

[Unit/Department Name]

IT DISASTER rECOVERY pLAN

(IT DRP)

Version [#]

REVISED

August 16, 2017.

### Preface

This document, **Department/Unit IT Disaster Recovery Plan (IT DRP)** is focused on the overall recovery of IT services based on the information resource owner’s established Recovery Time Objective (RTO) and Recovery Point Objective (RPO). Detailed recovery procedures and assumptions of individual or a group of interdependent mission critical electronic information resources or essential IT services are stored in the department/unit’s Information System Contingency Plan(s) (ISCP).

Other related documents include:

**Business Impact Analysis (BIA) of IT Services**

A BIA of a unit/department’s IT services is a systematic assessment of the potential impact of a loss of the service due to an interruption of computing and/or infrastructure support services resulting from a disruptive event or incident. All IT services must be included in a BIA. All IT services must be assigned a Recovery Time Objective (RTO) and a Recovery Point Objective (RPO) by their information resource owner.

**Facility Assessment for Mission Critical or Essential IT Facilities**

An integral part of an IT DR Program is taking steps to prevent a disaster or to mitigate its effects beforehand. A Facility Assessment examines various threats that could lead to a disaster, vulnerable areas, and steps taken to minimize risk to IT infrastructure and hardware that support mission critical electronic information resources and essential IT services. The threats covered in the assessment are both natural and human-created.

**Department/Unit IT Disaster Recovery Plan (IT DRP)**

IT DRP is focused on the overall recovery of IT services based on the information resource owner’s established Recovery Time Objective (RTO) and Recovery Point Objective (RPO). Detailed recovery procedures and assumptions of individual or a group of interdependent mission critical electronic information resource or essential IT services are stored in the department/unit’s Information System Contingency Plan(s) (ISCP).

**Information System Contingency Plan (ISCP) for Mission Critical / Essential IT Services.**

IT Services that have been identified by the information resource owner or the Chief Information Security Officer (CISO) as either an essential IT service or a mission critical electronic information resource must be included in an ISCP. An ISCP can be completed for an individual IT service or a group of interdependent IT services. AnISCP contains detailed procedures to recover a ***mission critical or essential IT service*** or a grouping of interdependent IT services following a disruption. Mission critical electronic information resources and essential IT services must be exercised annually.

**Cost Benefit Analysis Reports**

A Cost Benefit Analysis is only required if the IT service is determined to be an essential IT service and the actual Recovery Time Objective (RTO) is not in alignment with the required RTO.

**Texas A&M University IT Disaster Recovery Plan (DRP)**

Texas A&M University IT DRP, explains how the university recovers Essential IT Services following an emergency or disruption. The Texas A&M University IT DRP is written in support of  [Annex J](https://www.tamu.edu/emergency/documents/AnnexJ.pdf) (Institutional Continuity Plan) of the [Texas A&M University Emergency Operation Plan](https://www.tamu.edu/emergency/documents/EOP.pdf). Organizations supporting the Essential IT Services shall maintain their own procedures and actively participate in the training, exercise, and maintenance needed to support this plan.

### Approval and Implementation

*<Provide a statement in accordance with the unit/department’s contingency planning policy to affirm that the IT DRP is complete. This statement should be approved and signed by the Information Resource Owner. Space should be provided for the Information Resource Owner(s) to sign, along with any other applicable approving signatures. A sample language is provided below: >*

The Information Resource Owner is responsible for plan oversight and coordination with IT Service stakeholders. This plan and its supporting contents, are hereby approved, and effective immediately upon the signing of all signature authorities noted below.

Approved: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name

Title

Unit/Department Name

**Note to the Author**

This document can be used as a template for unit/department IT Disaster Recovery Plan (IT DRP). This template includes instructions to the author, boilerplate text, and fields that should be replaced with the values specific to the project.

