Policy Title: ITS Disaster Recovery Policy	**Policy Number:**
Date Issued: June 10, 2020	**Responsible Executive: Vice President of Information Technology**
Date Last Revised: June 10, 2020	**Responsible Office: Information Technology Services**

ITS Disaster Recovery Policy

Policy Statement

This policy provides a framework for the management, development, implementation, and maintenance of the disaster recovery framework for the data/technology services managed by Baylor Information Technology Services ("ITS").

The primary objectives of the disaster recovery framework are to:

- Establish operational control over the disaster
- Communicate with relevant parties about the disaster
- Activate a specific recovery plan

Reason for the Policy

While Baylor University ("Baylor" or the "University") has taken measures to prevent disasters, emerging risks continue to threaten university data/technology capabilities. This framework has been created to address a non-routine event that could significantly impair Baylor's data/technology capabilities.

Individuals/Entities Affected by this Policy

Baylor data/technology services are used by members of the University community, including faculty, staff, students, and affiliates. A disaster could impair the ability to access Baylor data/technology resources.

Exclusions

NONE

Related Documents and Forms

University Policies and Documents

BU-PP 025 – Technology Use Policy
BU-PP 029 – Handling of Confidential Information
Technology Incident Reporting Policy
Privacy Policy

Other Documents

- Family Educational Rights and Privacy Act (FERPA) 20 USC §1232g and 34 CFR Part 99
- Health Insurance Portability and Accountability Act (HIPAA) 42 USC §300gg and 1320d; 29 USC §1181 and 45 CFR Parts 146160, 162 and 164
- Gramm-Leach-Bliley Act 15 USC §6801 et seq and 16 CFR Part 313 et seq
- Fair and Accurate Credit Transactions Act (Red Flags Rule) 15 USC §1601 et seq
- Protection of Human Subjects Regulations ("Common Rule") 45 CFR Part 46
- Texas Business and Commerce Code privacy laws Tex. Bus. & Comm. Code Chapters 501-503
- Privacy Act of 1974 5 USC §552a et seq
- Texas Public Information Act Texas Government Code Chapter 552
- Children's Online Privacy Protection Act (COPPA) 15 USC §6501 et seq and 16 CFR Part 312
- European Union General Data Protection Regulation (EU GDPR) EU 2016/679

Definitions

These definitions apply to terms as they are used in this policy.

Disaster	Disaster for the purpose of this framework is a non-routine event that significantly impairs Baylor's data/technology capabilities.
Disaster Recovery (DR)	Disaster Recovery is ITS's response to minimize the disruption of operations and expedite the recovery of data/technology.
Business Continuity	Business Continuity addresses the strategy to continue business operations at the University without the use of technology/data. DR is a part of the Business Continuity plan.
University Community	Faculty, staff, students, and affiliates, and authorized visitors, guests, and others for whom University technology resources or access to the network have been granted.
Baylor University Technology Systems	Including, but not limited to: computers, computer accounts, internet access, printers, networks, network devices, software, electronic mail ("e-mail"), Web home pages, video systems, telephones, mobile devices, telephone long distance and voice mail accounts that are provided for the use of University community in support of the programs of the University
ITS	Information Technology Services

Contacts

Subject	Contact	Telephone	Office email/web site
Policy Management	Information Technology Services	254-710-2711	https://www.baylor.edu/its/
Disaster Coordination	Department of Public Safety	254-710-2211	https://www.baylor.edu/dps/

Responsibilities

Chief Information Officer or Designee	Has the ability to declare a disaster involving Baylor technology systems Responsible for ensuring the policy remains current and for managing the application of the policy
Baylor Senior Management & ITS Senior Management	Has the ability to declare a disaster involving Baylor technology systems
ITS Emergency Response Team	The response team assembled by senior ITS management with the talents and skills necessary to facilitate the University's response to a particular crisis.
System Owners of non-ITS Managed Systems	Individuals and departments that own non-ITS managed systems are responsible for the backup/recovery of those systems.
Baylor Marketing and Communications	Baylor Marketing and Communications is the lead to disseminate communications regarding a disaster.

