to avoid an incident or to intervene to stop an incident from occurring. Prevention involves actions to protect lives and property. It involves applying intelligence and other information to a range of activities that may include such countermeasures as deterrence operations; heightened inspections; improved surveillance and security operations; investigations to determine the full nature and source of the threat; public health and agricultural surveillance and testing processes; immunizations, isolation, or quarantine; and, as appropriate, specific law enforcement operations aimed at deterring, preempting, interdicting, or disrupting illegal activity

and apprehending potential perpetrators and bringing them to justice. http://www.fema.gov/media-library-data/20130726-1828-25045-0014/cpg_101_comprehensive_preparedness_guide_developing_and_maintaining_emergency_operations_plans_2010.pdf

Enterprise Risk Management (ERM): In business includes the methods and processes used by organizations to manage risks and seize opportunities related to the achievement of their objectives. ERM provides a framework for risk management, which typically involves identifying particular events or circumstances relevant to the organization's objectives (risks and opportunities), assessing them in terms of likelihood and magnitude of impact, determining a response strategy, and monitoring progress. By identifying and proactively addressing risks and opportunities, business enterprises protect and create value for their stakeholders, including owners, employees, customers, regulators, and society overall

Hazard Vulnerability Analysis: (Used interchangeably with Risk Assessment) Hospitals are required to conduct and annually review their Hazard Vulnerability Analysis (HVA). The HVA provides a systematic approach to recognizing hazards that may affect demand for the hospitals services or its ability to provide those services. The risks associated with each hazard are analyzed to prioritize planning, mitigation, response and recovery activities. The HVA serves as a needs assessment for the Emergency Management program. This process should involve community partners and be communicated to community emergency response agencies. http://www.calhospitalprepare.org/hazard-vulnerability-analysis

Maximum Tolerable Period of Disruption**:** Is the maximum amount of time that an enterprise's key products or services can be unavailable or undeliverable after an event that causes disruption to operations, before its stakeholders perceive unacceptable consequences. MTPD may be included in the Business Impact Analysis.

National Response Framework: The Response Framework covers the capabilities necessary to save lives, protect property and the environment, and meet basic human needs after an incident has occurred. Response activities take place immediately before, during, and in the first few days after a major or catastrophic disaster. https://www.fema.gov/media-library-data/1466014682982-9bcf8245ba4c60c120aa915abe74e15d/National_Response_Framework3rd.pdf

National Disaster Recovery Framework: A guide that enables effective recovery support to disaster-impacted States, Tribes, Territorial and local jurisdictions. It provides a flexible structure that enables disaster recovery managers to operate in a unified and collaborative manner. It also focuses on how best to restore, redevelop and revitalize the health, social, economic, natural and environmental fabric of the community and build a more resilient Nation. http://www.fema.gov/national-disaster-recovery-framework

Risk Assessment: (Used Interchangeably with Hazard Vulnerability Analysis) A risk assessment is the determination of quantitative or qualitative value of risk related to a concrete situation and a recognized threat (also called hazard). *Quantitative risk assessment* requires calculations of two components of risk *(R)*, the magnitude of the potential loss *(L)*, and the probability *(p)* that the loss will occur.

Recovery Point Objective: Is the maximum tolerable period in which data might be lost from an IT service due to a major incident. UTMB uses a Tiered System to categorize the RPO for critical information systems. As part of the Business Impact Analysis process, departments should list the critical information systems used and confirm that those systems are on the appropriate Tier level for restoration.

Recovery Time Objective: Is the targeted duration of time and a service level within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity.

Resilience: The adaptive capacity of an organization in a complex and changing environment. The ability of an organization to resist being affected by an event or the ability to return to an acceptable level of performance in an acceptable period of time after being affected by an event. The capability of a system to maintain its functions and structure in the face of internal and external change and to degrade gracefully when it must.
http://www.ndsu.edu/fileadmin/emgt/ASIS_SPC.1-2009_Item_No._1842.pdf

Resilience Management Model: The Resilience Management Model (RMM) is an innovative and transformative way to approach the challenge of managing operational resilience in complex, risk-evolving environments. It is the result of research into the ways that organizations manage the security and survivability of the assets that ensure mission success. It incorporates concepts from an established process improvement community to allow organizations to holistically mature their security, business continuity, and IT operations management capabilities and improve predictability and success in sustaining operations whenever disruption occurs. http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=9479

## VI. Relevant Federal and State Statutes

Health Insurance Portability and Accountability Act's (HIPAA) Security Rule

Texas Education Code 51.217 Multihazard Emergency Operations Plan; Safety and Security Audit

Texas Administrative Code (TAC), Part 10, Chapter 202: Information Security Standards

## VII. Relevant System Policies and Procedures

The University of Texas System Emergency Management Policy (UTS172)

Information Resources Use and Security Policy (UTS165)

## VIII. Related UTMB Policies and Procedures

IHOP - 02.01.05 - Business Continuity Planning

## IX. Additional References

Developing and Maintaining Emergency Operations Plans

DRII Professional Practices

Organizational Resilience Management Standard SPC.1-2009

National Incident Management System (NIMS) and Hospital Incident Command System (HICS) incident management standards

Joint Commission on Accreditation of Healthcare Organizations (TJC) standards (e.g., Emergency Management, Environment of Care, and Information Management)

National Fire Protection Association (NFPA)1600: Standard on Disaster/Emergency Management and Business Continuity as adopted by the United States Department of Homeland Security's (voluntary) Private Sector Preparedness Program (PS-Prep)

Presidential Policy Directive Eight (PPD-8)

National Preparedness Goal

Texas State Office of Risk Management's Texas Continuity Policy and minimum business continuity requirements crosswalk (i.e., incorporates Texas legislative requirements, guidance from the Federal Emergency Management Agency, best practices, and other applicable standards)

## X. Dates Approved or Amended

| *Originated:* 4/20/2015 | |
|---|---|
| *Reviewed with Changes* | *Reviewed without Changes* |
| | 06/04/2018 |