

## ICT Backup and Recovery policy

### 1. Scope

This policy covers all backup and recovery functions for the group (this includes Finchoice Africa) hereinafter referred to as Homechoice.

### 2. Purpose

The policy aims to protect data and systems at Homechoice and to achieve a balance between ensuring legislative compliance and service efficiency for continued operations.

### 3. Data backup standard

- 3.1 All backup data must be stored at a location that is physically different from its original creation and usage location.
- 3.2 Data must be stored offsite where possible and at a minimum of 6 kilometres away to prevent a single destructive event from destroying all copies of the data.
- 3.3 All backups must be made to a secure device from which it could be retrieved such as a Storage Area Network (SAN), reputable Cloud provider or tape.
- 3.4 All data must be secured so that it is only accessible by staff that may be required to retrieve it for recovery purposes. All backup procedures should be automated and decentralized (i.e. Wynberg, Blackheath, Jetpark, Azure and AWS).

### 4. Data backup selection

- 4.1 All data and software essential to the continued operation of Homechoice as well as all data that must be maintained for legislative purposes, must be backed up.
- 4.2 All supporting material required to process the information must be backed up as well. This includes programs, control files, install files, operating systems and documents.
- 4.3 The product owner will determine and document what information must be backed up, in what form, and how often.
- 4.4 It is the responsibility of the product owner to ensure that all legislative requirements are adhered to and met by the backup selection.

### 5. Backup schedule

- 5.1 Choosing the correct Backup Schedule:
  - 5.1.1 Backup schedules must not interfere with day to day operations. This includes any end of day or batch operations on the systems.
- 5.2 Frequency and time of data backup:
  - 5.2.1 When the data in a system changes frequently, backups needs to be taken more frequently to ensure that data can be recovered in the event of a system failure.
  - 5.2.2 Immediate full data backups are recommended when data is changed to a large extent.

## 6. Data backup owner

6.1 The Server Team Leader is the owner of all data backups and recovery. He or she must delegate two employees (one primary and one secondary) to commit and adhere to all backup and recovery policies, procedures and schedules.

## 7. Retention period

7.1 At a minimum data should be retained in line with current legislative requirements.

## 8. Recovery of backup data

8.1 Recovery procedures i.e. restores from tape must be documented and tested on a quarterly basis for all critical or key systems.

8.2 Outcomes of quarterly recovery tests must be documented and reviewed by the ISO.

## 9. Breach of policy

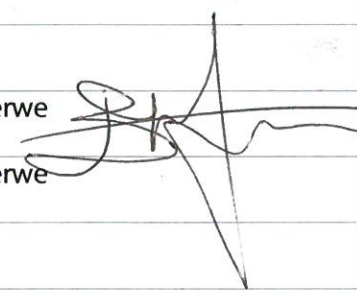

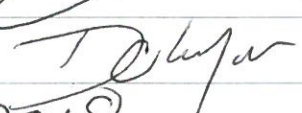
9.1 Any failure to comply with this policy may be subject to disciplinary action up to and including termination of employment.

## 10. Exceptions

10.1 Any exception to the policy must be approved by the Infosec Committee in advance.

## 11. Policy review

11.1 This policy will be reviewed by ICT Management as and when appropriate.

Document title	ICT Backup and Recovery policy
Version number	V1.0
Date published to intranet (if applicable)	
Author of document	Bernard van der Merwe 
Document expert	Bernard van der Merwe
Department	ICT
Authorised date	
Authorising authority (pre-approval)	André Mathee 
Authorising authority (final approval)	Dirk Oberholster 
Document review date	19/02/2018