

[System Name]

*Security Categorization: Mission Critical*

[Unit/Department name]

Information System Contingency Plan (ISCP)

Version [#]

REVISED

August 23, 2017

### Preface

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

**Facility Assessment for Mission Critical or Essential IT Facilities** is an integral part of an IT DR Program. By 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.

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.

**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 ISCP is complete and has been tested sufficiently. The statement should also affirm that the IT Service Manager is responsible for continued maintenance and testing of the ISCP. This statement should be approved and signed by the IT Service Manager. Space should be provided for the IT Service Manager to sign, along with any other applicable approving signatures. A sample language is provided below: >*

As the IT Service Manager for [IT Service name], I hereby certify that the information system contingency plan (ISCP) is complete, and that the information contained in this ISCP provides an accurate representation of the application, its hardware, software, and telecommunication components. I further certify that this document identifies the criticality of the IT Service as it relates to the mission of the [unit/department name], and that the recovery strategies identified will provide the ability to recover the IT Service functionality in the most expedient and cost-beneficial method in keeping with its level of criticality.

I further attest that this ISCP for [IT Service name]will be tested at least annually. This plan was last tested on [insert exercise date]; the test, training, and exercise (TT&E) material associated with this test can be found [TT&E results appendix or location]. This document will be modified as changes occur and will remain under version control, in accordance with [unit/department name]’s contingency planning policy.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**IT Service Manager Name Date**

Name

Title

[Unit/Department name]

Texas A&M University

**Note to the Author**

NOTE: This sample template has been modified from the original template created by NIST to address NIST SP 800-53 security controls from the Contingency Planning family for a high impact information system.

This document can be used as a template for an Information System Contingency Plan (ISCP). 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.

**Find and Replace**

[unit/department name]

[IT Service name]

[RTO hours]

[Maximum Tolerable Downtime]

[name of recovery team] - IT Damage Assessment Unit

[IT Service Manager]

[Building #, City, State]

[insert exercise date]

[RPO hours]

Table of Contents

[1 Overview 6](#_Toc490042157)

[1.1 Background 6](#_Toc490042158)

[1.2 Scope 6](#_Toc490042159)

[1.3 Assumptions 6](#_Toc490042160)

[2. Concept of Operations 8](#_Toc490042161)

[2.1 System Description 8](#_Toc490042162)

[2.2 Overview of Three Phases 8](#_Toc490042163)

[2.3 Roles and Responsibilities 9](#_Toc490042164)

[3. Activation and Notification 10](#_Toc490042165)

[3.1 Activation Criteria and Procedure 10](#_Toc490042166)

[3.2 Notification 10](#_Toc490042167)

[3.3 Outage Assessment 10](#_Toc490042168)

[4. Recovery 12](#_Toc490042169)

[4.1 Sequence of Recovery Activities 12](#_Toc490042170)

[4.2 Recovery Procedures 12](#_Toc490042171)

[5. Reconstitution 13](#_Toc490042172)

[5.1 Concurrent Processing 13](#_Toc490042173)

[5.2 Validation Data Testing 13](#_Toc490042174)

[5.3 Validation Functionality Testing 13](#_Toc490042175)

[5.4 Recovery Declaration 14](#_Toc490042176)

[5.5 Notifications (users) 14](#_Toc490042177)

[5.6 Cleanup 14](#_Toc490042178)

[5.7 Offsite Data Storage 14](#_Toc490042179)

[5.8 Data Backup 14](#_Toc490042180)

[5.9 Event Documentation 15](#_Toc490042181)

[5.10 Deactivation 15](#_Toc490042182)

[SUGGESTED APPENDICES 16](#_Toc490042183)

[APPENDIX A PERSONNEL CONTACT LIST 16](#_Toc490042184)

[APPENDIX B VENDOR CONTACT LIST 17](#_Toc490042185)

[APPENDIX C DETAILED RECOVERY PROCEDURES 17](#_Toc490042186)