Red *italicized text enclosed in angle brackets* (<text>) *provides instructions to the document author, or describes the intent, assumptions and context for content included in this document. Delete the blue text as you fill out the document.*

Blue *italicized text enclosed in square brackets* ([text]) *indicates an example/field that should be replaced with information specific to a particular project.*

Text and tables in black are provided as boilerplate examples of wording and formats that may be used or modified as appropriate to a specific project. These are offered only as suggestions to assist in developing project documents; they are not mandatory formats.

Table of Contents

[Overview 6](#_Toc490139862)

[Purpose 6](#_Toc490139863)

[Scope 6](#_Toc490139864)

[Changes and Updates 6](#_Toc490139865)

[Roles and Responsibilities 7](#_Toc490139866)

[Information Resource Owner 7](#_Toc490139867)

[IT Service Owner 7](#_Toc490139868)

[IT Service Manager 7](#_Toc490139869)

[[Unit/department Name] IT Services 8](#_Toc490139870)

[Order of Restoration (prioritized) 9](#_Toc490139871)

[Timeline Overview 10](#_Toc490139872)

[Information Resource Crisis Identification 10](#_Toc490139873)

[Immediately Following Activation 10](#_Toc490139874)

[Within 4 Hours 10](#_Toc490139875)

[Within 12 Hours 11](#_Toc490139876)

[Within 24 Hours 11](#_Toc490139877)

[Within 48 Hours 11](#_Toc490139878)

[Within 72 Hours 12](#_Toc490139879)

[Within 5 Days 12](#_Toc490139880)

[On-Going 12](#_Toc490139881)

[Personnel Contact List 13](#_Toc490139882)

[Index 14](#_Toc490139883)

[Glossary 15](#_Toc490139884)

[Record of Change 21](#_Toc490139885)

# Overview

## Purpose

The [Unit/Department Name] IT Disaster Recovery Plan (IT DRP) is a compilation of IT Service’s recovery procedures and resource requirements. These procedures and resource requirements are intended to be used by the IT Service Owner during a “non-business as usual event” to guide the recovery of Mission Critical and Essential IT Services.

## Scope

The [Unit/department Name]IT DRP is focused on the recovery of IT Services based on the Information Resource Owner’s established Recovery Time Objective (RTO) and Recovery Point Objective (RPO).

## Changes and Updates

IT Service Manager is responsible for notifying the CISO of changes in Essential IT Services that may impact the Texas A&M IT DRP.

# Roles and Responsibilities

## Information Resource Owner

Responsible for a business function(s) and for determining controls and access to information resources supporting that business function.

The Information Resource Owner oversees and prioritizes the actions of the [Unit/department Name]IT DRP activation.

## IT Service Owner

Accountable for ensuring the effective management of tasks associated with fulfilling the roles related to a specific service.

Reports to the Information Resource Owner and is responsible for coordinating the recovery of IT Services.

.

## IT Service Manager

Responsible for the effective completion of task associated with fulfilling the roles related to a specific service.

Reports to the IT Service Owner and is responsible for recovering the IT Service that they manage.

# [Unit/department Name] IT Services

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **RTO** | **RPO** | **IT Service Name** | **Business Function** | **Description of IT Service** | **Mission Critical** | **Essential IT Service** |
|  |  |  |  |  | Yes/No | Yes/No |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

<NOTE. RTO is define as; 0 Hours, 1 Hour, 2 Hours, 4 Hours, 8 Hours, 12 Hours, 24 Hours, 48 Hours, 72 Hours, 1 Weeks (7d), 2 Weeks (7d), 3 Weeks (7d), 4 Weeks (7d), 5 Weeks (7d), and 6 Weeks (7d)>

# Order of Restoration (prioritized)

<NOTE. List the IT Services in the order that they would need to be restored. The order should take into account the IT Service’s dependencies.>



# Timeline Overview

The following overview outlines the service level(s) that each IT Service Manager has committed to provide when the [Unit/Department Name] IT DRP is activated.

## Information Resource Crisis Identification

### IT Service Owner

* Potential Information Resource Crisis is detected or reported to the Information Resource Owner.
* Conduct an initial IT event assessment.
* The Information Resource Owner has up to 48 hours from the time of the initial incident identification to determine if an [Unit/Department Name] IT DRP activation should be made.
* Instruct IT Services Managers to conduct a damage assessment.

