<Organisation Name>

Data Management Policy [Template]

<Document Version & Date>



Copyright © 2021 <Organisation Name>

This document is based on a template document provided by Real World Technology Solutions.

Real World Technology Solutions grants permission for the template document to be modified in any manner <Organisation Name> wishes, provided this acknowledgement remains in place.

Document Owner: <Person’s Name>

Contact: <Person’s email and/or mobile telephone>

**How to use this template document**

This is a template document. It contains suggested or recommended content.

It is content that can be freely added to, moved, modified, or deleted.

Do not feel obliged to use the content as-is if it does not suit your organisation.

You should read and adopt, adapt or remove, as appropriate!

What to do:

1. This document uses generic text for certain items that need to be updated by the organisation. These template text items are formatted in red with angle brackets (e.g. <Organisation Name> representing the organisation’s name), and should be updated to replace the template text with appropriate text specific to the organisation.
2. Using global replace, change <Organisation Name> to the organisation’s name
3. On the front page and in the page headers, change the Document Title to remove
“ [Template]” from the title, if present
4. On the front page and in the page footers, update the <Document Version & Date> to a new version of this document after your editing, and as you edit it in the future; e.g. V1.5 2025-05-05
5. Edit the document header to include the organisation’s logo, or remove the <Organisation Logo> template text
6. Find any other template text items and update them with the appropriate text for the organisation
7. Sometimes <there will be additional usage guidance formatted in blue like this comment> – it provides guidance and a reminder that the content can be freely edited to make it appropriate for your organisation
8. Review all the content and change anything as required to meet the organisation’s requirements and circumstances – sections and text can be modified, moved, deleted or added
9. Update the Contents table after updates by clicking on “Contents” and “Update Table…”; you may occasionally be prompted and can “Update entire table”
10. When ready, delete these instructions on this page and update the Contents again
11. Save the updated document

Contents

[1 Data Management Policy 5](#_Toc88812420)

[1.1 Overview 5](#_Toc88812421)

[1.2 Scope 5](#_Toc88812422)

[1.3 Objectives 5](#_Toc88812423)

[1.4 Obligations 6](#_Toc88812424)

[1.5 Data Classification Scheme 6](#_Toc88812425)

[1.6 Data Classifications 7](#_Toc88812426)

[1.7 Data Stewards 7](#_Toc88812427)

# Data Management Policy

This document is the Data Management Policy for all data within <Organisation Name>.

## Overview

<Adapt the wording to be appropriate to your organisation>

<Organisation Name> creates, stores, uses, transmits and deletes data of various types for various purposes. The sensitivity and value of the data ranges from publicly available data to highly sensitive personal data. This policy details how <Organisation Name> manages data to meet its cyber security obligations, and where appropriate, complies with other policies, legislation and regulations.

This Data Management Policy ensures <Organisation Name>:

* Complies with data protection laws and regulations, and follows good practice
* Protects the rights of clients, personnel, volunteers and partners
* Is transparent about how it stores and processes data, particularly personal data
* Protects itself from the risks of data breaches

## Scope

<Adapt the wording to be appropriate to your organisation, and adjust the list to describe the types of data that are relevant for your organisation. The list here is simply examples.>

All data created, stored, used, transmitted or deleted by <Organisation Name> are within the purview of this Policy. This includes:

* Publicly available data on websites and other disseminated sources
* Low value and low sensitivity data (e.g. general documents, advertising material, etc)
* High value and highly sensitive data (e.g. commercial-in-confidence documents, etc)
* Personnel data
* Client data
* Financial records
* Emails and messages, including voice messages
* Data belonging to, or managed on behalf of, third-parties
* Data stored locally, off-site, remotely, in-cloud and with third-parties

This policy applies to all internal personnel, volunteers, consultants, contractors, and third-parties acting on behalf of <Organisation Name>.

## Objectives

All data in the scope of this policy will be managed to achieve and maintain the following objectives:

* Confidentiality – protecting data in appropriate ways so that only authorised access and disclosure is permitted in accordance with the classification of the data
* Integrity – guarding against improper data modification, destruction or corruption, including ensuring data non-repudiation and authenticity where relevant
* Availability – maintaining timely and reliable access to and use of data

## Obligations

All data in the scope of this policy will be managed in accordance with the data standards and classifications defined in this policy. These include:

* Classifying all data appropriately
* Storing all data in ways appropriate for its classification, including encrypted as required
* Transmitting and transporting data securely
* Destroying sensitive and high value data securely

<Organisation Name> will comply with all relevant legislation and regulations, including:
 <Choose the ones that apply to your organisation, and add others that are relevant; e.g. industries such as healthcare, insurance and retail may have specific compliance requirements.>

* Privacy Act 1988 (Commonwealth)
* Australian Privacy Principles (Commonwealth)
* Australian Copyright Act 1968 (Commonwealth)
* Freedom of Information Act 1982 (Commonwealth)
* Freedom of Information Act 2016 (ACT)
* Privacy and Personal Information Protection Act 1998 (NSW)
* Information Privacy Act 2014 (ACT)
* Information Act 2002 (NT)
* Workplace Privacy Act 2011 (ACT)
* Information Privacy Act 2009 (Qld)
* Invasion of Privacy Act 1971 (Qld)
* Privacy and Data Protection Act 2014 (Vic)
* Personal Information Protection Act (Tas)

Legal and regulatory obligations may include data creation, storage, access protection, transmission, retention, sharing and destruction.

<Organisation Name> will ensure it remains in compliance with relevant legislation and regulations as they are enacted in the future.

## Data Classification Scheme

<This is an example scheme. Modify as appropriate for your organisation.>

Data is classified into one of the following <three> classification levels:

* **Public** – data that can be shared publicly or disclosed without restriction
* **Internal** – data that is restricted to <Organisation Name> personnel and others engaged by <Organisation Name>
* **Private** – data that is sensitive or high value and must be protected against unauthorised viewing, modification, distribution, sharing and deletion; access to Private data must be restricted to personnel formally approved to have that access

## Data Classifications

All data in the scope of this policy will be classified as follows:

<These are examples only. Create the relevant list for your organisation.>

* Personnel records – Private
* Client records – Private
* Proprietary materials – Internal
* General and miscellaneous information – Internal
* Websites – Public

## Data Stewards

All data in the scope of this policy will be assigned to <individual personnel within Organisation Name> who will have overall responsibility for the management of that data as data stewards.

<These are examples only. Create the relevant list for your organisation.>

The following data stewards are assigned:

* Personnel records – Human Resources Manager
* Client records – Clinic Manager
* Proprietary materials – Business Manager
* General and miscellaneous information – IT Manager
* Websites – IT Manager