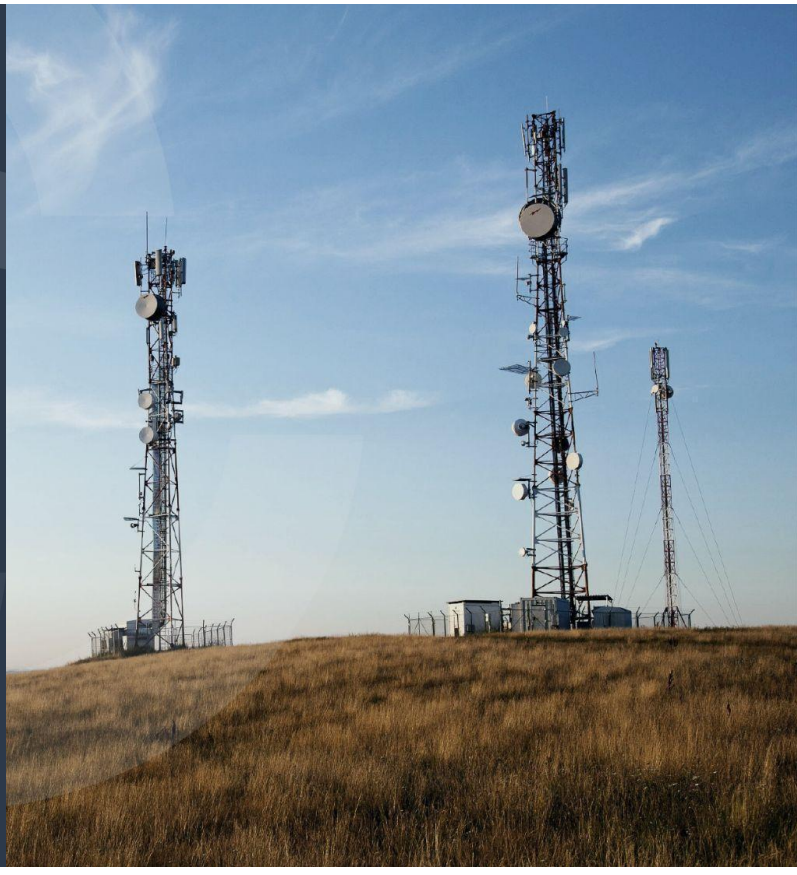
t) +27 10 500 1414 **e)** sales@izwi.co.za | support@izwi.co.za
Unit 13, Tyger Chambers II, Willie van Schoor Ave, Tygervalley, 7530

INTERNAL USE

Acceptable Use Policy



Introduction

This document defines the appropriate use of information, information technology ("IT") resources and effective security of those resources which require the participation and support of Izwi Technology Group's (Izwi) workforce. Inappropriate use exposes Izwi to potential risks including virus attacks, compromise of network systems and services, and legal issues.

This policy applies to anyone employed directly (e.g. full time staff, interns, work placements, etc.), or indirectly (e.g. independent contractors, consultants, or temporary employees); collectively referred to as "Individuals" or "users", who use any system's information or physical infrastructure regardless of its form or format, created or used to support Izwi.

Scope

This policy must be included in the induction of new employees of each Izwi business unit, having their reading acknowledgement collected and its communication must be reinforced at least annually.

It is the user's responsibility to read and understand this policy and to conduct their activities in accordance with its terms.

Compliance

This policy shall take effect upon publication. Compliance is expected with all Izwi policies and standards. Policies and standards may be amended at any time.
Izwi operates various monitoring systems to preserve the security and integrity of its information systems.
Individuals shall not have privacy expectations for any content created, sent, received or stored in email systems, other than where it is annotated Confidential / Private in the subject line.
Izwi's monitoring activities (based on the principles of proportionality, relevancy, data minimisation and operational necessity) also respect your dignity and fundamental rights, comply with our policies and applicable data protection laws. We reserve the right to:

a. Monitor electronic systems, including conducting periodic reviews, to verify its use is in accordance with legitimate business purposes, adheres to corporate policies and ethical standards.
b. Prevent the unauthorised and unintentional disclosure of business information.
c. Assess, review and audit the use of business systems and technologies.
d. Review email contents and social media posts, including associated attachments (see note below*).
e. Record some telephone systems, meetings, presentations and training sessions with designated staff authorised to listen to the recording for the purposes of staff training, quality control, investigations relating to complaints, incidents and problem resolution.
f. Monitor access to company property which may include, but is not limited to:
    i. CCTV at premises access points and other sensitive areas;
    ii. Proximity card reader readers, swipe card readers, key fobs or other controls at entrance / exit points;
    iii. Written visitor logs recording access to premises and controlled facilities within them.