[APPENDIX D ALTERNATE PROCESSING PROCEDURES 17](#_Toc490042187)

[APPENDIX E SYSTEM VALIDATION TEST PLAN 17](#_Toc490042188)

[APPENDIX F ALTERNATE STORAGE, SITE, AND TELECOMMUNICATIONS 18](#_Toc490042189)

[APPENDIX H HARDWARE AND SOFTWARE INVENTORY 20](#_Toc490042190)

[APPENDIX I INTERCONNECTIONS TABLE 20](#_Toc490042191)

[APPENDIX J TEST and MAintenance SCHEDULE 20](#_Toc490042192)

[APPENDIX K ASSOCIATED PLANS AND PROCEDURES 21](#_Toc490042193)

[APPENDIX L BUSINESS IMPACT ANALYSIS 21](#_Toc490042194)

[APPENDIX M DOCUMENT CHANGE PAGE 21](#_Toc490042195)

[Index 23](#_Toc490042196)

[Record of Change 30](#_Toc490042197)

# 1 Overview

IT Services are vital to [Unit/Department Name]’s mission/business processes; therefore, it is critical that services provided by [IT Service name] are able to operate effectively without excessive interruption.  This Information System Contingency Plan (ISCP) establishes comprehensive procedures to recover [IT Service name] quickly and effectively following a service disruption.

## 1.1 Background

This [IT Service name] ISCP establishes procedures to recover [IT Service name] following a disruption. The following recovery plan objectives have been established:

* Maximize the effectiveness of contingency operations through an established plan that consists of the following phases:
  + ***Activation and Notification phase*** to activate the plan and determine the extent of damage;
  + ***Recovery phase*** to restore [IT Service name] operations; and
  + ***Reconstitution phase*** to ensure that [IT Service name] is validated through testing and that normal operations are resumed.
* Identify the activities, resources, and procedures to carry out [IT Service name]processing requirements during prolonged interruptions to normal operations.
* Assign responsibilities to designated [unit/department name] personnel and provide guidance for recovering [IT Service name] during prolonged periods of interruption to normal operations.
* Ensure coordination with other personnel responsible for [unit/department name]contingency planning strategies. Ensure coordination with external points of contact and vendors associated with [IT Service name] and execution of this plan.

## 1.2 Scope

This ISCP has been developed for [IT Service name], which is classified as a Mission Critical Information Resource, in accordance with CP-2 Contingency Plan. Procedures in this ISCP are for Mission Critical IT Service and designed to recover [IT Service name] within [RTO hours]with a recovery point objective of[RPO hours].This plan does not address replacement or purchase of new equipment, short-term disruptions lasting less than [Maximum Tolerable Downtime] or loss of data at the onsite facility or at the user-desktop levels.

## 1.3 Assumptions

The following assumptions were used when developing this ISCP:

* [IT Service name] has been established as a mission critical IT Service, in accordance with *CP-2.*
* Alternate processing sites and offsite storage are required and have been established for this system.
* Current backups of the system software and data are intact and available at the offsite storage facility in [Building #, City, State]*.*
* Alternate facilities have been established at [Building #, City, State] and are available if needed for relocation of [IT Service name]*.*
* The [IT Service name] is inoperable at the [unit/department name] and cannot be recovered within [Maximum Tolerable Downtime] *.*
* Key [IT Service name] personnel have been identified and trained in their emergency response and recovery roles; they are available to activate the [IT Service name] Information System Contingency Plan.

<Additional assumptions as appropriate.>

The [IT Service name] ISCP does not apply to the following situations:

* **Overall recovery and continuity of mission/business operations.** The Business Continuity Plan (BCP) and Continuity of Operations Plan (COOP) address continuity of business operations.
* **Emergency evacuation of personnel.** The Building Emergency Evacuation Plan addresses employee evacuation.

<Any additional constraints and associated plans should be added to this list.>

# 2. Concept of Operations

The Concept of Operations section provides details about [IT Service name], an overview of the three phases of the ISCP (Activation and Notification, Recovery, and Reconstitution), and a description of roles and responsibilities of [Unit/Department name]’s personnel during a contingency activation.