Principles

Assumptions

The disaster response and recovery plan is based on the following assumptions:

- The safety of students, faculty, and staff is the primary concern of the University.
- Once a disaster has been declared, appropriate priority and support will be given during the recovery effort.
- A disaster may range significantly in regards to scope and impact. This framework is put into place to address any disaster, from a significant outage to a major loss. Not every section of this policy will apply to every disaster, but it should serve as a framework of possible options given the impairment to University data/technology.
- ITS provides centralized backups for faculty and staff primary computers, as well as University systems. System administrators need to ensure systems are backed up if they are not part of the ITS centralized backup process.
- During the recovery period, several departments and offices on campus may need to modify their current operations and plan for the unavailability of data/technology capabilities. The business continuity plan to accommodate such disruptions is not part of the ITS disaster recovery plan. Additionally, ITS's primary focus will be on the recovery effort for University-wide data/technology. Departments and offices should have plans in place to modify their operations during a disaster.
- While recovering data/technology, the University still has obligations to be compliant with data protection requirements during the recovery process.
- There are several systems on campus that are not supported by ITS. ITS will assist to the extent possible, but it is the responsibility of the systems owners to recover their data/technology on non-ITS managed systems.

Declaring a Disaster

Senior University Management and/or available senior ITS leadership team members will consult and determine whether a disaster should be declared based on an initial assessment of a prolonged unplanned disruption of normal operations.

Additionally, University Compliance and Risk Services may need to be contacted when a disaster is declared, so as to put our insurance carriers on notice of the event. The policies may provide immediate assistance or possible future reparations for losses incurred.

Once a disaster is declared, ITS senior management will update the appropriate senior management personnel. ITS senior management will establish a schedule of communication to provide updates regarding the recovery.

Emergency Response

ITS Recovery Team

ITS senior management will assemble key members of the ITS leadership team and other staff members who will provide the technical and management skills necessary to achieve a smooth technology and business recovery.

During the disaster, staff members' duties may be reassigned to the recovery team efforts based on their skillsets. Depending on the timing and duration of the disaster, normal schedules may be adjusted to focus on the recovery effort.

Outward Communications in an Emergency

In the event of an outage of the Baylor websites (including emergency situations), it may be necessary to communicate with a broad range of constituencies (faculty, staff, students, alumni, parents, community members, and the media). Baylor Marketing and Communications will take the lead on communications.

The following methods, depending on availability, will be used to provide ongoing updates regarding the recovery:

- ITS DOWN Line (254-710-3696/DOWN)
- ITS Website (www.baylor.edu/its)
- Email messages to the faculty/staff and student lists
- Baylor ITS Alert Twitter account
- Baylor ITS Facebook page

Disaster Recovery Priorities

The overarching goal of the disaster recovery framework is to minimize the disruption of operations and recover data/technology. While a disaster may vary in size and scope, ITS will focus on the core areas:

- Authentication and network delivery services
- Cloud systems
- Data networks and telecommunication
- Website and services
- On-premises enterprise applications

Once the core areas are functional, ITS will address priorities established by the ITS Emergency Response Team and/or senior management in the recovery effort.

Note: Response to and recovery from a disaster at Baylor University will be coordinated by the University's Emergency Management Team within the Department of Public Safety. Their response and actions are governed by the Baylor University Emergency Operations Plan. This policy serves as a supplement to the University's plan.

Disaster Recovery Framework

Depending on the impact and scope of the event, the ITS disaster recovery framework has been compiled into distinct profiles. While assessing the significance of the event, some or all of the profiles may be useful during the recovery. The profile categories are:

- Facilities Profiles
- Software Profiles
- Employee Profiles
- Vendor Profiles
- Insurance Profiles

The frameworks will be reviewed on an annual basis or as needed based on gaps between the current and required capabilities for system recovery.

Recovery Evaluation

It's important to remember that some of the best lessons are learned during difficult times. While our efforts attempt to identify and mitigate emerging risks, the potential for an unforeseen event remains. Therefore, after the completion of significant recovery of operations at the University, lessons learned meetings will take place within ITS and senior management to determine what part of the framework was successful and which parts need to be improved going forward.