**<Client Name>**

**Data Backup Plan Template**

 ****

**Revisions Control Page**

|  |  |  |
| --- | --- | --- |
| **Date** | **Summary of Changes Made** | **Changes Made By (Name)** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Purpose

The purpose of this data backup plan is to ensure that <Client> can safely and securely back up mission-critical data, systems, databases and other technology so that it will be available in the event of a disruption affecting business operations. All <Client> locations are expected to implement data backup measures whenever possible to minimize operational disruptions and to recover as rapidly as possible when an incident occurs.

The plan encompasses <Client> data backup operations in all locations.

## Scope

The scope of this plan is limited to data backup activities, and is not a daily problem resolution procedures document.

## Plan Objectives

* Serves as a guide for <Client> IT data backup teams
* References and points to the location(s) of backed-up data, systems, applications and other mission-critical data resources
* Provides procedures and resources needed to back up data, systems and other resources
* Identifies vendors and customers that must be notified in the event of a disruption that may necessitate recovering backed-up data and other resources
* Minimizes operational disruptions by documenting, testing and reviewing data backup procedures
* Identifies alternate sources for data backup activities
* Documents data storage, backups and retrieval procedures for vital records and other relevant data

## Assumptions

* Key IT data backup employees (e.g., lead data backup administrator, team leaders, technicians and alternates) will be available following a disaster.
* This plan and related documents are stored in a secure off-site location and not only survived the disaster but are accessible immediately following the disaster.
* The IT organization will have technology disaster recovery (DR) plans that align with this data backup plan.

## Disaster Definition

A disaster is any disruptive or catastrophic event (e.g., power outage, weather, natural disaster, vandalism) that causes an interruption in technology relating to data, databases, systems, archived data and other resources provided by <Client> IT operations.

## Data Backup and Related Teams

* Data Backup Team
* IT Technical Support Team

See Appendix A for details on the roles and responsibilities of each team.

##

## Team Member Responsibilities

* Each team member will designate an alternate/backup.
* All team members should keep an updated calling list of team members’ work, home and cell phone numbers both at home and at work.
* All team members should keep this plan for reference at home in case a disruption occurs after normal work hours.
* All team members should familiarize themselves with the contents of this plan.

**Backup Policy**

Full and incremental backups protect and preserve corporate network information and should be performed on a regular basis for system logs and technical documents that are not easily replaced, have a high replacement cost, or are considered critical. Backup media should be stored in a secure, geographically separate location from the original and isolated from environmental hazards. Backup network components, cabling and connectors, power supplies, spare parts and relevant documentation should be stored in a secure area on-site as well as at other corporate locations.

Data and document retention policies are established to specify what records must be retained and for how long. All departments are responsible for specifying their data management, data retention, data destruction and overall records management requirements.

IT Technical Support follows these standards for data backup and archiving:

**System Databases**

* A copy of the most current mission-critical databases must be made at least twice per month, or based on frequency of changes made.
* Backups must be stored off-site.
1. The lead data administrator is responsible for this activity.

**Mission-Critical Data**

* Current mission-critical data and databases must be backed up according to the established recovery point objectives (RPOs), and must be mirrored or replicated to secure backup locations within the RPO time frames.
* Backups must be stored off-site at one or more secure cloud locations or at alternate company data centers or offices, or a combination of these.
1. The lead data administrator is responsible for this activity.

**Non-Mission-Critical Data**

* Current non-mission-critical data and databases must be backed up according to the established RPOs, and can be mirrored or replicated to secure backup locations within the RPO time frames.
* Alternatively, copies of current data and databases must be made at least twice per week, or based on RPO metrics or the frequency of changes made.
* Backups may be stored on-site in secure storage facilities, or stored off-site at one or more secure cloud locations or at alternate company data centers or offices, or a combination of these.
1. The data administration team is responsible for this activity.

Backup media are stored at locations that are secure, isolated from environmental hazards, and geographically separate from the location housing network components.

**Off-site Storage Procedures**

* Tapes and disks, and other suitable media are stored in environmentally secure facilities.
* Tape or disk rotation occurs on a regular schedule coordinated with the storage vendor.
* Access to backup databases and other data is tested annually.

**Tapes (if used)**

1. Tapes greater than three years old are destroyed every six months.
2. Tapes less than three years old must be stored locally off-site.
3. The system supervisor is responsible for the transition cycle of tapes.

