# Server Backup Policy

## Introduction

Data is one of Banks DIH Limited's most important assets. In order to protect this asset from loss or destruction, it is imperative that it be safely and securely captured, copied, and stored. The goal of this document is to outline a policy that governs how and when data residing on company servers will be backed up and stored for the purpose of providing restoration capability. In addition, it will address methods for requesting that backed up data be restored to individual systems.

## What Is Backed Up - Systemi

.

This policy refers to the backing up of data that resides on Banks DIH Limited's Systemi Logical Partition (LPAR) servers, LPAR 1 – Production Server and LPAR 2 – Development Server. Servers and the files/folders and/or data types on these servers that are covered by this policy include:

System i Server

Daily – All changed files

Weekly – All IFS files, all Libraries

Monthly – All IFS files, all Libraries, security and configuration data

Yearly – All LIC, all IFS files, all Libraries

It is the responsibility of server administrators to ensure that all new LPAR servers be added to this policy, and that this policy be applied to each new server's maintenance routine. Prior to deploying a new LPAR, a full backup must be performed and the ability to perform a full restoration from that backup confirmed. Prior to retiring a server, a full backup must be performed and placed in permanent storage.

## What Is Backed Up - Intel

.

This policy refers to the backing up of data that resides on Banks DIH Limited's servers. Servers and the files/folders and/or data types on these servers that are covered by this policy include:

All Intel servers use Veeam Backup and Replication application. Veeam Backup and Replication provides fast, flexible, and reliable recovery of virtualized applications and data. It unifies backup and replication in a single solution while offering increased data protection for VMware vSphere environment. Veeam has implemented both compression and deduplication features to help recover what would otherwise be a significant amount of data storage space used to store backups of vm's. D**ata deduplication i**s a specialized data compression technique for eliminating coarse-grained redundant data, typically to improve storage utilization. In the deduplication process, duplicate data is deleted, leaving only one copy of the data to be stored, along with references to the unique copy of data.

The backup job for the below-listed servers are managed by the Veeam Backup and Replication whose schedule is configured for a full backup of all VM's, followed by deduplicated, incremental backups. Hence, a full backup is always available for restore.

Note: The following are Banks DIH Limited's VMWare servers and are backed up using Veeam. Restoration takes place at file level or as an entire server.

- **Tp-dcserver**
- **Tp-adminserv01**
- **Tp-appserv01**
- **Tp-managserver**
- **Tp-managserv01**
- **Tp-exectermserv**
- **Tp-termserv01**
- **Tp-termserv02**
- **Tp-termserv03**
- **Tp-termserv04**
- **Tp-termserv05**

- **Tp-bbserver01**
- **Tp-bbserver02**
- **Tp-cctvserv01**
- **Tp-exectermserv**
- **Tp-fileserv00**
- **Tp-fileserv01**
- **Tp-solarwinds01**
- **Tp-onlinebackup**
- **Tp-printserver01**
- **Tp-solarwinds01**
- **Tp-veeamproxy01**
- **Tp-veeamsvr01**
- **Tp-webmanager**
- **Tp-websense-appliance**
- **Tp-vmadmin**
- **Tp-wsuserv01**
- **Tp-iasserv01**

This policy does not refer to backing up of data that resides on individual PC or notebook hard drives. Responsibility for backing up data on local desktop systems or laptops rests solely with the individual user. It is strongly encouraged that end users save their data to the appropriate server listed above in order that their data is backed up regularly in accordance with this policy.

In addition, files that are left open at the time the backup procedure is initiated may not be backed up. End users are reminded to save and close all files, as well as all related applications, prior to the backup procedure window.

It is the responsibility of server administrators to ensure that all new servers be added to this policy, and that this policy be applied to each new server's maintenance routine. Prior to deploying a new server, a full backup must be performed and the ability to perform a full restoration from that backup confirmed. Prior to retiring a server, a full backup must be performed and placed in permanent storage.

## Systemi Backup Schedule

Backups are conducted automatically. System i backups utilize the system's backup utility on both servers (partitions) which backs up to tape for offsite storage.
. This method ensures that no more than one day's working data will be missing in the event of a data loss incident:

All backups tapes are to be labeled using the following labeling conventions:

System i backups – MONTH\DATE\YEAR

All backup tapes stored on site are to be stored in a fireproof Chubb. All backup tapes stored off site are to be stored at the Citizen Banks Thirst Park Branch location in a fireproof Chubb in the care of the Branch Manager.

