**POPI Personal Information Back-up policy**

Table of Contents

[1 Purpose 1](#_Toc434827699)

[2 Scope 1](#_Toc434827700)

[3 Policy 1](#_Toc434827701)

[3.1 Policy Statement 1](#_Toc434827702)

[3.2 Policy Objectives 1](#_Toc434827703)

[3.3 Policy Overview 2](#_Toc434827704)

[3.4 Policy Maintenance 2](#_Toc434827705)

[4 Policy Requirements 2](#_Toc434827706)

[4.1 Build Documentation 2](#_Toc434827707)

[4.2 Back-up Schedules 2](#_Toc434827708)

[4.3 Restoration 3](#_Toc434827709)

[4.4 Software Compatibility 3](#_Toc434827710)

[4.5 Back-up Retention 3](#_Toc434827711)

[4.6 Media Storage 4](#_Toc434827712)

[4.7 Reporting Security Incidents 4](#_Toc434827713)

[4.8 Business Continuity 4](#_Toc434827714)

[4.9 User Awareness 4](#_Toc434827715)

[5 Disciplinary Process 4](#_Toc434827716)

[6 Deviations from Policy 4](#_Toc434827717)

[7 Policy updating 4](#_Toc434827718)

# Purpose

* The purpose of this policy is to ensure that [company name]’s electronic information resources are backed-up at scheduled intervals to suitably secure storage media in order to facilitate the restoration of all or part of those information resources in the event of loss or corruption of the original data.
* This policy is to help to meet the requirement of the POPI Act Condition 7: Security safeguards. This policy only applies to electronic records stored on [company name] servers.
* This policy may be extended to cover all electronic data, not just Personal Information as required by the POPI Act.

# Scope

The scope of this policy applies to:

* Any of [company name]’s premises where electronic information is stored; and
* Information system resources, including data networks and servers located at [company name] and non-[company name] locations, where these systems are under the jurisdiction and/or ownership of [company name], and any servers authorised to access [company name]’s data networks.

Out of Scope:

* [company name] is not responsible for backing up non-[company name] machines. [company name] IT Service Desk also does not back up PCs or laptops. Users should always save data to servers. i.e. data on users’ laptops and PCs is their own responsibility.
* It should be noted that personal drives on individual PCs and laptops will not be backed-up. Only data stored on corporate servers is subject to this Policy.

# Policy

## Policy Statement

[company name]’s information system resources are assets important to [company name]’s business and stakeholders and its dependency on these assets demands that appropriate levels of information security be instituted and maintained. It is [company name]’s policy that appropriate back-up measures are implemented to protect its information system resources from loss or corruption, and to maintain appropriate levels of confidentiality, integrity and availability of such information system resources.

## Policy Objectives

The objectives of this policy with regard to the protection of information system resources against

loss or corruption are to:

* Minimise the threat posed by the potential loss or corruption of electronic information owned by [company name] or temporarily entrusted to it; and
* Minimise reputation exposure, which may result from the loss or corruption of [company name]’s electronic information resources.

## Policy Overview

[company name] information system resources are important business assets that are vulnerable to loss or corruption due to technical failure, human error or malicious attack. It is therefore essential to ensure that verified back-ups are taken in order to be able to restore lost or corrupted data to its original state at a specified point in time.

## Policy Maintenance

Supporting standards, guidelines and procedures will be issued on an on-going basis by [company name]. Users will be informed of any subsequent changes or updated versions of such standards, guidelines and procedures by way of e-mail or other relevant communication media. Users shall then have the obligation to obtain the current information systems policies from [company name] IT department on an on-going basis and accept the terms and conditions contained therein.

# Policy Requirements

[company name]’s information system resources shall be backed-up at scheduled intervals in order to provide assurance of restoration in the event of loss or corruption of data and for business continuity planning purposes.

## Build Documentation

The [company name] IT department will document and build processes and test recovery routines to mitigate risks of data loss.

## Back-up Schedules

Back-ups are scheduled as one of the following:

* Daily
* Weekly
* Monthly
* Annual
* Archive
* As requested

According to standard definitions of terms, back-ups are determined as:

* Full
* Differential
* Incremental

Back-up logs will be reviewed daily by the IT department.

Tests will be conducted to investigate the cause of back-up failures and action taken accordingly to prevent recurrence.

## Restoration

* Test restorations will be conducted by the IT department at regular intervals using a disparate cross-section of application types to ensure that back-ups are working correctly and that restorations can be successfully executed.
* Requests for restoration of live systems must be logged with the IT department.
* Where possible, restores are made initially to an alternate location, and then copied to the live location following verification.
* Where restoration is to a live system and the system is not terminally corrupt, the existence of a suitably-recent back-up is confirmed in case the restoration fails. Where no suitably-recent backup exists, a back-up is taken first.
* Users will be notified of the outcome of the restore.

## Software Compatibility

A secure library of application software versions will be maintained for as long as corresponding back-ups are retained in order to ensure that a compatible version of the software will be available for use if the need arises to restore an application to a pre-upgrade state.

## Back-up Retention

Back-ups are retained in accordance with the following periods of time: [to be agreed]

Back-up Schedule Retention Period

Daily Minimum 1 month

Weekly Minimum 2 months

Monthly Minimum 3 months

Annual 6 years

Archive Indefinite

Once-off As requested

## Media Storage

Back-up tapes are collected and stored offsite by an appropriately-resourced third party contractor. Tapes held temporarily onsite are stored in a controlled, secure environment.

## Reporting Security Incidents

All security incidents, including significant back-up or restoration failures, should be reported immediately to the IT Service Desk.

## Business Continuity

Business continuity plans shall include provision for the restoration of information resources from back-ups. This document is supported and guided by the Business Continuity Plan for IS.

## User Awareness

Users shall be made aware of this Policy and all its provisions.

# Disciplinary Process

[company name] reserves the right to audit compliance with the policy from time to time. Any disciplinary action, arising from breach of this policy, shall be taken in accordance with [company name]’s Rules and Disciplinary Code as amended from time to time. Disciplinary action may ultimately lead to dismissal.

# Deviations from Policy

Unless specifically approved, any deviation from this policy is strictly prohibited. Any deviation to or non-compliance with this policy shall be reported to the Head of IT.

# Policy updating

This policy will updated annually.

Source acknowledgement: this document is largely based on the Back-Up Policy and Guidance, the Crown Estate, 2013