January 1, 20XX

ABC Company

123 Main Street

Los Angeles, CA 90744

(800) ABC-COMP

[www.ABCCompany.com](http://www.ABCCompany.com)

Table of Contents

[I. Purpose of the Backup Plan 3](#_Toc365554540)

[II. Overview of the Backup Plan 3](#_Toc365554541)

[III. Business Continuity Objectives 4](#_Toc365554542)

[IV. Responsibilities 5](#_Toc365554543)

[V. Backup Procedures 6](#_Toc365554544)

[VI. Storage of Backups 9](#_Toc365554545)

[Exhibit A – Archiving and Rotation Schedule 10](#_Toc365554546)

# I. Purpose of the Backup Plan

The purpose of this Backup Plan (Plan) is to document the processes related to backing up of ABC Company’s Information Systems, storing of backup information, testing of backups, and security related to backups.

# II. Overview of the Backup Plan

This Plan documents our structured process of ensuring system availability and our ability to recover Information Systems from backups. Backups are used to provide corrective action against various types of threats including:

* Human error – a user accidentally deletes a file.
* Malicious software – a virus deletes files or corrupts systems and data.
* Intentional actions – a hacker deletes files.
* Hardware failure – a hard drive fails and files must be deleted.
* Application processing errors – a database is corrupt and must be restored.
* Facility issues – a fire, water pipe, or electrical surge damages equipment.

This Plan was developed to ensure:

* Business recovery objectives can be achieved.
* Backup solutions are scalable and can adapt to a changing business environment.
* Backups are robust and can be used to restore information when needed.
* Responsibility for ensuring sufficient and effective backups.
* Information systems and related data are properly identified so that they can be backed up.
* The location of backups has been properly identified along with the individuals who have access to the backups.
* Procedures to restore systems from backups are complete and maintained.
* Backups are periodically tested to ensure they are reliable and contain the necessary information.

ABC Company’s Backup Policy provides direction and guidance to this Plan and related activities.

# III. Business Continuity Objectives

ABC Company is committed to protecting its business operations, investments by its stakeholders, and assets of the organization. Risks assessments are used as a tool to help identify and mitigate risks to assets. ABC Company’s Risk Assessment Policy specifies that the risk assessment, risk analysis, and risk treatment plan shall be reviewed on an annual basis to ensure that controls are sufficient and effective at treating risks.

Our recent risk assessment identified important Information Systems. Our most recent Business Impact Analysis, part of our business continuity process, identified important Information Systems as well as our required recovery time objectives (acceptable downtime) and recovery point objectives (acceptable data loss).

Backups are an important part of providing Information System availability and are critical to ABC Company’s business continuity. Per the Backup Policy, the Chief Security Officer (CSO) has performed a review and analysis of our Business Impact Analysis and costs and determined that ABC Company shall operate at Tier 2: Data backups with hot site. See the Backup Policy for more information about the recovery Tiers.

# IV. Responsibilities

The IT Director has been assigned the responsibility of implementing and managing ABC Company’s Backup Plan and related processes and procedures. The IT Director delegates some or all of the following backup related responsibilities to a Backup Coordinator:

* Requirements – systems to be backed up, acceptable downtime, acceptable data loss.
* Documentation – maintain a record of backup related documentation including flow charts, locations of backups, use of backup/recovery third party service providers, backup requirements, individuals with access to backup media, personnel contacts, etc.
* Procedures – backup procedures used to ensure business continuity and recovery objectives are achieved.
* Integrity – review testing of backups to ensure they are complete, reliable, and error free.
* Recommendations – recommendations to enhance the Backup Policy and/or Plan.

The IT Director periodically reviews the most recent Business Impact Analysis and the above information maintained by the Backup Coordinator to ensure:

* Backup solutions meet recovery Tier and Business Impact Analysis requirements.
* Backup solutions are scalable and can adapt to a changing business environment.
* Backup are robust and can be used to restore information when needed.
* Information systems and related data are properly identified so that they can be backed up.
* The location of backups has been properly identified along with the individuals who have access to the backups.