All LPAR Production System i backups will take place between the hours of 11:00 PM and 03:00AM. These timeframes have been selected to minimize the impact of server downtime on end users that may be caused by the need to take servers offline in order to perform the backup itself. If this backup schedule in some way interferes with a critical work process, then the affected user(s) is to notify the IT Department so that exceptions or alternative arrangements can be made.

Incremental backups (only files changed since the last backup) will be performed daily, Monday through Friday. These tapes will be stored onsite during the following backup cycle. At the end of the latter cycle, the daily tapes will be removed to a predetermined offsite location for storage for 1 week. When this 1 week period has elapsed, the tapes will be brought back on site for reuse for a period not to exceed one year.

A full backup will be performed for System i on a weekly/monthly basis. These tapes will be stored on site during the following backup cycle. At the end of the latter cycle, the weekly tape will be removed to a predetermined offsite location for storage for 1 week. When this 1week period has elapsed, the tapes will be brought back on site for reuse for a period not to exceed one year.

A full backup will be performed at the end of each month. This tape will be immediately removed to a predetermined offsite location for permanent storage. These tapes will never be reused.

All server backups performed must be noted in the server backup log immediately upon completion. All server backup log sheets must be kept in an appropriately labelled three-ring binder in an agreed-upon, centralized location. The log must include:

Server name,

Date and time of backup,

Name of administrator performing the backup,

Files backed up and/or skipped,

Software used to perform the backup,

Backup medium used and its label/name, and

Whether the backup was successful or not.

If, for some reason, the backup cannot be completed, is missed, or crashes, then it must be completed by 9:00 a.m. the following morning. The reason for non-completion of the originally scheduled backup must be noted in the server backup log. In addition, if a backup fails more than one day in a row, end users in the organization must be notified.

If a tape is discovered to be damaged or corrupt, then the tape must be destroyed to prevent further use and replaced with a new one.

## Intel Backup Schedule

Backups are conducted automatically. Intel servers use Veeam Backup and Replication application, which backs up to on-site SAN and NAS storage devices. The servers listed above must be backed up according

to the following procedure. This method ensures that no more than one day's working data will be missing in the event of a data loss incident:

All Intel backups are scheduled from 06:00 PM to completion. These timeframes have been selected to minimize the impact of server performance degradation. If this backup schedule in some way interferes with a critical work process, then the affected user(s) is to notify the IT Department so that exceptions or alternative arrangements can be made.

Veeam Backup and Replication application runs Reverse incremental backups (only files changed since the last backup) daily, Monday through Sunday.

All server backups results, whether successful or not, are emailed to all members of Technical Support team and summary or detailed reports can be run for review or filing. All server backup log sheets must be kept in an appropriately labelled three-ring binder in an agreed-upon, centralized location. The log must include:

Server name,

Date and time of backup,

Name of administrator performing the backup,

Files backed up and/or skipped,

Software used to perform the backup,

Backup medium used and its label/name, and

Whether the backup was successful or not.

If, for some reason, the backup cannot be completed, is missed, or crashes, then it must be completed by 9:00 a.m. the following morning. The reason for non-completion of the originally scheduled backup must be noted in the server backup log. In addition, if a backup fails more than one day in a row, end users in the organization must be notified.

### Warm Site and Replication

One of the most important aspects of disaster recovery is to have a location from which the recovery can take place. This location known as a Warm Site, is situated at the Berbice Branch of the company's operations. In the event of a disaster at the main site the Company's data center will be recreated and operations continued from the warm site, for the length of the disaster.

The warm site is already stocked with hardware representing a reasonable facsimile of that found in the Banks DIH data center. To restore service, the last backups from our off-site storage facility must be delivered, and bare metal restoration completed, before the real work of recovery can begin.

In any replication scenario, it is VERY important to account for the bandwidth requirements for the data being copied from site to site. Data replication can consume significant bandwidth, and therefore it is important to plan this and ensure that disaster recovery replication does not consume precious Internet access bandwidth or WAN links and compete with existing applications. WAN acceleration, via products such as Veeam Backup and Replication application, can provide a valuable option to get the most out of existing links without needing to purchase extra bandwidth or new links (but this varies situation by situation). Timing of replication can also be an issue – for example, it might be acceptable to throttle communications during the work day, and have replication "catch up" after 6pm if the Recovery Window allows for loss of a few hours' data.