## Immediately Following Activation

### IT Service Owner

* Receive input from the IT Services Managers damage assessments.
* Make the determination that IT is affected.
* Notify Texas A&M IT Operation Center of the information resource crisis.
* Condition and activate the information technology recovery site.
* Instruct IT Service Managers to begin recovery of Mission Critical and Essential IT Services (see Information System Contingency Plans (ISCP).

## Within 4 Hours

### IT Service Owner

* Review the order of restoration list located in Annex.
* Make the IT assessment decision.
* Following the direction of the Information Resource Owner to alert the recovery site of possible activation.

### IT Service Managers

* Report status of all IT Services with a 0 to 72 hour RTO.
* Report status of Essential IT Services to the IT Service Owner.
* {IT Service Name Example 1 ] ISCP
  + - * Break all the replication contexts on the destination appliance
      * Verify route information exists on backup system
      * Verify necessary appliance and server
      * Validate or create mount points on the server
      * Prepare restore
      * Restore to server
      * Verify server application restored successfully and is running in the background
      * Confirm integrity of file device type client data
      * Restore/retrieve client backup/archive data base on establish it service.
* [IT Service Name Example 2] ISCP
  + - * Verifies operation of shared virtualize service located at operational site.
      * Begins the process of initializing system copies.
      * Begins the process of restoring backup copies of systems based on each IT Service’s established RTOs.
* {IT Service Name Example 3] ISCP
  + - * Step 1
      * Step 2
      * Step 3

## Within 12 Hours

### IT Service Owner

* Report status of Essential IT Services to the Texas A&M IT Operation Center. .

### IT Service Managers

* {IT Service Name Example 3] ISCP
  + - * Step 4
      * Step 5
      * Step 6

## Within 24 Hours

### IT Service Owner

* Report status of Essential IT Services to the Texas A&M IT Operation Center. .

### IT Service Manager

* {IT Service Name Example 3] ISCP
  + - * Step 7
      * Step 8
      * Step 9

## Within 48 Hours

### IT Service Owner

* Report status of Essential IT Services to the Texas A&M IT Operation Center. .

### IT Service Manager

* {IT Service Name Example 3] ISCP
  + - * Step 10
      * Step 11
      * Step 12

## Within 72 Hours

### IT Service Owner

* Report status of Essential IT Services to the Texas A&M IT Operation Center. .

### IT Service Manager

* {IT Service Name Example 1] ISCP
  + - * Step 13
      * Step 4
      * Step 5

## Within 5 Days

### IT Service Owner

* Report status of Essential IT Services to the Texas A&M IT Operation Center. .

### IT Service Manager

* {IT Service Name] ISCP
  + - * Step 16
      * Step 17
      * Step 18

## On-Going

### IT Service Owner

* Continues to manage recovery activities until normal business operations resume
* Report status of Essential IT Services to the Texas A&M IT Operation Center. .

### IT Service Manager

* Report status of Essential IT Services to the Texas A&M IT Operation Center.
* {IT Service Name Example 3] ISCP
  + - * Step 19
      * Step 20

# Personnel Contact List

Worksheet H of the [Unit/department Name]Continuity of Operation Plan provides the details of the personnel contact list.

# Index

B

BIA 6

I

Information Resource Owner 6

IT Service Manager 6

ITC-01 10

O

On-Going 12

Overview 6

P

Purpose 6

R

RPO 6

RTO 6

S

Scope 6

W

Within 12 Hours 11

Within 24-Hours 11

Within 48-Hours 11

Within 4-Hours 10

Within 5-Days 12

Within 72-Hours 11

# Glossary

**Administrator**

* Responsible for configuring, managing, overseeing and maintaining a computing environment or system. Responsibilities vary depending on an organization's requirements. This person should possess strong technical knowledge and skills

**Business Function**

* Process or operation performed routinely to carry out a part of the mission of an organization.