g. Where an individual is unexpectedly absent for a period of time and there is an operational necessity to access emails or other work files used and/or held by the individual another person can be authorised through the Managing Director or Technical Director to access specific items in order that relevant actions in the business interest can be taken. The absent individual is to be informed of such activity on their return to work.

Opening mailboxes or accessing IT equipment for investigation requires authorisation by Izwi management on a case-by-case basis according to a specified data access procedure – only subsequently can an individual's mailbox, hard disk, network drive, relevant backups, mobile device (company provided laptop and/or mobile phone along with any backups or links to cloud storage sites) be subject to search and analysis.

Izwi may impose restrictions, at the discretion of their executive management, on the use of a particular IT resource. For example, Izwi may block access to certain websites or services not serving legitimate business purposes or may restrict user ability to attach devices to Izwi's IT resources (e.g., personal USB drives).

Users accessing Izwi's applications and IT resources through personal devices must only do so with prior approval or authorisation from Izwi.

Violations of corporate policies, whether known or suspected, may be investigated, and subject to the findings of the investigation, individuals may be sanctioned in accordance with respective legislation. This in turn may result in action up to and including dismissal, or the termination of contracts for contractors, temporary staff or third parties.

Depending on the nature of the offence that has occurred, Izwi reserves the right, in the most extreme circumstances, to consider pursuing legal action against offenders.

Exception Process

If compliance with this standard is not feasible or technically possible, or if deviation from this policy is necessary to support a business function, entities shall request an exception through the Director/s exception process. Requests should be sent to the Director/s formally via email to the following addresses

francois@izwi.co.za
rafeeq@izwi.co.za

Users may be exempted from one or more of these restrictions during their authorised job responsibilities, after approval from Izwi management (e.g., storage of objectionable material in the context of a disciplinary matter).

Personal Use

Izwi's IT resources are primarily for business purposes which are a privilege not a right; and must not be abused. Izwi may revoke or limit this privilege at any time. Occasional and necessary personal use of Izwi's IT

resources is permitted, provided such use is otherwise consistent with this policy; is limited in amount and duration; and does not impede the ability of the individual or other users to fulfil Izwi's responsibilities and duties, including but not limited to, extensive bandwidth, resource, or storage utilisation.

Individual Accountability

Individual accountability is required when accessing all IT resources and Izwi information.

Everyone is responsible for protecting against unauthorised activities performed under their user ID and for safeguarding business information from unauthorised access. This includes clearing your desk and locking your computer screen when you walk away from your system, and protecting your credentials (e.g., passwords, tokens or similar technology) from unauthorized disclosure.

Credentials must be treated as confidential information and must not be disclosed or shared.

Transmission and Storage of Information

Users must not transmit restricted Izwi, non-public, personal information from third parties, private, sensitive, or confidential information to or from personal email accounts (e.g., Gmail, Hotmail, Yahoo) or use a personal email account to conduct Izwi's business unless explicitly authorised.

Users must not store restricted Izwi, non-public, personal information from third parties, private, sensitive, or confidential information on a non-Izwi issued device, or with a third-party file storage service that has not been approved for such storage by Izwi.

Devices that contain Izwi's information must be attended at all times or physically secured and must not be checked in transportation carrier luggage systems.

Guidelines for Personal Use of Social Media

Staff should be sensitive to the fact that information posted on social media sites clearly reflects on the individual and may also reflect on the individual's professional life. As a reminder, no employee is allowed to issue statements or opinions about the Izwi brand or business where their employment status could be viewed by the message recipient as that of an Izwi company representative.

