kruin.
—Huise wat Jesus volg —

# NG KERK KEMPTON KRUIN

# INFORMATION AND COMMUNICATIONS TECHNOLOGY ("ICT") POLICY

| | |
|---|---|
| **Document Ref.** | POPI-6 |
| **Version:** | 1.0 |
| **Dated:** | 29 June 2021 |

**Revision History**

| Version | Date | Revision Author | Summary of Changes |
|---|---|---|---|
| | | | |
| | | | |

**Distribution**

| Name | Title |
|---|---|
| | |
| | |
| | |

**Approval**

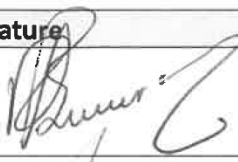
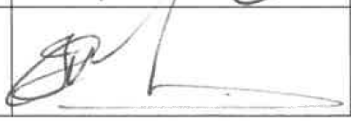
| Name | Position | Signature | Date |
|---|---|---|---|
| R J Burger | Head of Organisation |  | 29 June 2021 |
| J Marais | Information Officer |  | 29 June 2021 |

**TABLE OF CONTENTS**

## 1. PURPOSE

The purpose of this document is to provide Employees with an official protocol for the handling of customer, Organisation and third-party information. Furthermore, it defines the responsibility of the Employee with regards to the security of Organisation assets and the etiquette of Organisation communication. Furthermore, this policy will enforce and ensure minimum information and network security standards to prevent any misuse by its own users and outsiders.

## 2. DEFINITIONS

| | | |
|---|---|---|
| 2.1 | **"Organisation ITC Assets"** | Means any company-owned information, systems, hardware, software and other electronics used in the course of the company's business activities. |
| 2.2 | **"Organisation Data"** | Means any information relating to the Organisation, Confidential or Personal Information obtained in the course of the Employee's employment. |
| 2.3 | **"Confidential Information"** | Means: |

2.3.1 any information or data relating to the Organisation (even if not marked as being confidential, restricted, secret, proprietary or any similar designation), in whatever format and whether recorded or not (and if recorded, whether recorded in writing, on any electronic medium or otherwise), which by its nature or content is identifiable as-, or could reasonably be expected to be confidential and/or proprietary to the Company;

2.3.2 information relating to the Company's, existing and future strategic objectives and existing and future business plans and corporate opportunities, trade secrets, technical information, techniques, know-how, operating methods and procedures;

2.3.3 details of costs, sources of materials and customer lists (whether actual or potential) and other information relating to the existing and prospective customers and suppliers of the Company, pricing, price lists and purchasing policies;

2.3.4 computer data, programs and source codes, whether relating to the Organisation or a third party;

2.3.5 Intellectual Property that is proprietary to the Organisation and/or in respect of which it has rights of use or possession; and

2.3.6 Personal Information, as defined in section 1 of the Protection of Personal Information Act, No. 4 of 2013 processed or stored by the Organisation or the Employee.

| | | |
|---|---|---|
| 2.4 | **"Employee"** | Means any person employed by the Organisation and includes a volunteer providing services to the Organisation; |
| 2.5 | **"ICT Accessories"** | Means equipment provided by the Organisation to be used in conjunction with the Organisation ICT Assets, including, screens, cables, laptops, external drives and software licenses. |
| 2.6 | **"ICT – Information and Communications Technology"** | ICT is an extensional term for information technology (IT) that stresses the role of unified communications and the integration of telecommunication (telephone lines and wireless signals) and computers, as well as necessary enterprise software, middleware, storage, and audio-visual systems, that enable users to access, store, transmit, and manipulate information. |
| 2.7 | **"Information Compromise"** | Means any unauthorised access to the Organisation Data. |
| 2.8 | **"Organisation"** | Means NG Kerk Kempton Kruin, with PBO registration number 930 007 184, a nonprofit organisation duly registered and incorporated in accordance with the Nonprofit Organisation Act 71 of 1997 and having its registered address at 30 Fiskaal Str, Glen Marais, Kempton Park, 1619. |

## 3. ASSETS AND SECURITY

It is the responsibility of each Employee to protect the Organisation ITC Assets and to ensure that all assets are used responsibly, safely, and for the purpose that it is intended.

