Contents

[1. Introduction to Backup & Recovery Policy……………………………………………………………………………….. 7](#_Toc77247034)

[2. Purpose……………………………………………………………………………………………………………………………………. 7](#_Toc77247035)

[3. Scope……………………………………………………………………………………………………………………………………….. 7](#_Toc77247036)

[4. Policy 7](#_Toc77247037)

[4.1. Data Backup 7](#_Toc77247038)

[4.2. Data Backup Selection 8](#_Toc77247039)

[4.3 Backup Types 8](#_Toc77247040)

[4.4 Backup Storage and Security 9](#_Toc77247041)

[4.5 Recovery of Backup Data 9](#_Toc77247042)

[5. STORAGE MANAGEMENT……………………………………………………………………………………………………… 10](#_Toc77247043)

[6. Business Continuity and Disaster Recovery Planning (BCDR)…………………………………………………. 10](#_Toc77247044)

**DOCUMENT REVISION CONTROL**

REVISION HISTORY

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Author** | **Version** | **Change Reference** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

REVIEWERS

| **Name** | **Position** | **Date** |
| --- | --- | --- |
|  |  |  |
|  |  |  |

DISTRIBUTION

| **Date** | **Distributed to** | **Version** | **Distribution Format** |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

APPROVALS

| **Date** | **Version** | **Approved by** | **Designation** | **Signature** |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |

CONTACT INFORMATION

| **Name** | **Designation** | **Phone** | **Mail** |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |

BACKUP PLAN OVERVIEW

|  |
| --- |
| (Description of backup plan to implement in case of emergency) |

RISK MANAGEMENT

| **Potential Disaster** | **Probability rating** | **Impact rating** | **Description of consequences** |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

EMERGENCY ALERT AND ESCALATION

|  |
| --- |
| (Description of the problem or disaster and the steps taken to deal with it) |

DISASTER RECOVERY TEAM

| **Name** | **Phone** | **Mail** | **Responsibilities** |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

DAMAGE ASSESSMENT FORM

| **Key Business Affected** | **Description of Problem** | **Extent of Damage** |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

INSURANCE

| **Policy name** | **Coverage Type** | **Coverage period** | **Amount of Coverage** | **Person Responsible for Coverage** | **Next Renewal Date** |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**LIST OF ABBREVIATIONS**

|  |  |  |
| --- | --- | --- |
| **Index** | **Abbreviation** | **Stands For** |
| I | IT | Information Technology |
| 2 | SLA | Service Level Agreement |
| 3 | IOT | Internet of things |
| 4 | IAS | International Accounting Standards |
| 5 | FDP | Finance Department |
| 6 | ITSM | Information Technology Service Management |
| 7 | NDA | Non-Disclosure Agreement |

# 1. Introduction to Backup & Recovery Policy

Backup Policy shall define standards of Backup & recovery control processes such that it achieves a balance between controls and efficiency, and follows the principle of Confidentiality, Integrity and Availability. Backup Policy will ensure data and infrastructure are protected from risks, such that the data is correctly and efficiently backed up and recovered in line with this policy and best practices.

# 2. Purpose

The aim of this policy is to ensure that <Company name> conforms to the standard backup & recover very control processes ensuring risks associated to the management of data backs and recovery are mitigated, and balance between controls and efficiency is maintained.

# 3. Scope

The scope of policy applies to everyone in the <Company name>, including its staff, service providers and consultants. This policy is regarded as crucial to the effective protection of data and other IT Assets.

# 4. Policy

## 4.1. Data Backup

1. Critical data, which is critical to <Company name>, must be defined in consultation with [IT Head] and backed up.
2. Backup data must be stored at a backup location that is physically different from its original creation and usage location (i.e., The Disaster Recovery Site).
3. The medium will dictate when to schedule Backup.
4. Data restores must at least be tested [**quarterly**].
5. Procedures for backing up critical data and the testing of the procedures must be documented by the Information Security Department. These procedures must include, as a minimum, for each type of data and system:
6. A definition of the specific data to be backed up.
7. The type(s) of backup to be used (e.g., full back up, incremental backup, etc.)
8. The frequency and time of data backup.
9. The number of generations of backed up data that are to be maintained (both on site and off site).
10. Responsibility for data backup.
11. The storage site(s) for the backups.
12. The storage media to be used.
13. Any requirements concerning the data backup archives.
14. Recovery procedure of backed up data.

## 4.2. Data Backup Selection

All data and essential IT Assets to continue operation of the <Company name> shall be backed up.

1. All supporting material required to process the information must be backed up as well. This includes programs; control files, install files, and operating system software.
2. The application owner, together with the Information Security, will determine what information must be backed up, in what form, and how often.

## 4.3 Backup Types

There are mainly 2 types of backups

1. Full backups shall be run [**XXXXXXX**] as these [**XXXXXX**] will be stored for a longer period.
2. Differential / Incremental Backup must be used for [**XXXXX**] backups

If a system requires a high degree of skill to recover from backup, consideration must be given to making full images of such servers as a backup.

This will ensure that the system shall be recovered with minimal knowledge of the system configuration.

Backup Schedule should not interfere with the day-to-day operations

Information Security along with [service/function] shall decide on centralized or decentralized backup, based on discussion, requirements, and constraints.

Storage medium shall be decided by information security, following aspects shall be considered,

1. Importance of data
2. Confidentiality & integrity
3. Retention Schedules
4. Storage capacity
5. Life and reliability of storage media

[IT HEAD & INFORMATION SECURITY HEAD] shall ensure that sufficient IT capacity is available to maintain the Backup and Disaster Recovery procedures to ensure segregation of duties and responsibilities and mitigate the risk of systems and data losses.

## 4.4 Backup Storage and Security

Appropriate security measures are to be implemented for backups, which includes all necessary physical security controls, such as those related to the safety and security of the actual backup media – specifically – disks, tapes, and any other medium containing backup data. This requires the use of a computer room or other designated area (facility) that is secured and always monitored and whereby only authorized personnel have physical access to the backups. Thus, "secured" and "monitored" implies that the facility has in place the following physical security and environmental security controls

* Constructed in a manner allowing for adequate protection of backups.
* Security alarms that are active during non-business hours, with alarm notifications directly answered by a third-party security service or local police force.
* The use of cages, cabinets, or other designated, secured areas for securing backups.
* Access control mechanisms consisting of traditional lock and key, and/or electronic access control systems (ACS), such as badge readers and biometric recognition (i.e. iris, palm, fingerprint scanners/readers). Furthermore, all electronic access control mechanisms are to record all activity and produce log reports that are retained for a minimum of [x] days.
* Adequate closed-circuit monitoring, video surveillance as needed, both internally and externally, with all videos kept for a minimum of [x] days for purposes of meeting security best practices and various regulatory requirements.
* Appropriate fire detection and suppression elements, along with fire extinguishers placed in mission critical areas.
* Appropriate power protection devices for ensuring a continued, balanced load of power to the facility for where the backups reside.

## 4.5 Recovery of Backup Data

Documentation of the procedure must include:

1. Procedures for the recovery
2. [**Provision for key management should the data be encrypted**].

Recovery procedures must be tested at least [**quarterly**], and Disaster Recovery procedures must be tested at least [**yearly**]. Recovery tests must be documented and submitted to the [**IT Head & Information Security Head**].

# 5. STORAGE MANAGEMENT

Storage management is a data storage process which moves data between high-cost and low- cost storage media. Storage management is needed because high speed storage devices, such as hard disk drive arrays are more expensive than slower services, such as optical discs and magnetic tape drives. While it could be ideal to have all data available on high-speed devices all the time, this is prohibitively expensive. Instead, Storage management policies are set so that bulk of the backup data is on slower devices, and then backup data is transferred to faster devices when needed.

# 6. Business Continuity and Disaster Recovery Planning (BCDR)

Documented Business Continuity and Disaster Recovery Planning (BCDRP) is vital to protecting all [company name] assets along with ensuring rapid resumption of critical services in a timely manner. Because disasters and business interruptions are extremely difficult to predict, it is the responsibility of authorized [company name] personnel to have in place a fully functioning BCDRP process, and one that also includes specific policies, procedures, and supporting initiatives relating to the safety and security of backups and supporting systems for which to restore backup data on.