On an annual basis the IT Director makes available to Data Owners an overview of the Backup Procedures to make them aware of recovery times and possible data loss. Data Owner concerns are brought to the attention of the CSO as a part of the annual evaluation of the recovery Tier, data loss and recovery time implications, and related costs.

# V. Backup Procedures

A. Overview

The IT Operations Department is responsible for developing and maintaining backup procedures. Such procedures include:

* Scheduling backups and troubleshooting backup issues.
* Monitoring backups and related log files.
* Documenting backup success/fail.
* Notifying the System Administrator of any issues that require attention (e.g. failed backups, capacity issues, time to backup files, etc.).
* Defining procedures and creating documentation for sending backups off-site.
* Maintaining the Backup Log Form of all backup media including their location and, if off-site, when backup is expected to return on-site.

ABC Company performs a full back up each evening for all important systems identified in the Business Impact Analysis. This ensures:

* *Integrity*. Since all important systems are backed up at the same time, transaction integrity between databases is achieved.
* *Recovery time*. Since all backups are full backups, no incremental backups are performed. This speeds recovery times as IT Operations Staff does not need to first restore from a full backup and then restore files from one or more incremental backups.

Full backups have the following constraints that are monitored by IT Operations Staff and the Backup Coordinator:

* *Capacity*. Since backups run unattended without operators present, sufficient storage capacity needs to be allocated for backups/media.
* *Time*. Backups generally start in the evening. To ensure integrity, they must complete before Staff returns to work the next day.

B. Archiving and Retention

ABC Company employs a robust backup and archiving scheme that protects against malware and other types of threats. A minimum of 14 backups are maintained at any point in time. Exhibit A – Archiving and Rotation Schedule documents our labeling, archiving, and rotation schedule.

Examples of backups:

* Monday – each Monday IT Operations will use the Monday backup. This backup is retained on-site. This media is overwritten the following Monday.
* 1st Friday – the 1st Friday of the month IT Operations uses the Friday 1 backup. The following work day it is taken to off-site storage. This backup is returned to IT Operations when the 2nd Friday backup is stored off-site. This backup is overwritten the 1st Friday of the following month.
* Month 1 – monthly backups are stored off-site until they are needed. IT Operations creates the Month 1 backup the last working day of the first month of each quarter (January 31, April 30, July 31, October 31). The following work day Month 1 is taken to off-site storage where it remains until it is needed again.
* Quarter 1 - quarterly backups are stored off-site until they are needed. IT Operations uses the Quarter 1 backup the last working day of each quarter (March 31, June 30, September 30). The following work day it is taken to off-site storage where it remains until it is needed again.
* Year end – year end backups are created the last working day of the year. They are stored off-site and retained per the Data Retention Policy. Year end backups are not overwritten or reused.
* Special – the IT Director may occasionally authorize Special or one-time backups be created. Examples include backups prior to IT hardware/software upgrades and moving equipment that contains important systems or data as identified in the Business Impact Analysis. IT Operations Staff is responsible for creating Special backups that contain retrievable exact copies of systems.

C. Off-site Storage

The CSO has determined that risks due to human error, hacker, equipment failure, or database integrity issues are more likely than environmental issues such as fire or flood. As a result, the IT Director has specified, with the approval of the CSO, that the most recent backups be stored on‑site.

* Monday through Thursday backups are always maintained on-site and reused the following week.
* Friday backups are rotated off-site. Only the most recent Friday backup is stored off-site. The remaining Friday backups are stored on-site.
* Monthly backups are stored off-site until they are needed and ready to be overwritten.
* Quarterly backups are stored off-site until they are needed and ready to be overwritten.
* Year end backups are stored off-site until disposal (never overwritten).

D. Disposal Procedures

Backups are retained according to Section V.B. Archiving and Retention. When backups are no longer needed and/or reach the end of their useful life, they are disposed of per ABC Company’s Disposal Policy.

E. Testing Backups

Testing provides assurance that backups are complete and error free. Testing can identify the following types of problems and issues:

* Inability to restore from older media (size, poor quality, too old, not properly stored).
* Current backup software cannot read old backups.
* Applications or data were not stored on original backups.
* Encryption or key management issues (can’t read encrypted backups).