**Business Impact Analysis**

* Business impact analysis is the activity in business continuity management that identifies vital business functions and dependencies. These dependencies may include suppliers, people, other business processes, IT services, etc. Business impact analysis defines the recovery requirements for IT services. These requirements include recovery time objectives, recovery point objectives and minimum service level targets for each IT service. (ITIL Service Strategy)

**Continuity of Operations**

* The ability of an organization to provide service and support for its customers and maintain its viability before, during, and after a business continuity event.

**Cost Benefit Analysis**

* Cost benefit analysis (CBA), sometimes called benefit cost analysis (BCA), is a systematic approach to estimating the strengths and weaknesses of alternatives (for example in transactions, activities, functional business requirements). It is used to determine options that provide the best approach to achieve benefits while preserving savings. The CBA is also defined as a systematic process for calculating and comparing benefits and costs of a decision, policy (with particular regard to government policy) or (in general) project. Broadly, CBA has two main purposes: 1. to determine if an investment/decision is sound (justification/feasibility) by verifying whether its benefits outweigh the costs, and by how much; 2. to provide a basis for comparing projects,which involves comparing the total expected cost of each option against its total expected benefits.

**Critical Infrastructure Functions**

* University-wide functions that must continue uninterrupted or can be resumed within a few hours. Examples of critical infrastructure include: - Emergency response services; - Utilities, including electricity, water, and reasonable climate control; - Communications with internal and external audiences to include students, faculty, staff, and media; - Internet, authentication, and voice communications; - Hazardous materials spill response and control to include safe handling and proper disposal of toxic substances, biologically hazardous materials, and radioactive materials.

**Custodian of an Information Resource**

* A person responsible for implementing owner-defined controls and access to an information resource. Custodians may include university employees, vendors, and any third party acting as an agent of – or otherwise on behalf of – the university and/or the owner.

**Essential Functions**

* Defined in the Institutional Continuity Plan ([Annex J](https://www.tamu.edu/emergency/documents/AnnexJ.pdf)) as functions that must be either Uninterrupted or resumed within a few hours of an incident.

Essential Functions support:

* + Emergency Response Services,
  + Utilities to include electricity, water, and reasonable climate control,
  + Communications with internal and external audiences to include students, faculty, staff and the media,
  + Internet, authentication, and voice communications,
  + Hazardous materials spill response and control, to include safe handling and proper disposal of toxic substances, biologically hazardous materials, and radioactive materials.

**Essential IT Service**

* An IT service with a Recovery Time Objective of less than 12 hours and one required to support the critical infrastructure functions of the university.

**IT Disaster Recovery Plan (IT DRP)**

* Department/unit-level plan that is focused on the overall recovery of Electronic Information Resources supported by the department/unit.

**IT Service**

* Made up of a combination of information technology, people, and processes. A customer-facing IT service directly supports the business processes of one or more customers. Other IT services, called supporting services, are not directly used by the business, but are required by the service provider to deliver customer-facing services.

**IT Service Manager**

* A person who is mostly responsible for the effective completion of task associated with fulfilling the roles related to a specific service.

**IT Service Owner**

* The person who is mostly accountable to ensure the effective management of tasks associated with fulfilling the roles related to a specific service. In some cases, the unit/department contact for the service is listed until the owner determined.

**Information Resource Owner**

* A person responsible for a business function and for determining controls and access to information resources supporting that business function.

**Information Resource User**

* An individual or automated application authorized to access an information resource in accordance with the owner-defined controls and access rules.

**Information Resources (IR)**

* The procedures, computer equipment, computing facilities, software and data which are purchased, designed, built, operated and maintained to collect, record, process, store, retrieve, display, report

and transmit information.

**Information Resources Crisis (formerly incident)**

* A situation declared as a crisis by designated Texas A&M IT personnel.

**Information System**

* A discrete set of information resources organized for the management and processing of information supporting a defined business, academic, or research function.

**Mission Critical Information**

* Information defined by the information resource owner (or by the University for Essential IT Services) to be crucial to the continued performance of the mission of the department/unit. Unavailability of such information would result in more than an inconvenience. An event causing the unavailability of mission-critical information would result in consequences such as significant financial loss, institutional embarrassment, failure to comply with regulations or legal obligations, or closure of the department/unit.

**NIST**

* The Texas A&M Information Security Controls, adopted from state requirements, align with the National Institute of Standards and Technology (NIST) Special Publication 800-53 Version 4 (NIST SP 800-53 Rev. 4). The risk assessment tool provided by the state, SPECTRIM, utilizes questions based on NIST SP 800-53 Rev. 4.

**Platform**

* Collective term for computer hardware and software components of a particular system. A platform includes a hardware architecture and a software framework (including application frameworks), where the combination allows software, particularly application software, to run. Typical platforms include a computer architecture, operating system, programming languages and related user interface (run-time system libraries or graphical user interface). Examples of common platforms would include servers, desktop/workstations, laptops, tablets, and smartphones. Special-purpose platforms include routers, remote access servers and database servers.

**Platform as a Service (PaaS)**

* Capability provided to the consumer to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control underlying cloud infrastructure, including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment (NIST 800-145 September 2011).

**Recovery Point Objective**

* Acceptable amount of data loss measured in time. Unless requested for by the information resource owner, offsite storage of daily incremental and full weekly backups are only taken off site once a week. (ITIL Service Design) (ITIL Service Operation)

**Recovery Time Objective**

* The maximum time allowed for the recovery of an IT service following an interruption. The service level to be provided may be less than normal service level targets. Recovery time objectives for each IT service should be negotiated, agreed and documented. See also business impact analysis. (ITIL Service Design) (ITIL Service Operation)

**Significant Information Security Incident**

* An information security incident is considered significant if it meets one or more of the following criteria: -involves actual or suspected unauthorized disclosure of confidential information; -involves consequential legal issues; -may cause severe disruption to unit mission-critical services or university wide Essential IT services; -involves active threats; -is widespread; -is likely to raise public interest

**Software**

* A computer program that provides the instructions enabling the computer hardware to work. System software, such as Windows or MacOS, operate the machine itself, and applications software, such as spreadsheet or word processing programs, provide specific functionality.

**Software as a Service (SaaS)**

* Capability provided to the consumer to use the provider’s applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings (NIST 800145 September 2011).

**Texas A&M University IT Disaster Recovery Plan**

* Limited to Essential IT Services supporting essential functions as defined by Institutional Continuity Plan [(Annex J](https://www.tamu.edu/emergency/documents/AnnexJ.pdf)) of the [Texas A&M University Emergency Operation Plan](https://www.tamu.edu/emergency/documents/EOP.pdf). Organizations that support Essential IT Services shall maintain their own procedures and actively participate in the training, exercise, and maintenance needed to support this plan.

**Texas A&M University IT Disaster Recovery Program**

* Builds on Institutional Continuity Plan [(Annex J](https://www.tamu.edu/emergency/documents/AnnexJ.pdf)) of the [Texas A&M University Emergency Operation Plan](https://www.tamu.edu/emergency/documents/EOP.pdf) by providing guidance and templates to relate a business function’s Recovery Time Objective (RTO) and Recovery Point Objective (RPO) to the IT services that support department/unit business functions.

**Third Party**

* Individual or entity who is not a university employee, i.e., vendors or other individuals acting in a capacity other than a university employee.

**Third-Party Vendor**

* An individual or organization separate from the two principals involved. A third party is typically a company that provides an auxiliary product or service not supplied by the primary provider to the end user (the two principals).

**Unit**

* A Texas A&M University (Texas A&M) organization, or affiliate, that is managed by an employee with hiring and firing authority. Examples are a division, a department, a research center, and others.

**Vendor**

* Individual or entity who has a contract with the university to provide goods or services for compensation. This term excludes contract employees.

# Record of Change

This plan is updated at least annually, as described in the ISRR Program document.

|  |  |  |  |
| --- | --- | --- | --- |
| **RECORD OF CHANGE** | **DATE OF**  **CHANGE** | **DESCRIPTION OF CHANGE** | **CHANGE MADE**  **BY:** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |