

<Project Name>

Disaster Recovery Plan

**Version: <Type Version #>**

 **Date:**

 **Prepared by:**

Project Manager

 **Approved by:**

Project Sponsor

 **Approved by:**

Agency CIO

 **Approved by:**

Executive Sponsor

**Table of Contents**

[**1**](#_30j0zll) **Introduction 4**

[1.1](#_3znysh7) Overview Of Software/System 4

[1.2](#_2et92p0) Intended Audience 4

[**2**](#_tyjcwt) **Business Impact Analysis 4**

[2.1](#_3dy6vkm) Scope 5

[2.2](#_1t3h5sf) Critical Timeframe 5

[2.3](#_4d34og8) System Impact Statements 5

[**3**](#_2s8eyo1) **Recovery Strategy 7**

[3.1](#_3rdcrjn) Recovery Approach 7

[3.2](#_26in1rg) Escalation Plans 7

[3.3](#_lnxbz9) Action Plans 8

[**4**](#_35nkun2) **Disaster Recovery Organization 8**

[4.1](#_44sinio) Recovery Organization Chart 9

[4.2](#_z337ya) Recovery Team 9

[**5**](#_1y810tw) **Program Execution 9**

[5.1](#_4i7ojhp) Recovery Management 9

[5.2](#_2xcytpi) Damage Assessment/Salvage 9

[5.3](#_3whwml4) Physical Security 10

[5.4](#_qsh70q) Hardware Installation 10

[5.5](#_1pxezwc) Systems, Applications and Network Software 11

[5.6](#_2p2csry) Frequently Asked Questions 11

[**6**](#_3o7alnk) **References 11**

[**7**](#_23ckvvd) **Acronyms and Definitions 12**

**Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Description | Author |
| XX/XX/XXXX | 0.00 | Baseline  | <First Name, Last Name> |
|  |  |  |  |

**Template Overview and Instructions:**

The intent of this document is to provide assistant in writing a Disaster Recovery Plan in the event of an interruption in continuous service resulting from an unplanned and unexpected disaster. The Disaster Recovery Plan preparation process includes several major steps as follows:

* Identify Systems and Applications currently in use.
* Analyze Business Impact of computer impact and determination of critical recovery time frames.
* Determine Recovery Strategy
* Document Recovery Team Organization
* Document Recovery Team Responsibilities
* Develop and Document Emergency Procedures
* Document Training & Maintenance Procedures.

# Introduction

<Describe and introduction to the document and its purpose>.

*For Example:*

*The Recovery plan is composed of several sections that document resources and procedures to be used if a disaster occurs. Each supported computing platform has a section containing specific recovery procedures. There are also sections that document the personnel that will be needed to perform the recovery tasks and an organizational structure for the recovery process.*

## Overview Of Software/System

<Describe a high-level overview of the original system/software application and its functionality. The overview should be oriented towards describing how the system or application solves the user’s problems or enables the user to accomplish their goal or mission. Functionality descriptions should be kept at a high level with more detailed explanations save for the program details section of the document.>

*For Example:*

*Application provides an analytical capability for medical planners. Using the application, medical planners determine the level and scope of medical support needed for an operation. The application allows medical planners to estimate and plan theater medical requirements and to develop and evaluate courses of action (COAs) for probable scenarios. The application has two main analytical functions. One function is to estimate medical supportability and sustainability requirements; this is performed by the requirements estimator. The other function is to assess medical supportability and sustainability capability; this is performed by the course-of-action analysis (COAA) tool. The matrix below defines terms used to describe various forms of assessment of medical readiness.*

## Intended Audience

< Provide a brief description of the intended audience for the Disaster Recovery Plan. Description can be kept at a high level but should include enough relevant information for the reader to determine whether the document was meant to address his or her specific needs.>

# Business Impact Analysis

< Enter a high-level description of the overall objective of the business impact analysis.>

*Examples below:*

*The purpose of the business impact analysis (BIA) was to help Sample Systems (SAMPLE) identify which business units, operations and processes are essential to the survival of the business. The BIA will facilitate the identification of how quickly essential business units and/or processes must return to full operation following a disaster situation. It will delineate the business impact of disaster impact scenarios on the ability to deliver product or to support mission-critical services. The BIA will also facilitate the identification of the resources required to resume business operations to a survival level.*

## Scope

<Define the scope of the Business Impact Analysis.>

*For Example:*

*The scope includes the following business units and shared services:*

* *Corporate Communications*
* *Engineering*
* *Facility Services*
* *Finance (Including AP and Payroll)*
* *Human Resources (Including Benefits, Employee Training, Safety/Risk Management)*
* *Marketing (Including Customer Care, Sales)*
* *Materials Management*
* *Operations*
* *Purchasing*
* *Mandated Requirements*

## Critical Timeframe

<Define the critical timeframes in terms of the effect of the services or functions of the system or software.>

*For Example:*

The following table can be used for each critical function or capability.

|  |
| --- |
| **Effect on Service** |
| Time | Effect on Service |
| First 24 Hours |  |
| 24-48 Hours |  |
| Up to 1 Week |  |
| Up to 2 Weeks |  |

## System Impact Statements

<Describe the operational impact of the system or software being unavailable. The impact value is an indication of the severity of the impact to the organization if the function or capability is unavailable. You should also include any findings the impact the organizations’ ability to restore loss functionality or capability, or that further support the impact value rating.>

*For Example:*

Operational impacts are rated on a scale of 0-4 where 0 = no impact and 4 = severe impact. The impact value is an indication of the severity of the impact to the company that would result if the business unit were unable to function.

|  |  |
| --- | --- |
| Operational Impact | Value |
| Cash Flow |  4 |
| Competitive Advantage |  2 |
| Shareholder Confidence |  2 |
| Financial Reporting |  4 |
| Industry Image |  2 |
| Employee Morale |  4 |
| Customer Service |  2 |
| Employee Resignations |  4 |
| Vendor Relations |  4 |
| Regulatory |  3 |
| Increases in Liability |  4 |
| Other |  0 |

The number of recovery personnel by day represents the number of internal personnel resources that the business unit may require to support minimal essential operations following a major disruption.

Number of Recovery Personnel by Day for Finance

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Day 1 | Day 2 | Day 3 | Day 4 | Day 5 | Day 6 | Day 7 | Day 14 | Day 21 | Day 28 |
| 13 |  13 |  18 |  18 |  22 |  22 |  22 | 22 | 28 | 28 |

* Findings
* Finance reported that it is difficult to recover.
* Finance reported that they are somewhat vulnerable to an outage.
* Finance reported that it would take six to 12 hours to complete the backlog of work for each day of outage.
* Finance reported that one week is the maximum length of outage before a significant impact SAMPLE occurred.
* Finance reported that severe operational impacts would occur during the month of December because of year-end payroll processing. Impacts are also significant during April, July, and October due to quarter-end and January and February for year-end.
* Finance stated that SAMPLE must transmit payroll information to ADP (third party processor) by Tuesday to avoid penalties
* Finance stated that while some payments (such as from some federal agencies) are made electronically and via credit card, most payments are received in the form of checks.
* Finance stated that a loss of communications would have a significant impact on business operations.
* Retention policies are followed, and records are stored both on- and off-site*.*

# Recovery Strategy

## Recovery Approach

<Outline the approach that will be used by the organization to recover from a disaster.>

*Example:*

*There are two types of recovery strategy. Depending on the severity of the disaster and the condition of the facilities and computer systems, it is feasible to have recovery of both areas in one location or in separate locations. They are not dependent on each other. Recovery for both can occur simultaneously at different locations.*

* *Level I: Short-Term Outage (less than 48 hours) – Ride-it-Out*
* *Level II: Mid-Term Outage (48 hours to 6 weeks) – Execute formal disaster recovery strategy which will include declaring a disaster and going to an alternate site.*
* *Level III: Long-Term Outage (6 weeks or more) – Execute formal disaster recovery strategy (Level II), and it may involve permanently making a physical move of the District Court’s personnel, resources, and daily*

## Escalation Plans

<Describe the methodology or approach that will be used to escalate the severity of the disaster on the given system or software.>

*For Example:*

*Once a disaster is declared based on the initial levels of outage as defined previously, the Main Campus immediately goes to Level I outage. In this section, the Main Campus must define the levels of outage that are acceptable and at what time (length of outage) to escalate to the next level.*

*Escalation to Level II Outage will occur if:*

*Define criteria and time outage to escalate to Level II – For instance, a hurricane hits and destroys the building. Building access is off-limits for 3 weeks. The Campus needs to escalate to this level of outage with pre-defined steps to take. Operations must be moved to offsite/hot-site recovery. This needs to be defined here.*

*Escalation to Level III Outage will occur if:*

*Define criteria and time outage to escalate to Level III – For instance, the building is deemed inoperable, and employees are not allowed back into the building for over two months. This means the Campus must execute the plan to begin move operations permanently. This needs to be defined here.*

*At any time after the disaster is escalated beyond Level I, the Main Campus needs to consider off-site recovery of daily operations.*

## Action Plans

< Detail in this section the plan of action that will be taken once a disaster has occurred.>

*For Example:*

*Incident Response Process*

* *Notice of problem occurs. Problems may be reported in a variety of ways, including phone or email to management personnel or staff. HQ IT uses a Service Center to receive and response to problems during the daytime hours. After hours, critical areas have staff on-call to resolve problems. In this context, usually an on-call person or the help desk will be notified that a problem exits. At this point the seriousness of the issue or incident has not been identified.*
* *Initial problem assessment. Performed by the support or on-call person in the relevant area.*
* *Initial problem resolution (see glossary for definitions of categories):*
* *If the incident is a category 1, routine incident, it is usually resolved and completed at this stage, using normal help desk or on-call procedures.*
* *If the incident is a category 2 or 3 incident, the team management unit(s) is notified by the help desk (during the day) or by the on-call person who originally received the notification (after hours). This will be the infrastructure team (for Windows, UNIX, Network or Voice issues), the Database team (for Database issues), the Security team (for Security issues), the Applications team (for application issues), or the Web team (for web and SharePoint issues). The team member working on the issue will contact his appropriate management unit to escalate the incident and begin the assessment process. This will allow other personnel resources to be brought in to assist with assessing the incident, if necessary.*
* *If the incident is a category 4 disaster, the head of IT in the office and the Local IT Disaster Recovery coordinator shall be notified and the Dorchester procedures will be followed*.

# Disaster Recovery Organization

< List the relevant information for the member of the disaster recovery team.>

*For Example:*

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Name** | **Project Role** | **Recovery Role** | **E-mail** | **Work Phone** | **Cell Phone** | **Primary/Secondary** |
|   |   |   |   |   |   |   |
|   |  |  |  |  |  |  |
|   |  |  |  |  |  |  |
|   |  |  |  |  |  |  |
|   |   |   |   |   |   |   |

## Recovery Organization Chart

<Insert an org chart of the disaster recovery team>

## Recovery Team

<List all recovery team roles and responsibilities.>

*For Example:*

|  |  |
| --- | --- |
| **Role** | **Responsibilities** |
|   |   |
|   |  |
|   |  |
|   |  |
|   |  |
|   |   |

# Program Execution

## Recovery Management

< Describe how the management of the recovery process will be handled.>

*For Example:*

*If a "disaster" occurs computing and networking services, the Management Team will be responsible for the disaster recovery process. The group must establish an adequate information processing and networking environment to support fundamental business and support activities. Functional areas that have local information processing operations will be responsible for their disaster recovery paradigm(s). The Management Team will be responsible for making decisions and determining directions based on information received from the Damage Assessment Team.*

*The Management Team will interface with all constituents to inform them of status of the disaster and direct recovery activities.*

## Damage Assessment/Salvage

<Describe in detail the damage assessment process and what the guidelines are for salvaging information and/or equipment.>

*For Example:*

*The process for determining the extent of the disaster and what is required to reestablish the computing and networking services is as follows:*