Twice each year the IT Director authorizes a test of backups and backup procedures. IT Operations Staff prepares a Test Case Scenario including:

* Test objectives – systems and/or applications to be tested.
* Tasks – detailed tasks needed to perform the test.
* Resources – resources required including timeframe, Information Systems, Staff (IT and users), backups, anticipated costs, etc.
* Validation – expected outcomes and validation processes.

Once the Test Case Scenario is approved by the IT Director, IT Operations Staff:

* Schedules – reserves Information Systems for testing and coordinates with user departments (if needed).
* Documentation – assembles system restore documentation, flowcharts, and any other documentation needed by IT Operations Staff.
* Resources – assembles backups used for the Test Case Scenario.
* Restore – restores systems according to documented procedures and the specific Test Case Scenario.
* Validation – documents actual events and compares with expected outcomes. Performs validation procedures identified in the Test Case Scenario. Involves users as needed to validate a successful restore.

Within one week of testing, IT Operations Staff prepares and delivers a report to the IT Director. Such report includes:

* An overview of the Test Case Scenario.
* Expected outcomes.
* Actual outcomes and other variances.
* Recommendations to enhance backup and recovery processes.

Based upon the testing results, the IT Director may recommend changes to the Backup Policy, this Plan, and/or backup/recovery procedures.

# VI. Storage of Backups

A. On-site Backups

Backups that are stored on-site are located in a safe and secure room restricted to IT Operations Staff, the IT Director, and Backup Coordinator (collectively termed Authorized Individuals). The list of Authorized Individuals is reviewed by the IT Director at least annually to ensure it is relevant and sufficient.

To meet the specified Recovery Time Objectives outlined in the Business Impact Analysis, on-site backups are immediately available to Authorized Individuals.

Backups are encrypted to protect against theft and unauthorized access.

B. Off-site Backups

Backups stored off-site meet the following requirements:

* Annual review by IT Director or designate to ensure the environment is suitable for storing ABC Company backups.
* Backups are encrypted to protect against theft and unauthorized access.
* Backups are stored in a safe and secure environment.
* Access to backups is restricted to authorized personnel approved by the IT Director or designate.
* The off-site environment allows ABC Company to meet or exceed specified Recovery Time Objectives outlined in the Business Impact Analysis.

Off-site backup/recovery third party service providers are cleared to handle the highest level (see Data Classification Policy) of information stored.

# Exhibit A – Archiving and Rotation Schedule

|  |  |  |
| --- | --- | --- |
| **Label and Description** | **Retention** | **Location** |
| Monday – backup performed each Monday | 1 week | Always on-site |
| Tuesday – backup performed each Tuesday | 1 week | Always on-site |
| Wednesday – backup performed each Wednesday | 1 week | Always on-site |
| Thursday – backup performed each Thursday | 1 week | Always on-site |
| Friday 1 – backup performed 1st Friday of each month | 1 month | Rotated off-site |
| Friday 2 – backup performed 2nd Friday of each month | 1 month | Rotated off-site |
| Friday 3 – backup performed 3rd Friday of each month | 1 month | Rotated off-site |
| Friday 4 – backup performed 4th Friday of each month | 1 month | Rotated off-site |
| Friday 5 – backup performed 5th Friday of each month | 1 month | Rotated off-site |
| Month 1 – backup performed end of month, 1st month of quarter | 3 months | Stored off-site |
| Month 2 – backup performed end of month, 2nd month of quarter | 3 months | Stored off-site |
| Quarter 1 – backup performed last day of 1st quarter (March 31) | 1 year | Stored off-site |
| Quarter 2 – backup performed last day of 2nd quarter (June 30) | 1 year | Stored off-site |
| Quarter 3 – backup performed last day of 3rd quarter (Sept 30) | 1 year | Stored off-site |
| Year End – backup performed on December 31 | 7 years | Stored off-site |
| Special – OS upgrades, data conversions, moving equipment, etc. | Varies | Always on-site |