


# Backup Policy

---

**Version 6.0**  
**23<sup>rd</sup> June 2025**

# Document History

---

Created by:	Eddy Lareine	
Approved by:	Areff Salauroo	

Release date	Version	Change Details	Reviewed by
22.10.19	1.0	Submitted for review	Legal Advisor
12.11.19	2.0	Apply changes submitted by legal advisor	Eddy Lareine
12.02.20	3.0	Submitted for review	Areff Salauroo
13.08.20	4.0	Apply changes to Tape Backups	Areff Salauroo
05.07.21	5.0	Apply changes to replication	Areff Salauroo
23.06.25	6.0	Apply changes to Scope & RTO	Areff Salauroo

## Table of Contents

<b>1.0</b>	<b><i>Objective.....</i></b>	<b>5</b>
<b>2.0</b>	<b><i>Scope.....</i></b>	<b>5</b>
<b>3.0</b>	<b><i>References ISO 27001:2013 Controls.....</i></b>	<b>6</b>
<b>4.0</b>	<b><i>Definitions .....</i></b>	<b>6</b>
<b>5.0</b>	<b><i>Policy Description .....</i></b>	<b>7</b>
<b>5.1</b>	<b><i>Veeam Backup and Replication.....</i></b>	<b>7</b>
<b>5.2</b>	<b><i>Validation of Backup Media and Recovery Processes .....</i></b>	<b>8</b>
<b>5.3</b>	<b><i>Backup of User Systems .....</i></b>	<b>9</b>
<b>6.0</b>	<b><i>Enforcement.....</i></b>	<b>9</b>
<b>7.0</b>	<b><i>Declaration of Understanding.....</i></b>	<b>10</b>

## Table of Figures

Figure 1- Replication & Backup of VMs workflow at DR site.....	7
--	---

# BACKUP POLICY

## 1.0 Objective

The objective of this policy is

- To protect against data loss in the case of an accidental deletion, corruption of data, system failure, or disaster.
- To maintain the integrity and availability of information and information processing facilities, regularly take and test back-up copies of information and software.
- To manage and secure backup and restoration processes and the media used for the backup process.

## 2.0 Scope

This policy applies to IT systems and data owned or under the responsibility of, operated by, La Sentinelle Group. It also covers Servers—listed below—located in La Sentinelle Data Centres and the files and/or data types on these servers.

- AdBooking (App & Database) servers
- Sage (App & Database) servers
- IntraPrint (App & Database) servers
- Sicorax (App & Database) servers
- Navision (App & Database) servers
- Documentation Server
- Marketing KPI Server
- Marketing Alfresco Server
- Marketing CCM Server
- Only Office Document Server
- Marketing Generator Server
- Domain Controller Server
- 3CX Server

### 3.0 References ISO 27001:2013 Controls

- **Information Back-up – A.12.3.1**

*Back-up copies of information, software, and system images shall be regularly tested per an agreed back-up policy.*

### 4.0 Definitions

**Backup** - The saving of files onto magnetic tape or other offline mass storage media for the purpose of preventing loss of data in the event of equipment failure or destruction.

**Archive** - The saving of old or unused files onto magnetic tape or other offline mass storage media for the purpose of releasing on-line storage room.

**Restore** - The process of bringing off line storage data back from the offline media and putting it on an online storage system such as a server and making it available for real time processing.

**Recovery Point Objective (RPO)** –The amount of data that can be lost before significant harm to the business occurs. The objective is expressed as a time measurement from the loss event to the most recent preceding backup.

**Recovery Time Objective (RTO)** – The duration of time within which a business process must be restored after a disaster in order to avoid unacceptable consequences associated with a break in continuity.

**IT Systems** – Information Technology applications used to process information.

**NAS (Network-attached storage)** – NAS is a high-speed sub network of shared storage devices. A NAS architecture works in a way that makes all storage devices available to all servers on a Local Area Network (LAN) or Wide Area Network (WAN).

**SLA (Service Level Agreements)** - SLA is a contract between a service provider and its internal or external customers that documents what services the provider will furnish and defines the service standards the provider is obligated to meet such as quality, availability, responsibilities, response time, resolution time, severity level of faults, etc.

## 5.0 Policy Description

Adequate back-up facilities are used to ensure that all essential information and software can be recovered following a disaster or media failure.

It is the responsibility of the System Administrator 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.

Backups and replication are performed using Veeam Backup and Replication Software. All critical servers located in the Data Centres must be backed up according to the procedure described below. This method ensures a maximum Recovery Point Objective (RPO) of 24 hours, that is, no more than one day's working data will be missing in the event of a data loss incident.

## 5.1 Veeam Backup and Replication

1. The VMs (Image-level Veeam Backup) are replicated on a NAS located at La Sentinelle Ltd Port Louis Office **using Veeam Replication Software**.
2. The VMs (Image-level Veeam Backup) are Backed up on a NAS located in the Data Center of La Sentinelle's head Office at Riche Terre Office **using Veeam Replication Software**.

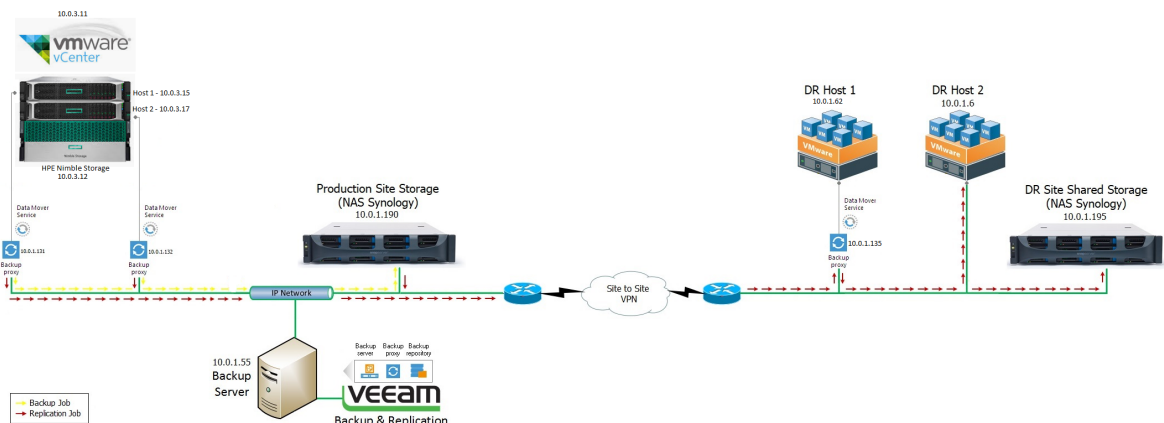


Figure 1- Replication & Backup of VMs workflow at DR site

3. Veeam Backup and Replication schedules:
  - Veeam Configuration Backup (Database) – Done daily at 10 am
  - Backup Jobs – Daily at 8 pm (7 Days restore points)
  - Replication Jobs – Daily (7 restore points)
  - Synthetic Full backup – Every Saturday (Transforms incremental/previous backup into Rollback)

- Active Full Backup – Monthly on Last Sunday
- Maintenance on storage-level – Health check on Last Sunday
- Replication Jobs
  - **RPO (Every 24 Hours)**
  - **RTO (< 5 Hours)**

## 5.2 Validation of Backup Media and Recovery Processes

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 is essential to regularly test one's ability to restore data from its storage media. Consequently, the recovery process is tested once a year to ensure that the recovery procedures are operational and valid.

1. 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 on an archived backup.
  - A Server or system has crashed.
  - A disaster recovery.
  
2. Restoration to a past state or recovery of files must be requested by the Head of IT through a formal request and approved by the system owner.
  
3. In the event a data restore is desired or required, the following policy will be adhered to:
  - The **System Administrator** is responsible for overseeing Backup and Restore procedures. If a user has a restore request, they can contact the System Administrator by sending an email to the Head of IT of La Sentinelle Ltd and filling out and submitting a request form located at [URL or shared drive location].
  - In unplanned downtime, attack, or disaster, consult La Sentinelle Ltd Disaster Recovery Plan/Business Continuity Plan for full restoration procedures.



4. In the event of a local data loss due to human error, the end user affected must contact the IT Department through his Head of Department and request for 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.
  
5. La Sentinelle Ltd also has maintenance agreements with suppliers for critical systems – both hardware & software, who are required to respond to call-out requests within time frames specified in respective SLAs. The agreements also include escalation procedures when faults have not been fixed within a specific time frame.

### **5.3 Backup of User Systems**

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 servers or their external hard disks to ensure that their data is backed up regularly.

### **6.0 Enforcement**

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

## 7.0 Declaration of Understanding

I acknowledge having read, understood, and agreed to adhere to La Sentinelle Ltd Backup Policy.

**Name** : \_\_\_\_\_

**Signature** : \_\_\_\_\_

**Date** : \_\_\_\_\_