ICT Physical Access Management Policy

1. Statement

This Policy applies to employees who require physical access to any room where Information Systems, such as network equipment (patch rooms) or server and storage equipment (computer rooms or data centres), are installed and is operated for any Company or Division within the HomeChoice Group (herein after referred to as the Company).

The purpose of this Policy is to ensure that only authorised employees gain access to the Company's physical information assets, UPS rooms and restricted areas. All such rooms are hereinafter referred to as secure areas.

2. Scope

This Policy is applicable to all employees at the Company's premises countrywide including, but not limited to, Head Office Wynberg, all Distribution Centres and Showrooms.

3. Access

3.1. Access should be restricted to employees whose job function require that they maintain the equipment and/or infrastructure located in a secure area.

3.2. Employees should be registered and granted access to a secure area via the Identity Access Management (IAM) system used by the Company.

3.3. Access to these rooms should be controlled by a card reader or biometric system which is administered by the Company's IAM system.

3.4. Access to secure areas must be reviewed by the Information Security Officer monthly.

3.5. Maintenance and repair employees who are required to remove equipment from the Company's premises must obtain written authorisation from the IT Manager.

3.6. Equipment that needs to be returned (not decommissioned, phased out or recycled) must be in the same physical condition, as it was prior to a fault or damage and within an agreed time period.

3.7. Device/s that contain data are not allowed to be removed from a secure area unless they have been factory reset or formatted with software from the department of defense.

3.8. In certain cases, devices will be transported from one secure area to another. Any employee required to perform such a task must have written approval from the IT Manager.

3.9. Third party maintenance and/or repair workers must adhere to the Company's confidentiality agreement requirements and are bound by the Company's standard non-disclosure agreement.

4. Visitors

Visitors to secure areas must be authorised by the IT Manager and accompanied at all times by an employee who has been granted permanent access to a secure area.

5. Breach of Policy

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

5.2. Any exceptions to the Policy must be approved by the Infosec Committee in advance.

6. Version Control

This is a non-contractual document and, as such, the Company reserves the right to modify this document at any time. Reasonable notice of any changes will be provided. Reasons for any modification may include employment legislation or other guideline changes.

Document title	ICT Physical Access Management Policy
Version number	V1
Author of document	Bernard van der Merwe
Document expert	Bernard van der Merwe
Department	ICT
Authorising authority (pre-approval)	Dirk Oberholster
Authorising authority (final approval)	HomeChoice Operating Board
Original authorisation date	01 October 2018
Date first published to intranet	29 October 2018