1. *The operations staff that is on duty will notify the Manager of Information Technology Systems that a disaster has occurred. If no operations personnel are on duty, then notify the Assistant Director of Information Technology Systems so they can assemble the Damage Assessment Team. If the building or the wing that houses the computer center is destroyed, the recovery team will be assembled immediately. The facilities management staff and capital projects people will develop the plan for restoring the building. The initial action will be to determine if the storage vault is in- tact. Efforts will be undertaken to provide access to the vault just in case some of the contents are needed for the recovery of the computing center.*
2. *The Director of the Information Technology Systems will assemble the Disaster Assessment Team. This team will determine the severity of the disaster by collecting the following information as outlined below. If the building or wing was destroyed, the Director of Information Technology Systems will assemble the Recovery Team instead of the Damage Assessment Team.*

*Damage Assessment Team.*

* *If operations staff were on duty, the status of personnel will be determined. Immediate notification will be given to Special Assistant for appropriate actions.*
* *Preliminary assessment of what is required to become operational*
* *To what extent essential resources were damaged?*
* *Is the on-site storage vault assessable?*
* *Is an alternate site required?*

*The Damage Assessment Team will determine the status of each administrative system, especially the Financial Records (FRS). If access to the computer room is denied due to the extent of damages, this team will terminate all efforts and the Recovery, and the Management Teams will be notified.*

## Physical Security

<Describe how the management of Physical Security will occur. How will the protection of personnel, hardware, software, networks and data from physical actions and events that could cause serious loss or damage to an enterprise, agency or institution be handled This includes protection from fire, flood, natural disasters, burglary, theft, vandalism, and terrorism.>

## Hardware Installation

<Describe the procedures required for performing hardware installation in support of disaster recovery efforts.>

*For Example:*

*If computer rooms or equipment become unusable, Information Technology Center (ITC) might have to find temporary floor space and replacement equipment to recover operations. The plan takes from five to eight days to execute, and it calls for all enterprise applications to be restored. It addresses a "worst" case disaster scenario. Users of ITC's enterprise applications must be prepared to function on their own for this length of time. (Processing an emergency payroll has been arranged, without needing the enterprise servers.)*

*(a) Hardware Configuration*

|  |  |
| --- | --- |
| *Server Type* |  |
| *Computer Model* |  |
| *RAM Memory* |  *3840 MB*  |
| *No. of CPU’s* |  *4*  |
| *Processor Type & Speed* |  |
| *Hard Disk Space* |  |

## Systems, Applications and Network Software

<Describe any steps that must be taken to facilitate the recovery of any addition systems, applications or networks that are not necessarily a part of the main system or software.>

*For Example:*

*Recovery time estimates for Unix systems vary depending on the severity of outage. If a few systems supporting services were lost, the Unix Recovery Team could reallocate and reconfigure systems within a few hours. However, if many systems were lost, replacements would need to be procured, and the recovery task could take from several days to more than a week.*

*ITC supports the data/video network and the network server infrastructure. Unlike the enterprise servers, networking is distributed, with switching equipment located in small areas in many user buildings and in central distribution points. Widespread equipment distribution and the number of components (along with the severity of the event) make Network recovery projections vary substantially. The Detailed Network Recovery Plan estimates as few as four hours for recovering from a minor event, to several days or weeks for a major event (where switching equipment and cable plant leading to the equipment are destroyed).*

## Frequently Asked Questions

<This section presents to the user frequents questions about the recovery of the system/program and the common answers to those questions. It can be formatted a variety of different ways to include a numbered listing of questions, questions grouped by functions, questions grouped by user types and so forth. References.>

# References

<This section contains any all-reference material used in the creation of the Disaster Recovery Plan or required for the operation of the system or program. It should include websites, system documents, references to other systems and their documents and any other document that was either used in the creation of the manual, referenced in the manual, or provides addition information useful to the user.>

**Table 1: References**

|  |  |
| --- | --- |
| **Document Number** | **Document Title** |
|  |  |
|  |  |

# Acronyms and Definitions

**Table 2: Acronyms and Definitions**

| **Acronym** | **Description** |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |