**Data Backup Plan Template**

**<Client Name>**

 ****

**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

This plan's scope is limited to data backup activities and is not a document for daily problem resolution procedures.

## 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 might 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.
* Addresses security issues to protect backed-up data from cyberattacks.

## 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 also accessible immediately following the disaster.
* Plan content is available in both hard copy and electronic formats.
* 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, cyberattack, 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.
* All team members must keep themselves up to date on all technical issues associated with data backup, including cloud backup services, advanced storage technologies and other third-party data backup service firms.

**Backup Policy**

Full and incremental backups protect and preserve corporate network information and should be performed on a regularly scheduled 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 (e.g., cloud backup service or other approved data backup service firm) from the original and isolated from environmental hazards and security breaches. 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 must be established to specify what records must be retained, in either hard copy or electronic form, and for how long. All departments are responsible for specifying their data management, data retention, data destruction and overall records management requirements. They are also responsible for assigning and approving data protection metrics, including recovery time objective (RTO) and recovery point objective (RPO).

IT Technical Support acknowledges the following standards and regulations for data backup and archiving:

* [ISO/IEC 27040:2024](https://www.iso.org/obp/ui/#iso:std:iso-iec:27040:ed-2:v1:en).
* [ISO/IEC 27001:2022](https://www.techtarget.com/whatis/definition/ISO-27001).
* [NIST SP 800-171](https://csrc.nist.gov/pubs/sp/800/171/r2/upd1/final).
* General Data Protection Regulation ([GDPR](https://www.techtarget.com/whatis/definition/General-Data-Protection-Regulation-GDPR)).
* Digital Operational Resilience Act ([DORA](https://www.techtarget.com/whatis/definition/What-is-the-Digital-Operational-Resilience-Act-DORA)).
* California Consumer Privacy Act ([CCPA](https://www.techtarget.com/searchcio/definition/California-Consumer-Privacy-Act-CCPA)).
* Health Insurance Portability and Accountability Act ([HIPAA](https://www.techtarget.com/searchhealthit/definition/HIPAA)).
* Sarbanes-Oxley Act ([SOX](https://www.techtarget.com/searchcio/definition/Sarbanes-Oxley-Act)).
* Payment Card Industry Data Security Standard ([PCI DSS](https://www.techtarget.com/searchsecurity/definition/PCI-DSS-Payment-Card-Industry-Data-Security-Standard)).

***System Databases***

* A copy of the most current mission-critical databases must be made at least twice per month or based on the frequency of changes made.
* Backups must be stored off-site, such as at an alternate data center, cloud storage service or other approved third-party data backup service.
* 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 RPOs and must be mirrored or replicated to secure backup locations within the RPO time frames.
* RPO values must be approved by the business unit(s) assigning them.
* Backups must be stored off-site at one or more secure cloud locations, at alternate company data centers or offices, or a combination of these locations.
* Backup frequency and the amount of data backed up must be reviewed with business unit leaders at least monthly.
* The lead data administrator is responsible for these activities.

***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.
* RPO values must be approved by the business unit(s) assigning them.
* Backups might be stored on-site in secure storage facilities, stored off-site at one or more secure cloud locations, at alternate company data centers or offices, or a combination of these locations.
* Backup frequency and the amount of data backed up must be reviewed with business unit leaders at least quarterly.
* The data administration team is responsible for these activities.

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

***Off-Site Storage Procedures***

* Tapes, disks, solid-state storage devices and other suitable media are stored in environmentally secure facilities.
* Backup schedules are coordinated with the IT storage team and are reviewed monthly.
* Tape, disk or solid-state drive (SSD) rotation occurs on a regular schedule coordinated with the storage vendor.
* Access to backup databases and other data is tested annually.
* The data storage team is responsible for these activities.

***Tapes (If Used)***

* Tapes more than 3 years old are destroyed every six months.
* Tapes less than 3 years old must be stored off-site in an approved storage facility.
* The data storage team is responsible for the transition cycle of tapes.

### Performing Data Backups

Data backups are to be scheduled hourly, daily, weekly and monthly, depending on the nature of the backup. Data administrators must use the approved data backup technology to prepare for, schedule, execute and verify backups. Backups might be made to local storage resources (e.g., disk, tape, NAS, SSD, 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 the Action** |
| 1. | Review program with IT management; secure approvals as needed. | Lead data backup admin and head of IT Ops. |
| 2. | Identify and categorize data to be backed up. | Lead backup admin, backup team and business unit. |
| 3. | Identify and categorize systems to be backed up. | Lead backup admin, backup team and business unit. |
| 4. | Identify and categorize other resources to back up. | Lead backup admin, backup team and business unit. |
| 5. | Schedule backup activities, e.g., date, time, frequency, type of resource to back up, destination for backups. | Lead backup admin, backup team and business unit. |
| 6. | Program backup systems and resources according to schedule and policy. | Lead backup admin and backup team. |
| 7. | Coordinate backup activities with third-party data backup vendors, e.g., cloud services, backup-as-a-service. | Lead backup admin and backup team. |
| 8. | Ensure security measures are in place, e.g., data encryption and network security measures to protect data confidentiality, integrity and availability. | Lead backup admin, backup team and cybersecurity team. |
| 9. | Schedule tape backup and rotation activities. | Lead backup admin and backup team. |
| 10. | Execute backups of data, systems and other resources. | Lead backup admin and backup team. |
| 11. | Ensure tapes are secured for pickup and properly labeled; verify pickup. | Lead backup admin and backup team. |
| 12. | Verify that backups were completed and all backed-up resources are unchanged. | Lead backup admin and backup team. |
| 13. | Prepare and distribute backup reports. | Lead backup admin and backup team. |
| 14. | Schedule and conduct tests of data backups. | Lead backup admin and backup team. |
| 15. | Schedule and perform patching of backup resources. | Lead backup admin and backup team. |
| 16. | Update backup systems and technologies as needed. | Lead backup admin and backup team. |

## Data Protection and Recovery

Procedures should be established, documented and periodically tested to ensure all data is fully protected from cyberattacks and other breaches. These procedures will also be used 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, Audit and Maintenance

This data backup plan must be reviewed and audited periodically, and the procedures maintained and updated, to ensure backups occur when needed and that compliance with the required standards and regulations is documented. 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.

Numerous controls can be identified for a data backup audit. The following table lists key backup and recovery audit controls and the evidence required to confirm them.

| **Backup Audit Controls** |
| --- |
| **Backup and recovery audit controls** | **Examples of audit evidence** |
| Data backup and recovery plan. | Documented plan. |
| Data backup and recovery policy. | Documented policy. |
| Data backup and recovery procedures, relevant documentation and forms. | Documented procedures, forms, templates and checklists. |
| Personnel authorized to access data backup and recovery resources. | Documentation of employees authorized to access data backup resources, with details on their credentials, security clearances and more. |
| Data backup and recovery schedules. | Paper copies or screenshots of backup and recovery schedules. |
| Data backup and recovery access elements. | Screenshots of access controls (sign-in and authentication methods). |
| Data backup and recovery reliability metrics. | Screenshots of backup and recovery performance metrics. |
| Data backup and recovery performance metrics for mainframes, servers, network devices, applications, data files and databases. | Documented reports on backup and recovery performance for all IT assets that need to be backed up. |
| Data backup and recovery test plans and documented results. | Copies of recent backup and recovery test plans, performance data from the tests and after-action reports. |
| Backup frequency metrics. | Screenshots of backup schedules showing frequency metrics for each kind of backup. |
| Data backup systems and software. | Operational documentation and relevant screenshots for applications and hardware used for backup and recovery activities. |
| Data backup storage resources -- local (data center). | Operational documentation and relevant screenshots for local storage systems and resources. |
| Data backup storage resources -- off-site (cloud, alternate data center, third-party storage firm). | Operational documentation and relevant screenshots for off-site storage systems and resources. |
| Data backup network services (bandwidth availability, latency). | Operational documentation and relevant screenshots for network services used when transmitting data for backups and recoveries. |
| Data backup and recovery sections of a BCDR plan. | Copies of BCDR plans outlining section(s) that address data backup and recovery activities. |
| Data backup and recovery security activities (data access management, data protection methods, security tools for protecting data). | Copies of BCDR plans outlining section(s) that address data backup and recovery activities. |
| Environmental requirements for data backup and recovery (secure physical site, power, security, HVAC). | Operational documentation and relevant screenshots for backup site physical security (door locks, proximity cards, CCTV), primary and backup power supplies, emergency lighting and exits, primary and backup HVAC systems. |

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

## Continuous Improvement

As part of the ongoing review and maintenance activities, this data backup plan must be continuously improved so that the most cost-effective and secure data backup activities are performed.

# Appendixes

##

## Appendix A: Teams

Data Backup Team

The team is responsible for the 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. The team is also responsible for supporting audit activities and other initiatives designed to improve the overall quality of data backups.

*Support Activities*

* Analyze data backup performance against specific metrics.
* Set backup priorities based on collaboration with IT Technical Support and user departments.
* Provide IT management with ongoing status and performance data.
* Support audit activities addressing data backups.
* Work with vendors and IT Technical Support to ensure the continuous operation of backups.

### IT Technical Support (ITS) Team

The 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** | **Email** | **Home/Cell Phone** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

### IT Technical Support (ITS) Team

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

## Appendix C: Approved Vendor Contact List

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Contact** | **Email** | **Work/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, SSD, Cloud, NAS, SAN, RAID)

|  |  |  |  |
| --- | --- | --- | --- |
| **Company Name** | **Contact** | **Email** | **Work/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