## 2.1 IT Service Description

<NOTE: Provide a general description of IT Service architecture and functionality>

<Indicate the operating environment, physical location, general location of users, and partnerships with external organizations/IT Services. Include information regarding any other technical considerations that are important for recovery purposes, such as backup procedures.>

## 2.2 Overview of Three Phases

This ISCP has been developed to recover the [IT Service name] using a three-phased approach. This approach ensures that IT Service recovery efforts are performed in a methodical sequence to maximize the effectiveness of the recovery effort and minimize IT Service outage time due to errors and omissions.

The three IT Service recovery phases are:

**Activation and Notification Phase –** Activation of the ISCP occurs after a disruption or outage that may reasonably extend beyond the RTO established for a IT Service. The outage event may result in severe damage to the facility that houses the IT Service, severe damage or loss of equipment, or other damage that typically results in long-term loss.

Once the ISCP is activated, IT Service owners and users are notified of a possible long-term outage, and a thorough outage assessment is performed for the IT Service. Information from the outage assessment is presented to IT Service owners and may be used to modify recovery procedures specific to the cause of the outage.

**Recovery Phase –** The Recovery phase details the activities and procedures for recovery of the affected IT Service. Activities and procedures are written at a level that an appropriately skilled technician can recover the IT Service without intimate IT Service knowledge. This phase includes notification and awareness escalation procedures for communication of recovery status to IT Service owners and users.

**Reconstitution –** The Reconstitution phase defines the actions taken to test and validate IT Service capability and functionality at the original or new permanent location. This phase consists of two major activities: validating successful reconstitution and deactivation of the plan.

During validation, the IT Service is tested and validated as operational prior to returning operation to its normal state. Validation procedures may include functionality or regression testing, concurrent processing, and/or data validation. The IT Service is declared recovered and operational by IT Service owners upon successful completion of validation testing.

Deactivation includes activities to notify users of IT Service operational status. This phase also addresses recovery effort documentation, activity log finalization, incorporation of lessons learned into plan updates, and readying resources for any future events.

## 2.3 Roles and Responsibilities

The ISCP establishes several roles for [IT Service name] recovery and reconstitution support*.* Persons or teams assigned ISCP roles have been trained to respond to a contingency event affecting [IT Service name]*.*

<Describe each team and role responsible for executing or supporting IT Service recovery and reconstitution. Include responsibilities for each team/role, leadership roles, and coordination with other recovery and reconstitution teams, as applicable. At a minimum, a role should be established for a IT Service owner or business unit point of contact, an IT Service Manager, and an application administrator point of contact>.

<Leadership roles should include an IT Service Owner, who has overall management responsibility for the plan, and an IT Service Manager, who is responsible to oversee recovery and reconstitution progress, initiate any needed escalations or awareness communications, and establish coordination with other recovery and reconstitution teams as appropriate.>

# 3. Activation and Notification

The Activation and Notification Phase defines initial actions taken once a [IT Service name] disruption has been detected or appears to be imminent.  This phase includes activities to notify recovery personnel, conduct an outage assessment, and activate the ISCP.  At the completion of the Activation and Notification Phase, [IT Service name] ISCP staff will be prepared to perform recovery measures.

## 3.1 Activation Criteria and Procedure

The [IT Service name] ISCP may be activated if one or more of the following criteria are met:

1. The type of outage indicates [IT Service name] will be down for more than [Maximum Tolerable Downtime] *;*
2. The facility housing [IT Service name] is damaged and may not be available within [Maximum Tolerable Downtime] *; and*
3. *Other criteria, as appropriate.*

The following persons or roles may activate the ISCP if one or more of these criteria are met:

<Establish one or more roles that may activate the plan based on activation criteria. Authorized persons may include the IT Service or business owner, or the operations point of contact (POC) for IT Service support.>

1. Information Resource Owner

## 3.2 Notification

The first step upon activation of the [IT Service name] ISCP is notification of appropriate business and IT Service support personnel. Contact information for appropriate POCs is included in Personnel Contact List Appendix A.

For [IT Service name], the following method and procedure for notifications are used:

<Describe established notification procedures. Notification procedures should include who makes the initial notifications, the sequence in which personnel are notified (e.g., IT Service owner, technical POC, IT Service Manager, business unit or user unit POC, and recovery team POC), and the method of notification (e.g., email blast, call tree, automated notification IT Service, etc.).>

## 3.3 Outage Assessment

Following notification, a thorough outage assessment is necessary to determine the extent of the disruption, any damage, and expected recovery time. This outage assessment is conducted by [name of recovery team]. Assessment results are provided to the IT Service Manager to assist in the coordination of the recovery of [IT Service name]*.*

<Outline detailed procedures to include how to determine the cause of the outage; identification of potential for additional disruption or damage; assessment of affected physical area(s); and determination of the physical infrastructure status, IS equipment functionality, and inventory. Procedures should include notation of items that will need to be replaced and estimated time to restore service to normal operations.>

# 4. Recovery

The Recovery Phase provides formal recovery operations that begin after the ISCP has been activated, outage assessments have been completed (if possible), personnel have been notified, and appropriate teams have been mobilized.  Recovery Phase activities focus on implementing recovery strategies to restore IT Service capabilities, repair damage, and resume operational capabilities at the original or an alternate location.  At the completion of the Recovery Phase, [IT Service name] will be functional and capable of performing the functions identified in Section 2.1 of this plan.

## 4.1 Sequence of Recovery Activities

The following activities occur during recovery of [IT Service name]*:*

Modify the following list as appropriate for the selected IT Service recovery strategy:

## 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 [Maximum Tolerable Downtime] from the time of the initial incident identification to determine if a [IT Service name] ISCP activation should be made.
* Instruct IT Service Managers to conduct a damage assessment.

## Immediately Following Activation

### IT Service Owner

* Receive input from the IT Service 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 Service (see Information System Contingency Plans (ISCP).

## Within 4 Hours

### IT Service Owner

* 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] 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] 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] 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] 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] 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] ISCP
  + - * Step 19
      * Step 20

## 4.2 Recovery Procedures

The following procedures are provided for recovery of [IT Service name] at the original or established alternate location*.* Recovery procedures are outlined per team and should be executed in the sequence presented to maintain an efficient recovery effort.

<Provide general procedures for the recovery of the IT Service from backup media. Specific keystroke-level procedures may be provided in an appendix. If specific procedures are provided in an appendix, a reference to that appendix should be included in this section. Teams or persons responsible for each procedure should be identified.>

## 4.3 Recovery Escalation Notices/Awareness

<Provide appropriate procedures for escalation notices during recovery efforts. Notifications during recovery include problem escalation to leadership and status awareness to IT Service owners and users. Teams or persons responsible for each escalation/awareness procedure should be identified.>

# 5. Reconstitution

Reconstitution is the process by which recovery activities are completed and normal IT Service operations are resumed. If the original facility is unrecoverable, the activities in this phase can also be applied to preparing a new permanent location to support IT Service processing requirements. A determination must be made on whether the IT Service has undergone significant change and will require reassessment and reauthorization. The phase consists of two major activities: validating successful reconstitution and deactivation of the plan.

## 5.1 Concurrent Processing

<Mission critical IT Services are not required to have concurrent processing as part of the validation effort. If concurrent processing does occur for the IT Service prior to making it operational, procedures should be inserted here. Procedures should include length of time for concurrent processing, processing information on both concurrent IT Services, and validating information on the new permanent IT Service.>

<For Mission Critical IT Services without concurrent processing, this section may either be removed or the following may be used:>

In concurrent processing, an IT Service operates at two separate locations concurrently until there is a level of assurance that the recovered IT Service is operating correctly*.* [IT Service name]does not have concurrent processing as part of validation. Once the IT Service has been tested and validated, it will be placed into normal operations.

