**Grant Investrade Backup Policy**



**Application Name: HP Data Protector**

**Primary Administrator: Amit Mishra/ Karamveer Prajapati**

**Secondary Administrator: Jitendra Rane**



**Prepared By:**

|  |  |
| --- | --- |
| **Document Owner(s)** | **Project/Organization Role** |
| Amar Alavane |  |
|  |  |

**Project Status Report Version Control:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Author** | **Change Description** |
| 1.0 | 16/05/2012 | Amar Alavane | Backup policy created |

**Table of Contents**

[1.0 Scope 2](#_Toc450036217)

[2.0 Backup Policy 3](#_Toc450036218)

[3.0 Locations covered 3](#_Toc450036219)

[4.0 Software and Hardware used 3](#_Toc450036220)

[5.0 Media usage guidelines 3](#_Toc450036221)

[6.0 Backup Sources and Backup Summary 3](#_Toc450036222)

[7.0 NAS Backup / VM Backup 3](#_Toc450036223)

[7.1 Labeling Conversation 3](#_Toc450036224)

[7.2 Media Usage 4](#_Toc450036225)

[7.3 Backup Type 4](#_Toc450036226)

[7.4 Backup Content 4](#_Toc450036227)

[8.0 Media Handling & Inventory 4](#_Toc450036228)

[9.0 Restoration 4](#_Toc450036229)

[11.0 Escalation Process 5](#_Toc450036230)

[12.0 Backup and Audit Report 5](#_Toc450036231)

[13.0 Annexure 5](#_Toc450036232)

# Scope

This document contains Grant Investrade backup policy and detailed process and procedures to ensure backup of important data sources such as File Servers, Application Database and shifting the backup media to a location other than where the Server exists, to protect the data against disasters like riot and fire.

# 2.0 Backup Policy

* Backups will be scheduled in accordance with the importance of the data acceptable risk as determined by the application owner.
* A restoration drill will be conducted every week / month to ensure that the backed up data is recoverable.
* Backup tapes must have identifying criteria that can be readily identified by bar-coding system.

# 3.0 Locations covered

**Grant Investrade**  
Incenter, 12th road Andheri (E) MIDC Mumbai

# 4.0 Software and Hardware used

* HP Data protector for File server and Application Database backup

|  |  |
| --- | --- |
| **STORAGE DEVICE** | LTO 6 Tape Library |
| **MEDIA** | LTO 6 6.25 TB |
| **MEIDA MAKE** | HP |
| **DRIVE MAKE** | HP MSL 4048 |

# 5.0 Media usage guidelines

* Backup Media life: Maximum usage limit of a media is 2000 times.
* In case the media is diagnose with any mechanical or read failure, the same will not be reuse and will be destroyed by accepted methods.
* Media usage life-cycle will be April to March.

# 6.0 Backup Sources and Backup Summary

**File server, Application and Database:** File Server & Application Databases will be backed-up using the HP Data Protector 10.30 as per the schedule. Backup logs should be reviewed by the backup administrator every day and the log will be preserved in a network location.

**Summary,**

|  |  |  |  |
| --- | --- | --- | --- |
| **Data** | **Backup Technology used** | **Backup Type** | **Retention** |
| **NAS Backup** | HP Data Protector 9.0 | Daily | 6 Days |
| Weekly | 5 weeks |
| Monthly | 104 weeks |
| **VM Backup** | HP Data Protector 9.0 | Daily | 6 Days |
| Weekly | 5 weeks |
| Monthly | 104 weeks |
| **AD backup** | HP Data Protector 9.0 | Daily | 6 Days |
| Weekly | 5 weeks |
| Monthly | 104 weeks |
| **Account File Server Backup** | HP Data Protector 9.0 | Daily | 6 Days |
| Weekly | 5 weeks |
| Monthly | 104 weeks |

# 

# 7.0 NAS Backup / VM Backup

HP Data Protector Backup utility used for backing up File Server and VM Database backup.

## 7.1 Labeling Conversation

The labeling will be maintained using bar codes, which is having unique numbers. **Refer Annexure C**

## 7.2 Media Usage

|  |  |
| --- | --- |
| **HP Data Protector 9.0 Tapes Usage Per Year** | |
|  | |
| **Backup Schedule** | **Tapes** |
| **Daily** | **12** |
| **Week** | **20** |
| **Monthly** | **96** |
| **Extra in case of emergency** | **2** |
| **Internal Database Backup** | **4** |
| **Cleaning Tape** | **2** |
| **Total** | **136** |

## 7.3 Backup Type

**Daily Backup:**

* Daily Differential backup taken for NAS & Active Directory.
* Daily backup will be taken as per the schedule.
* Daily backup will be preserved for 6 Days.
* Daily backup is scheduled from Monday to Sunday.
* Daily tapes will be reused every alternate week. For instance, tapes used on 1st of this Monday will be reused on 2nd of next Monday and so on so forth.

**Weekly Backup:**

* Weekly FULL Backup taken for NAS, Active directory and Virtual machines.
* Weekly backup will be taken as per the schedule.
* Weekly backup will be preserved for 5 weeks.
* Weekly backup is scheduled on Sunday.
* Weekly tapes will be reused every alternate week. For instance, tapes used in 1st week of this month will be reused in 1st week of next month and so on and so forth.

**Monthly Backup:**

* Monthly FULL Backup taken for NAS, Active directory and Virtual machines
* Monthly backup will be taken as per the schedule.
* Monthly backup will be preserved for 104 weeks.
* Monthly backup is scheduled on the 30th/31st Day of month.

## 

## 7.4 Backup Content

Refer **Annexure A** for Application / Database backup policy for details of backup content.

# 8.0 Media Handling & Inventory

In case of media problem, the tape cartridge should be destroyed immediately by the accepted methods. Refer **Annexure C** for Tape Inventory.

# 9.0 Restoration

**Restoration Requests from users:** User file restorations will be accepted on receiving an approved request from the user. This will be subject to appropriate authorization from the reporting manager on the Backup Restore Form.

**Restoration Drill:** File server and Application Database backup restoration drill will be undertaken by the system administrator. After the restoration, application owner will check the restored data and sign the acceptance form. Sample of acceptance form can be found in **Annexure B** - Monthly Restoration Drill.

# 11.0 Escalation Process

If for some reason it is not possible to complete the daily / weekly / monthly scheduled backup, it must be done on the next working day at the start of working hours. If the System administrator is unavailable, the Program Manager will ensure that somebody is designate to perform the backup operation.

If the backup cannot be taken due to a hardware failure, the matter must be escalated to the application owner immediately. If the failure persists for more than 24 hours, the matter should be escalating to the FMS In-charge at Service Office. The communication must be ensure through fax/email, indicating clearly the type of error, date and time of failure, action taken, and the status.

# 12.0 Backup and Audit Report

This report will be generated by the system administrator and will be provided every month to the respective Application Owner at Service Office.

|  |  |  |  |
| --- | --- | --- | --- |
| **Sr. No.** | **Activity** | **Confirmation (Y/N)** | **\* NEXT STEPS** |
| 1 | Backup Logs available for the entire month. | Y |  |
| 2 | Backup successful for 97% of times (if not then specify the % of times its successful and why it went down from 97%). | Y |  |

***Note****: Next steps will define the further action if the backup was not completed.*

# 13.0 Annexure

|  |  |  |
| --- | --- | --- |
| **Annexure** | **Details** | **Attachment** |
| Annexure A | Application / Database Backup Policy |  |
| Annexure C | Tape Inventory |  |