White
Rose

GUIDE

Data Security Guide

Why is this important?

A Data Security policy is important because it protects an organisation's assets, both physical and digital.

Document control
This document is uncontrolled when printed or downloaded and should be discarded after use. Always source the most recent version from the White Rose *Governance Fundamentals Library* and share only the document link.

Document title	**Quick Investigation**	Verbatim of above
Identification	**FORM004**	A unique identification number: letters followed by three digits.
Status	**Published**	The lifecycle status: draft/published.
Version	**2**	Major number only (0=draft; 1; 2; etc)
Approval Date	**26 February 2026**	The date this version of the document was approved
Revalidation Date	**26 February 2028**	The date the document is due for review. A maximum of two years after the approval date.
Approver	**Lee Mason**	Title of the person who owns and is responsible for the document

Revision History		
Revised by	Revisions/changes/comments	Date re-published
Lee Mason	**First drafting**	**20 July 2022**
Lee Mason	**Revision**	**20 August 2022**

Table of Contents

1. Data Security Guide

We are committed to protecting your data at White Rose Loan Processing (White Rose LP). This Data Security Policy outlines behaviours expected of our employees and its purpose to protect information handled and processed by White Rose LP staff, per *OR004 Information Governance & Controlled Documents* and *OR011 Technology & Cybersecurity*.

From time to time, we may review and update this Data Security Policy, including considering new laws, regulations and technology. All personal information held by us will be governed by our most recent Data Security Policy, posted on our website at: www.whiteroselp.com.au

Throughout this Data Security Policy, "White Rose LP" refers to the business services provided by White Rose Loan Processing (also referred to as "we", "us", or "our").

Purpose

White Rose LP must restrict access to confidential and sensitive data to protect it from being lost or compromised to avoid adversely impacting our customers, incurring penalties for non-compliance and damaging our reputation. At the same time, we must ensure users can access data as required to work effectively.

It is not anticipated that this policy can eliminate all malicious data theft. Rather, its primary objective is to increase user awareness and avoid accidental loss scenarios, so it outlines the requirements for data breach prevention.

Our Employees

- In selecting our staff, we will take all reasonable care to ensure adequate security background, understanding of our processes and policies, operational training and supervision.
- All staff must sign the Privacy Agreement to maintain private client information.
- Individual client information will only be known to the Director and an employee responsible for entering data into systems.
- All employees will receive Data Protection and Privacy Laws training during their induction.

Principles

Our clients shall provide White Rose LP with access to the information they need to carry out their responsibilities as effectively and efficiently as possible.

General

- Each user shall be identified by a unique user ID so that individuals can be held accountable for their actions.
- The use of shared identities is permitted only where they are suitable, such as training accounts or service accounts.
- Each user shall read this data security policy and sign a statement that they understand the access conditions.
- Records of user access may be used to provide evidence for security incident investigations.

- Access shall be granted based on the principle of least privilege, which means that each program and user will be granted the fewest privileges necessary to complete their tasks.

Access Control Authorisation

- Risk evaluation will be based on threats relevant to information handled by White Rose LP.
- Appropriate infrastructure and systems will be used, with the staff receiving adequate training to mitigate information security risks.
- Access to our client's Information Computing Technology (ICT) systems will be given through the provision of a unique user account and complex password. Our client provides User Accounts based on records within their IT department.
- Role-based access control (RBAC) will be used to secure access to all file share-based resources in Active Directory domains (Google Drive, Microsoft OneDrive, Dropbox etc.)

Network Access

- All White Rose LP employees shall be given network access by business access control procedures and the least-privilege principle.
- All White Rose LP employees shall only authenticate using the VPN authentication mechanism.
- Segregation of networks shall be implemented as recommended by the company's network security research. Network administrators shall appropriately group information services, users and information systems to achieve the required segregation.
- Network routing controls shall be implemented to support the access control policy.

Electronic File Storage

- We don't hold paper copies of any client files.
- We use Google Drive, Microsoft OneNote or Dropbox for Business in our clients' data storage and Microsoft 365 for all email services. All client files are encrypted in storage and transfer.
- Sync Files stored in a workstation are encrypted.
- We will often rename the client file to a standard naming convention, identifying the document and its receipt/processing date.
- Upon client request or once the client information is processed and files attached/passed to the client, we will remove all client data from our storage systems.
- We will ensure all data files that might be stored on the hard drive are erased when removing the redundant computer systems.
- We do not use portable storage devices.

User Responsibilities

- All computer platforms and networks we operate are subject to username and password protection.
- All users must lock their screens whenever they leave their desks to reduce the risk of unauthorised access.

- All users must keep their passwords confidential and not share them. All passwords are a minimum of ten characters in length and contain at least one of each: a capital letter, a lower case letter, a number and a special symbol.
- Each workstation has a screen saver that requires a password re-entry after being idle for 5 minutes.

Application and Information Access

- Users shall be granted access to the data and applications required for their job roles.
- All users shall access sensitive data and systems only if there is a business need to do so, and they have approval from higher management.
- Sensitive systems shall be physically or logically isolated to restrict access to authorised personnel only.

Access to Personal or Sensitive information

- Access to data classified as 'Personal or 'Sensitive' shall be limited to authorised persons whose job responsibilities require it, as determined by the Data Security Policy or higher management.
- The responsibility to implement access restrictions lies with our client's IT department.

Ownership and Responsibilities

- **Data owners** are employees who have primary responsibility for maintaining information that they own (our clients).
- **Information Security Administrator** is an employee designated by our client who provides administrative support for implementing, overseeing and coordinating security procedures and systems concerning specific information resources.
- **Users** include everyone with access to information resources, such as our clients and White Rose LP employees.

Risk Management

- White Rose maintains and regularly updates the Risk Assessment – *Form002 Risk Assessment,* per *OR004 Risk Management* and *OR011 Technology and cybersecurity.*
    - A copy of Form002 can be made available upon request.

Incident Reporting & Investigation

- Any data security or security incidents breaches are reported to the Director/Founder and the affected client.
- Any data security or security incidents breaches are investigated to prevent future breaches of future incidents.

Enforcement

- Any user found violating this policy is subject to disciplinary action, up to and including termination of employment.