A "Warm Site" typically has live communication links and some amount of hardware, but typically requires installation of software and/or restoration of data from tape or another media format – typically in a span of hours or a day before the site is operational;

## Managing Restores

The ultimate goal of any backup process is to ensure that a restorable copy of data exists. If the data cannot be restored, then the process is useless. As a result, it's essential to regularly test one's ability to restore data from its storage media.

## System i

1. All daily tapes should be tested at least once every 2 months to ensure that the data they contain can be completely restored.
2. All weekly tapes should be tested at least once every 3 months to ensure that the data they contain can be completely restored.
3. All monthly tapes should be tested at least once every year to ensure that the data they contain can be completely restored.

## Intel - SureBackUp

A SureBackup job is a task for VM backup recovery verification. Such a job was created to ensure that the CRITICAL servers existing in the Banks DIH environment can be restored successfully. The SureBackup job aggregates all settings and policies of a recovery verification task, such as application group and virtual lab to be used, VM backups that should be verified in the virtual lab and so on. The SureBackup job runs manually or can be scheduled to be performed automatically.

By default, you can start and test up to three VMs at the same time. You can also increase the number of VMs to be started and tested simultaneously. These VMs are resource demanding, performance of the SureBackup job as well as performance of the ESX(i) host holding the virtual lab may decrease.

Once the verification process is complete, VMs from the application group are powered off. Optionally, you can leave the VMs from the application group running to perform manual testing or enable user-directed application item-level recovery.

In some cases, the SureBackup job schedule may overlap the schedule of the backup job linked to it. The backup file may be locked by the backup job and the SureBackup job will be unable to verify such backup. In this situation, Veeam Backup & Replication will not start the SureBackup job until the corresponding backup job is over.

When a SureBackup job runs, Veeam Backup & Replication first creates an environment for VM backups verification:

1. Veeam Backup & Replication starts the virtual lab.

2. In the virtual lab, it starts VMs from the application group in the required order. VMs from the application group remain running until the verified VMs are booted from backups and tested. If Veeam Backup & Replication does not find a valid restore point for any of VMs from the application group, the SureBackup job will fail.

3. Once the virtual lab is ready, Veeam Backup & Replication starts verified VMs from the necessary restore point, tests and verifies them one by one or, depending on the specified settings, creates several streams and tests a number of VMs simultaneously. If Veeam Backup & Replication does not find a valid restore point for any of verified VMs, verification of this VM fails, but the job continues to run.

Data will be restored from a backup if:

There is an intrusion or attack.

Files have been corrupted, deleted, or modified.

Information must be accessed that is located on an archived backup.

In the event a data restore is desired or required, the following policy will be adhered to:

4. Responsibility for overseeing backup and restore procedures is the Service Desk. If a user has a restore request, they can contact Service Desk by calling ext. 2129 or 2409, or by sending an e-mail to helpdesk@banksdih.com.
5. In the event of unplanned downtime, attack, or disaster, consult Banks DIH Limited's Disaster Recovery Plan for full restoration procedures.
6. In the event of a local data loss due to human error, the end user affected must contact the IT Department and request a data restore. The end user must provide the following information:

   Name.

   Contact information.

   Name of file(s) and/or folder(s) affected.

   Last known location of files(s) and/or folder(s) affected.

   Extent and nature of data loss.

   Events leading to data loss, including last modified date and time (if known).

   Urgency of restore.

7. Depending on the extent of data loss, a daily tape, weekly tape, or combination of both will need to be used. The timing in the cycle will dictate whether or not these tapes are onsite or offsite. Tapes

must be retrieved by the server administrator or pre-determined replacement. If tapes are offsite and the restore is not urgent, then the end user affected may be required to wait up 8 hours for the tape(s) to be retrieved.

8. If the data loss was due to user error or a lack of adherence to procedure, then the end user responsible may be required to participate in a tutorial on effective data backup practices.

## Use of Contractors

### Confidentiality Statement

IBM and SPECOM have signed contracts with Banks DIH that includes contract guidelines for confidentiality and protection of Banks DIH data.

**Validation**

Files Restored.

## Declaration of Understanding

I, , have read, understand, and agree to adhere to Banks DIH Limited's Server Backup Policy.

**Name (Printed):** _____

**Name (Signed):** _____

**Today's Date:** _____

_____