Consequently, staff should use discretion when posting information on these sites and be conscious of the potential perceptions of and responses to the information. It is important to remember that once information is posted on a social media site, it can be captured and used in ways not originally intended. It is nearly impossible to retract, as it often lives on in copies, archives, backups, and memory cache.

Users should respect the privacy of Izwi's staff and not post any identifying information of any staff without permission (including, but not limited to, names, addresses, photos, videos, email addresses, and phone numbers). Users may be held liable for comments posted on social media sites.

Users should not use their personal social media accounts for official business, unless specifically authorised by the organisation. Users are strongly discouraged from using the same passwords in their personal use of social media sites as those used on Izwi devices and IT resources, to prevent unauthorized access to resources if the password is compromised.

User Responsibility with IT Equipment

Users are routinely assigned or given access to IT equipment in connection with their official duties. This equipment belongs to Izwi and must be immediately returned upon request or at the time an employee is separated from the organisation.

Users may be financially responsible for the value of equipment assigned to their care if it is not returned to Izwi. Should IT equipment be lost, stolen or destroyed, users are required to provide a written report of the circumstances surrounding the incident.

Acceptable Use

All uses of information and information technology resources must comply with Izwi's policies, standards, procedures, and guidelines, as well as any applicable license agreements and laws including Federal, State, local and intellectual property laws.

Consistent with the foregoing, the acceptable use of information and IT resources encompasses the following duties:

- Understanding the baseline information security controls necessary to protect the confidentiality, integrity, and availability of information;
- Protecting Izwi's information and resources from unauthorised use or disclosure;
- Protecting personal, private, sensitive, or confidential information from unauthorised use or disclosure;
- Observing authorised levels of access and utilising only approved IT technology devices or services; and
- Immediately reporting suspected information security incidents or weaknesses to the appropriate manager and a designated Information Security representative.

Unacceptable Use

The following list is not intended to be exhaustive but is an attempt to provide a framework for activities that constitute unacceptable use.

Unacceptable use of information or information technology resources includes, but is not limited to the following:

- Unauthorised use or disclosure of personal, private, sensitive, and/or confidential information, including the sending unencrypted customer credit/debit card details (i.e. full card number, also referred to as PAN – Primary Account Number);
- Unauthorised use or disclosure of Izwi information and resources;
- Distributing, transmitting, posting, or storing any electronic communications, material or correspondence that is threatening, obscene, harassing, pornographic, offensive, defamatory, discriminatory, inflammatory, illegal, or intentionally false or inaccurate;
- Circulation and dissemination of copyright materials (including articles and software) without appropriate authority;
- Attempting to represent Izwi in matters unrelated to official authorised job duties or responsibilities;
- Connecting unapproved devices to Izwi's network or any IT resource;
- Connecting Izwi IT resources to unauthorised networks;
- Bridging networks by connecting simultaneously to wireless and wired networks;
- Installing, downloading, or running software that has not been approved following appropriate security, legal, and/or IT review in accordance with Izwi policies;
- Using Izwi's IT resources to circulate unauthorised solicitations or advertisements for non-Izwi purposes including religious, political, or not-for profit entities;
- Providing unauthorised third parties, including family and friends, access to Izwi's IT information, resources or facilities;
- Using Izwi IT information or resources for commercial or personal purposes, in support of "for-profit" activities or in support of other outside employment or business activity (e.g., consulting for pay, business transactions);
- Gaining or attempting to gain unauthorised access to another workstation, computer network, system or application within the corporate computer resources;
- Using work email address and credentials to sign up for applications and accounts on external websites for personal use, or using private email accounts (e.g. Hotmail, Yahoo, Gmail, etc.) for business purposes;
- Disrupting or attempting to disrupt the proper functioning of any computer equipment, system or application, including altering, tampering with, disabling or otherwise disrupting any anti-virus, malware protection systems or any other security features;
- Propagating chain letters, fraudulent mass mailings, spam, or other types of undesirable and unwanted email content using Izwi IT resources; and
- Tampering, disengaging, or otherwise circumventing Izwi or third-party IT security controls.

Reference Documentation

ID	*Name*	*Link*

Change / Review Control

Issue	Author	Reason for Change	Change Date
1.0	Francois Swart	Document Creation	01 March 2022

getting you connected.