### Performing Data Backups

Data backups are to be scheduled daily, weekly and monthly depending on the nature of the backup. Data administrators are to use the approved data backup technology to prepare for, schedule, execute and verify backups. Backups may be made to local storage resources (e.g., disk, tape, RAID) locally or to off-site secure locations (e.g., cloud data backup service providers, backup-as-a-service providers) approved by IT management.

**Data Backup Activities**

The following table lists data backup activities to be performed on a regularly scheduled basis.

|  |  |  |
| --- | --- | --- |
|  | **Action** | **Who Performs** |
| 1. | Review program with IT management; secure approvals as needed | Lead data backup admin, Head of IT Ops |
| 2. | Identify and categorize data to be backed up | Lead backup admin; backup team |
| 3. | Identify and categorize systems to be backed up | Lead backup admin; backup team |
| 4. | Identify and categorize other resources to back up | Lead backup admin; backup team |
| 5. | Schedule backup activities, e.g., date, time, frequency, type of resource to back up, destination for backups | Lead backup admin; backup team |
| 6. | Program backup systems and resources according to schedule and policy | Lead backup admin; backup team |
| 7. | Schedule tape backup and rotation activities | Lead backup admin; backup team |
| 8. | Execute backups of data, systems and other resources | Lead backup admin; backup team |
| 9. | Ensure that tapes are secured for pickup and are properly labeled; verify pickup  | Lead backup admin; backup team |
| 10. | Verify that backups were completed and all backed-up resources are unchanged  | Lead backup admin; backup team |
| 11. | Prepare and distribute backup reports | Lead backup admin; backup team |
| 12. | Schedule and conduct tests of data backups | Lead backup admin; backup team |
| 13. | Schedule and perform patching of backup resources | Lead backup admin; backup team |
| 14. | Update backup systems and technologies as needed | Lead backup admin; backup team |
|  |  |  |

## Data Recovery

Procedures are to be established, documented and periodically tested to recover data, databases, systems, applications and other information assets if a disruptive event occurs that necessitates the recovery of those assets and resources.

## Plan Review and Maintenance

This data backup plan must be reviewed periodically and the procedures validated (and updated as needed) to ensure that backups will occur as needed and when needed. As part of this activity, it is advisable to review the listings of data backup team personnel, data backup service vendors and cloud data backup vendors, and update contact details as needed.

The hard-copy version of this data backup plan will be stored in a common location where it can be viewed by IT personnel, such as data administrators. Electronic versions will be available from IT Technical Support.

# Appendixes

##

## Appendix A: Teams

Data Backup Team

Responsible for overall planning, management and execution of data backup activities and providing regular reports to IT management on backup performance according to specific data backup metrics

Support Activities

* Analyzes data backup performance against specific metrics
* Sets backup priorities based on collaboration with IT Technical Support and user departments
* Provides IT management with ongoing status and performance data
* Works with vendors and IT Technical Support to ensure continuous operation of backups

### IT Technical Support (ITS) Team

Supports the performance of data backup and related data storage activities

Support Activities

* Assist with data backup activities as needed
* Provide guidance on equipment, systems and other services, as required
* Coordinate testing of data backup operations to ensure they are functioning normally

## Appendix B: Data Backup Team Contact Lists

### Data Backup Team (DBT)

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Address** | **Home** | **Mobile/Cell Phone** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

### IT Technical Support (ITS) Team

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Address** | **Home** | **Mobile/Cell Phone** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## Appendix C: Approved Vendor Contact List

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Contact** | **Email** | **Mobile/Cell Phone** |
| Backup vendor 1 |  |  |  |
| Backup vendor 2 |  |  |  |
| Backup vendor 3 |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

##

## Appendix D: Data Backup Locations

### Backup Resource 1 – <Location Name>

Primary: Address

 Room

 City, State

Contact:

Alternate: Address

 Room

 City, State

 Contact:

### Backup Resource 2 – <Location Name>

Primary: Address

 Room

 City, State

Contact:

Alternate: Address

 Room

 City, State

 Contact:

### Data Storage Facilities (e.g., Tape, Disk, Clouds, NAS, SAN, RAID)

|  |  |  |  |
| --- | --- | --- | --- |
| **Company Name** | **Contact** | **Work** | **Mobile/Cell Phone** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## Appendix E: Inventory of Data Resources, Databases to Back Up

Provide list of resources

## Appendix F: Inventory of Hardware and Software to Back Up

Provide list of resources

## Appendix G: Inventory of Network Services and Equipment to Back Up

Provide list of resources