## 5.2 Validation Data Testing

Validation data testing is the process of testing and validating recovered data to ensure that data files or databases have been recovered completely. The following procedures will be used to determine that the recovered data is complete and current to the last available backup:

<Provide procedures for testing or validation of recovered data to ensure that data is correct and up to date. This section may be combined with the Functionality Testing section if procedures test both the functionality and data validity. Teams or persons responsible for each procedure should be identified. An example of a validation data test for a Mission Critical IT Service would be to log into the IT Service database and check the audit logs to determine that all transactions and updates are current. Detailed data test procedures may be provided in Appendix E, IT Service Validation Test Plan.>

## 5.3 Validation Functionality Testing

Validation functionality testing is the process of verifying that [IT Service name] functionality has been tested, and the IT Service is ready to return to normal operations.

<Provide IT Service functionality testing and validation procedures to ensure that the IT Service is operating correctly. This section may be combined with the Data Testing section if procedures test both the functionality and data validity. Teams or persons responsible for each procedure should be identified. An example of a functional test for a Mission Critical IT Service may be logging into the IT Service and running a series of operations as a test or real user to ensure that all parts of the IT Service are operating correctly. Detailed functionality test procedures may be provided in Appendix E, IT Service Validation Test Plan.>

## 5.4 Recovery Declaration

Upon successfully completing testing and validation, the IT Service Manager will formally declare recovery efforts complete, and that [IT Service name] is in normal operations. [IT Service name] business and technical POCs will be notified of the declaration by the IT Service Manager.

## 5.5 Notifications (users)

Upon return to normal IT Service operations, [IT Service name] users will be notified byIT Service Manager [or designee]using *predetermined notification procedures (e.g., email, broadcast message, phone calls, etc.).*

## 5.6 Cleanup

Cleanup is the process of cleaning up or dismantling any temporary recovery locations, restocking supplies used, returning manuals or other documentation to their original locations, and readying the IT Service for a possible future contingency event.

<Provide any specific cleanup procedures for the IT Service, including preferred locations for manuals and documents and returning backup or installation media to its original location.>

## 5.7 Offsite Data Storage

It is important that all backup and installation media used during recovery be returned to the offsite data storage location. The following procedures should be followed to return backup and installation media to its offsite data storage location.

<Provide procedures for returning retrieved backup or installation media to its offsite data storage location. This may include proper logging and packaging of backup and installation media, preparing for transportation, and validating that media is securely stored at the offsite location.>

## 5.8 Data Backup

As soon as reasonable following recovery, the IT Service should be fully backed up and a new copy of the current operational IT Service stored for future recovery efforts. This full backup is then kept with other IT Service backups. The procedures for conducting a full IT Service backup are:

<Provide appropriate procedures for ensuring that a full IT Service backup is conducted within a reasonable time frame, ideally at the next scheduled backup period. This backup should go offsite with the other media in Section 5.7.>

## 5.9 Event Documentation

It is important that all recovery events be well-documented, including actions taken and problems encountered during the recovery and reconstitution effort, and lessons learned for inclusion and update to this ISCP. It is the responsibility of each ISCP team or person to document their actions during the recovery and reconstitution effort, and to provide that documentation to the IT Service Manager.

<Provide details about the types of information each ISCP team member is required to provide or collect for updating the ISCP with lessons learned. Types of documentation that should be generated and collected after a contingency activation include:

Activity logs (including recovery steps performed and by whom, the time the steps were initiated and completed, and any problems or concerns encountered while executing activities);

Functionality and data testing results;

Lessons learned documentation; and

After Action Report.

Event documentation procedures should detail responsibilities for development, collection, approval, and maintenance.>

## 5.10 Deactivation

Once all activities have been completed and documentation has been updated, the IT Service Managerwill formally deactivate the ISCP recovery and reconstitution effort. Notification of this declaration will be provided to all business and technical POCs.

# SUGGESTED APPENDICES

<ISCP appendices included should be based on IT Service and plan requirements. The following appendices are recommended: >

## APPENDIX A PERSONNEL CONTACT LIST

<Provide contact information for each person with a role or responsibility for activation or implementation of the ISCP, or coordination with the ISCP. For each person listed, at least one office and one non-office contact number is recommended. Note: Information may contain personally identifiable information and should be protected.>

| *[IT Service name]*  **ISCP Key Personnel** | | |
| --- | --- | --- |
| **Key Personnel** | **Contact Information** | |
| **Information Resource Owner** | Work | Insert number |
| *Insert Name and Title* | Home | Insert number |
|  | Cellular | Insert number |
|  | Email | Insert email address |
|  |  |  |
| **IT Service Owner** | Work | Insert number |
| *Insert Name and Title* | Home | Insert number |
|  | Cellular | Insert number |
|  | Email | Insert email address |
|  |  |  |
|  |  |  |
| **IT Service Manager** | Work |  |
|  | Home |  |
|  | Cellular |  |
|  | Email |  |
|  |  |  |
| **Application Support** | Work |  |
|  | Home |  |
|  | Cellular |  |
|  | Email |  |
|  |  |  |
| **VM Support** | Work |  |
|  | Home |  |
|  | Cellular |  |
|  | Email |  |
|  |  |  |
| **OS / Hardware Support** | Work |  |
|  | Home |  |
|  | Cellular |  |
|  | Email |  |
|  |  |  |
| **Database Support** | Work |  |
|  | Home |  |
|  | Cellular |  |
|  | Email |  |
|  |  |  |
| **Customer Support** | Work |  |
|  | Home |  |
|  | Cellular |  |
|  | Email |  |

## APPENDIX B VENDOR CONTACT LIST

<Contact information for all key maintenance or support vendors should be included in this appendix. Contact information, such as emergency phone numbers, contact names, contract numbers, and contractual response and onsite times should be included.>

## APPENDIX C DETAILED RECOVERY PROCEDURES

<This appendix includes the detailed recovery procedures for the IT Service, which may include items such as:

Keystroke-level recovery steps;

IT Service installation instructions from tape, CD, or other media;

Required configuration settings or changes;

Recovery of data from tape and audit logs; and

Other IT Services recovery procedures, as appropriate.

If the IT Service relies totally on another group or IT Service for its recovery and reconstitution (such as a mainframe system), information provided should include contact information and locations of detailed recovery and reconstitution procedures for that supporting IT Services.>

## APPENDIX D ALTERNATE PROCESSING PROCEDURES

<This section should identify any alternate manual or technical processing procedures available that allow the business unit to continue some processing of information that would normally be done by the affected system. Examples of alternate processes include manual forms processing, input into workstations to store data until it can be uploaded and processed, or queuing of data input.>

## APPENDIX E IT SERVICE VALIDATION TEST PLAN

<This appendix includes IT Service acceptance procedures that are performed after the IT Service has been recovered and prior to putting the IT Service into full operation and returned to users. The IT Service validation test plan may include the regression or functionality testing conducted prior to implementation of a IT Service upgrade or change.

An example of a IT Service validation test plan:>

Once the IT Service has been recovered, the following steps will be performed to validate IT Service data and functionality:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Procedure** | **Expected Results** | **Actual Results** | **Successful?** | **Performed by** |
| At the Command Prompt, type in sysname | IT Service Log-in Screen appears |  |  |  |
| Log in as user test user, using password test pass | Initial Screen with Main Menu shows |  |  |  |
| From Menu - select 5- Generate Report | Report Generation Screen shows |  |  |  |
| - Select Current Date Report  - Select Weekly  - Select To Screen | Report is generated on screen with last successful transaction included |  |  |  |
| - Select Close | Report Generation Screen Shows |  |  |  |
| - Select Return to Main Menu | Initial Screen with Main Menu shows |  |  |  |
| - Select Log-Off | Log-in Screen appears |  |  |  |