## 4. SECURITY MEASURES

4.1 Employees shall adhere to the following clear screen / clear desk guidelines:

4.1.1 **Use of locked areas:** lockable drawers, archive cabinets, safes, and file rooms should be used to store information media (e.g., paper documents, USB flash drives, memory cards, etc.) or easily transportable devices (e.g., cell phones, tablets, and notebooks) when not in use.

4.1.2 **Protection of devices and information systems**: computers and similar devices should be positioned in such a way as to avoid people passing by to have a chance to look at other Employee's screens, and configured to use time-activated screen savers and password protection. Additionally, information systems should be logged off when not in use. At the end of the day the devices should be shut down.

4.1.3 **Adoption of a paperless culture:** documents should not be printed unnecessarily.

4.1.4 **Disposal of information remaining in meeting rooms:** all information on white boards should be erased and all pieces of papers used during a meeting should be subject to proper disposal (e.g., by using a shredder).

4.1.5 **Safe destruction of documents:** documents containing Confidential Information must be safely destroyed as soon as it is no longer useful. Employees tasked with the destruction of documents are required to obtain a valid destruction certificate issued by an approved service provider.

4.2 The above guidelines shall apply to the office, and any alternative place of work, including but not limited to, a client's office, a conference facility, a venue at the Employee's home, if applicable.

## 5. CLIENT SYSTEMS AND ACCESS CREDENTIALS

5.1 Under no circumstances are passwords allowed to be stored unencrypted and/or in text files, excel spreadsheets, cell phones, MS Word documents, email or sticky notes.

5.2 All passwords are to conform to the "strong password characteristics" listed below.

5.3 Keep the following in mind when creating a password:

5.3.1 It should ideally have a minimum of 16 (Sixteen) characters;

5.3.2 It should not contain any of the Employee's personal information, more specifically their real name, user name or Organisation name;

5.3.3 It should not be similar to a previous password;

5.3.4 The Organisation recommends the use of long passphrases of randomly chosen words to ensure strong passwords. Commonly used phrases in popular ("pop") culture are not permitted.

## 6. SAFEGUARDING ORGANISATION DATA USED IN CONNECTION WITH ORGANISATION ITC ASSETS

6.1 The use of Organisation Data for any purpose other than the execution of the Employee's duties is strictly prohibited and subject to disciplinary action.

6.2 Employees shall not disseminate or permit the dissemination by any unauthorised third party of Organisation Data to any person, except with the prior written consent of The Company.

6.3 Employees are not allowed to store Organisation Data on any personal devices, except with the prior consent of The Company.

6.4 Employees shall not send Organisation Data to their personal email addresses or cloud storage applications (Dropbox, Google Drive etc.).

6.5 Upon termination of an Employee's employment for any reason, he shall afford The Organisation a reasonable opportunity to download the Organisation Data stored on his personal devices, if requested by The Company, and/or permanently delete same. The Organisation reserves the right to request reasonable proof of compliance with the aforementioned.

6.6 Employees are responsible for ensuring that any Organisation Data in their possession or under their control is safely and securely handled and stored.

## 7. SAFEGUARDING OF ORGANISATIONICT ASSETS

7.1 Organisation ITC Assets should remain in custody with the Employee as far as possible, and stored in a protective, case or bag when travelling by motor vehicle.

7.2 In the event that an Organisation ITC Asset is damaged, lost or stolen as a result of the Employee's negligence, the Employee will be held liable for the cost of repairs or the full value of an equivalent replacement.

7.3 Damage, loss or theft of a Organisation ITC Asset under circumstances contemplated in clause 7.2, may lead to:

7.3.1 disciplinary action being taken against the Employee; or

7.3.2 summary dismissal of the Employee, if the above is coupled with a reasonable and substantial risk of an information compromise.

## 8. INTERNET AND EMAIL USE

8.1 Access to- and use of- the Company's IT Network and related infrastructure is restricted to employees of The Company.

8.2 Employees will not allow any unauthorised access or use of the Company's IT Network and Infrastructure. Failure to comply with this clause may result in disciplinary proceedings being taken against the Employee.

8.3 The Employee shall not copy/forward/distribute any electronic communications or hard copies of any documents/files or the like generated or received in the office environment to an unauthorised third party. Failure to adhere thereto may lead to summary dismissal and the institution of criminal and civil proceedings against the Employee.

8.4 The Organisation reserves the right to restrict or otherwise control the internet usage of Employees on Organisation ITC Assets or ICT Accessories.

8.5 Any act of publication by means of any internet protocol expressing a personal opinion must reflect this fact.

8.6 The following practices are prohibited-

8.6.1 viewing, storing, downloading or forwarding images, moving images, sound files, texts or recordings that are sexually explicit or sexually suggestive, racist, harassing, intimidating or defamatory, except where this is both legal and there is demonstrable academic need to access or distribute such content;

8.6.2 hacking, including gaining or attempting to gain access to restricted resources either inside or outside of the Organisation computer network, except when authorised by management;

8.6.3 unauthorised downloading and sharing of copyrighted content using The Organisation equipment;

8.6.4 the use of torrent sites for downloading or sharing of copyrighted material, or seeding information from your computer (or similar device) to a torrent network;

8.6.5 Impersonating another user or another person, except if authorised by management for legitimate testing/trial purposes;

8.6.6 damaging or deleting files relating to any aspect of The Company, or of another user;

8.6.7 obtaining without authorization, the access codes and/or passwords of another user;

8.6.8 software piracy, or other infringement of intellectual property rights in digital content;

8.6.9 the sending, whether on the internal email system or externally, of bulk unsolicited mail, commercial advertising of other businesses, mail-flooding, or excessive cross postings on newsgroups (spam);

8.6.10 the use of any computer resource to promote any business or enterprise, except that of The Company;

8.6.11 issuing of unsolicited communications in any form or any other mediums of communication/social media platform to indicate or gain support for any religious or political purposes;

8.6.12 connecting a modem to the Organisation telephone network without authorization from management; and

8.6.13 use of a PC connected to the Organisation network without running virus detection software.

## 9. INFORMATION COMPROMISE

9.1 Should it be suspected that an Information Compromise data has occurred, then the discovering individual must report the incident immediately to the Company.

9.2 Should a password, pass-phrase, or key be believed to have been compromised, it must be changed immediately and the incident must be reported to The Company.

9.3 Any information compromises will be dealt with in accordance with The Company's Data Breach Management Policy.

## 10. USAGE AND COMMUNICATION ETIQUETTE

### 10.1 E-Mail and Instant Messaging

10.1.1 Employees must be mindful that they represent The Organisation when sending an email or instant message. Therefore, all outgoing emails and instant messages should be written professionally and should contain clear, understandable and appropriate content.

10.1.2 Employees must ensure that all emails are in the font, size and formatting prescribed by The Company.

10.1.3 Employees should avoid long discussions over email and/or instant messaging that may be best dealt with by a telephone call or face to face.

10.1.4 Employees are required to set up their email signatures and to add his/her Organisation photo to both his/her The Organisation email and Discord profile as directed by The Organisation from time to time.

## 11. RETURN OF ORGANISATION DATA AND ORGANISATION ITC PROPERTY

11.1 Upon termination of an Employee's employment for any reason, he shall immediately return all Organisation ICT Assets, ICT Accessories and Organisation Data to the Organisation in good and working condition.

11.2 In the event that an Employee's employment is summarily terminated, he will be required to leave the company's premises immediately and shall not be permitted to remove any Organisation ITC Assets or ICT Accessories from the premises.

# 6.(POPI-6) ICT POLICY (for approval)

Final Audit Report 2021-06-29

| | |
|---|---|
| Created: | 2021-06-29 |
| By: | Jacobus Marais (cobus@kruin-kerk.co.za) |
| Status: | Signed |
| Transaction ID: | |

## "6.(POPI-6) ICT POLICY (for approval)" History

Document created by Jacobus Marais (cobus@kruin-kerk.co.za)
2021-06-29

Document emailed to Roelof Jacobus Burger (roelf@skybegsol.co.za)
2021-06-29

Email viewed by Roelof Jacobus Burger (roelf@skybegsol.co.za)
2021-06-29

Document signed by Roelof Jacobus Burger (roelf@skybegsol.co.za)
Signature Date: 2021-06-29

Agreement completed.
2021-06-29