## APPENDIX F ALTERNATE STORAGE, SITE, AND TELECOMMUNICATIONS

<This appendix provides information for alternate storage, alternate processing site, and alternate telecommunications for the IT Service. Alternate storage, site, and telecommunications information is required for high-impact IT Services, per NIST SP 800-53 Rev. 3. Refer to NIST SP 800-53 Rev. 3, for details on control specifics. Information that should be provided for each area includes:>

*Alternate Storage:*

* City and state of alternate storage facility, and distance from primary facility;
* Whether the alternate storage facility is owned by the organization or is a third-party storage provider;
* Name and points of contact for the alternate storage facility;
* Delivery schedule and procedures for packaging media to go to alternate storage facility;
* Procedures for retrieving media from the alternate storage facility;
* Names and contact information for those persons authorized to retrieve media;
* Alternate storage configuration features that facilitate recovery operations (such as keyed or card reader access by authorized retrieval personnel);
* Any potential accessibility problems to the alternate storage site in the event of a widespread disruption or disaster;
* Mitigation steps to access alternate storage site in the event of a widespread disruption or disaster;
* Types of data located at alternate storage site, including databases, application software, operating IT Services, and other critical information IT Service software; and
* Other information as appropriate.

*Alternate Processing Site:*

* City and state of alternate processing site, and distance from primary facility;
* Whether the alternate processing site is owned by the unit/department or is a third-party site provider;
* Name and points of contact for the alternate processing site;
* Procedures for accessing and using the alternate processing site, and access security features of alternate processing site;
* Names and contact information for those persons authorized to go to alternate processing site;
* Type of alternate processing site, and equipment available at site;
* Alternate processing site configuration information (such as available power, floor space, office space, telecommunications availability, etc.);
* Any potential accessibility problems to the alternate processing site in the event of a widespread disruption or disaster;
* Mitigation steps to access alternate processing site in the event of a widespread disruption or disaster;
* SLAs or other agreements of use of alternate processing site, available office/support space, setup times, etc.; and
* Other information as appropriate.

*Alternate Telecommunications:*

* Name and contact information of alternate telecommunications vendors;
* Geographic locations of alternate telecommunications vendors facilities (such as central offices, switch centers, etc.);
* Contracted capacity of alternate telecommunications;
* SLAs or other agreements for implementation of alternate telecommunications capacity;
* Information on alternate telecommunications vendor contingency plans;
* Names and contact information for those persons authorized to implement or use alternate telecommunications capacity; and
* Other information as appropriate.

## APPENDIX G Diagrams (IT Service and Input/Output)

<NOTE: Include any IT Service architecture, input/output, or other technical or logical diagrams that may be useful in recovering the IT Service. Diagrams may also identify information about interconnection with other IT Services.>

## APPENDIX H HARDWARE AND SOFTWARE INVENTORY

<Provide the hardware and software inventory for the IT Service. Inventory information should include type of server or hardware on which the IT Service runs, processors and memory requirements, storage requirements, and any other pertinent details. The software inventory should identify the operating IT Service (including service pack or version levels, and any other applications necessary to operate the IT Service, such as database software).>

## APPENDIX I INTERCONNECTIONS TABLE

<NOTE: This appendix includes information on other IT Services that directly interconnect or exchange information with the IT Service. Interconnection information should include the type of connection, information transferred, and contact person for that IT Service.>

<If the IT Service does not have any direct interconnections, then this appendix may be removed, or the following statement may be used:>

[IT Service name] does not directly interconnect with any other IT Service.]

## APPENDIX J TEST and Maintenance SCHEDULE

<All ISCPs should be reviewed and tested at the organization defined frequency (e.g. yearly) or whenever there is a significant change to the IT Service. Provide information and a schedule for the testing of the IT Service. The full functional test should include all ISCP points of contact and be facilitated by an outside or impartial observer. A formal test plan is developed prior to the functional test, and test procedures are developed to include key sections of the ISCP, including the following:

Notification procedures;

IT Service recovery on an alternate platform from backup media;

Internal and external connectivity; and

Reconstitution procedures.

Results of the test are documented in an After Action Report, and Lessons Learned are developed for updating information in the ISCP.

NOTE: Full functional tests of IT Services normally are failover tests to the alternate locations, and may be very disruptive to IT Service operations if not planned well. Other IT Services located in the same physical location may be affected by or included in the full functional test. It is highly recommended that several functional tests be conducted and evaluated prior to conducting a full functional (failover) test.

Examples of functional tests that may be performed prior to a full functional test include:

Full notification and response of key personnel to recovery location;

Recovery of a server or database from backup media; and

Setup and processing from a server at an alternate location.

The following is a sample of a yearly test and maintenance schedule for a high-impact IT Service: >

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Step | Date Due by | Responsible Party | Date Scheduled | Date Held |
| Identify failover test facilitator. | March 1 | IT Service Manager |  |  |
| Determine scope of failover test (include other IT Services?). | March 15 | IT Service Manager, Test Facilitator |  |  |
| Develop failover test plan. | April 1 | Test Facilitator |  |  |
| Invite participants. | July 10 | Test Facilitator |  |  |
| Conduct functional test. | July 31 | Test Facilitator, IT Service Manager, POCs |  |  |
| Finalize after action report and lessons learned. | August 15 | IT Service Manager |  |  |
| Update ISCP based on lessons learned. | September 15 | IT Service Manager |  |  |
| Approve and distribute updated version of ISCP. | September 30 | ISCP Director, IT Service Manager |  |  |

## APPENDIX K ASSOCIATED PLANS AND PROCEDURES

<NOTE: ISCPs for other IT Services that either interconnect or support the IT Service should be identified in this appendix. The most current version of the ISCP, location of ISCP, and primary point of contact (such as the IT Service Manager) should be noted. >

## APPENDIX L BUSINESS IMPACT ANALYSIS

<The Business Impact Analysis results should be included in this appendix.>

Texas A&M IT Business Impact Analysis (BIA) Spreadsheet list personnel responsible for executing or supporting system recovery and reconstitution. The following Tabs of the spreadsheet contain;

* 3 Unit Level Assessments - IT Service Name\*, Business Function or Group\*, Essential IT Service\*, Mission Critical\*, RTO \*, RPO\*, Engineered Redundant\*, Recovery Tier, Priority for Restoration, and Comments
* 4 IT Services - IT Service Name \*, Business Function or Group \*, Description \*, Service Owner\*, Service Manager\*, Application Support, VM Support, Hardware/OS Support, Customer Support, and Vendor(s)
* 5 Dependencies - IT Service Name\*, VM / Hardware Provider\*, Restoration Type\*, Equipment Type\*, Primary Locations\*, Second Locations, Other Locations, Backup Copy Location\*, Backup Service, Database Type, Database Provider, Upstream Dependencies, Downstream Dependencies, and Primary Communication Channel

## APPENDIX M DOCUMENT CHANGE PAGE

Modifications made to this plan since the last printing are as follows:

|  |  |  |  |
| --- | --- | --- | --- |
| **Record of Changes** | | | |
| **Page No.** | **Change Comment** | **Date of Change** | **Signature** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Index

IT Service Manager, 3

# 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.

**Maximum Tolerable Downtime**

* The amount of time mission/business process can be disrupted without causing significant harm to the organization’s mission.

**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.

|  |  |  |  |
| --- | --- | --- | --- |
| **RECORD OF CHANGE** | **DATE OF**  **CHANGE** | **DESCRIPTION OF CHANGE** | **CHANGE MADE**  **BY:** |
| 1.0 | 8/10/17 | Change “system” to IT Service and positions to TAMU positions | Peter Walsh |
|  |  |  |  |
|  |  |  |  |

Figure : XXXX

Table : XXXX