The Compensation Claims Management System (CCMS)

Lodgement Service Provider System Requirements

TABLE OF CONTENTS

1. INTRODUCTION

Lodgement of Mine workers/Claimants currently happen at decentralized lodgement sites. The lodgement process requires/allows that living Mine workers be medically examined on or nearby lodgement site.

The Mine Workers are administratively lodged and managed by the CCMS system on site and the medical examination reports and outcome needs to be captured and up- or downloaded onto CCMS from the medical provider systems.

2. INFORMATION SECURITY

The TSHIAMISO TRUST recognizes its dependence on applications, systems and information for the effective operation of its function for claims management. It is essential that information and any supporting infrastructure and systems be secured against all measurable threats such as unplanned destruction, unauthorized access, fraud, inadvertent error, and breach of confidentiality, lack of integrity and unavailability of systems. To this effect the Trust has put in place an ICT policy framework whose objective is to

- provide a secure and effective Information and Communications Technology (ICT) based Information Security environment
- ensure all information assets when in electronic form are continuously available and protected to a level commensurate with the assessed risk and value/classification of the asset.
- define standards for the defense against unauthorised access, use, modification, disclosure, damage or destruction of information assets.
- mandate processes to minimise risks associated with disruption or failure of ICT systems.

The Information Technology Policy framework provides a consistent approach that reflects the TSHIAMISO TRUST ’s culture, and is implemented to provide management direction and support for information security, applications and systems.

This policy framework provides an Information security regulatory framework to ensure the Tshiamiso Trust meets its obligations to protect and safeguard official information assets as set out in, but not limited to, the following legislation and authorities including but not limited to **The South African National Cybersecurity Framework**, **SOX**, **ISO/IEC 27001** – Information Security Management, **ISO/IEC 27002** – Code of Practice for Information Security Practice , **ISO/IEC 31000** - Risk Management, **POPIA** and **GDPR**

This policy framework must be observed by all Tshiamiso Trust employees, contractors, consultants, service providers and agents of the Tshiamiso Trust, and incorporated bodies.

It applies to all ICT assets including but not limited to:

- physical or logical computing devices either owned, leased, or used by the Tshiamiso Trust to hold or process Tshiamiso Trust electronic information.
- cloud services and outsourced ICT solutions, and
- ICT hardware, software and operating systems
- any electronic information held on those assets.

The applicable policy documents are available on request and by acting for and or processing the Trust's IT you agree to observing and complying with these policies and thus failure to comply with these policies will result in disciplinary action under the terms and conditions of the contract of engagement or prosecution under the appropriate Act.

3. SCOPE

This document focusses on the high-level IT infrastructure requirements for lodgement service providers.

4. LODGEMENT DOMAINS

Recommended lodgement stations depending on size of lodgement site:

- Small site: One lodgement officer, would require only one station
- Medium/Large site: 2 lodgement officers required

It is also required that an officer is stationed at the entrance scanning mineworkers for infectious disease symptoms which must also be uploaded to CCMS.

The stations need to be connected to CCMS and need be equipped with a signature pad, fingerprint reader, external webcam, access to printer/scanner and internet access to CCMS.

Workstation minimum recommended spec:

Type	Product	Comment
Workstation	The following hardware serves as examples and the make are not prescribed. Provider can procure similar in specification (PC or Notebook) • Lenovo Idea center 520 All-In-One • HP All-in-One 200 G3 Standalone Workstation • CPU: INTEL i5 or higher; • Ram: 8GIG; • HDD: 1T 720rpm; • OS: WIN10 (Home/Pro); • 21" screen; and • Build in Camera to read QR codes. Or Notebook • CPU: INTEL i5 or higher;	Stations: 1 x Per station If SSD drives are installed, CPU and RAM requirements can be less: I3, 4G Ram

Type	Product	Comment
	• Ram: 8GIG; • HDD: 1T 720rpm; • OS: WIN10 (Home/Pro); • 21” screen; and • Build in Camera to read QR codes.	
Fingerprint scanner/reader	Morpho Biometric Reader Model: MSO 300 NB: E-Verify software must be installed on device	1 x Per station These devices must match exact specifications
Signature pad, USB	Wacom LCD Signature Pad Model: STU-430	1 x Per station These devices must match exact specifications
Camera, USB	Any windows compatible camera to scan QR code if miner do not have fingerprints	1 x Per station
Multifunction Printer scanner	Preferably a laser jet printer/scanner, inkjet printers are not recommended	If devices are shared between workstations the printer must be network shared to simplify scanning of documents and upload thereafter.
Services	IT maintenance & support (hard and software/anti-virus) Internet access Email (If applicable)	These are services required from service providers.

5. INFRASTRUCTRE REQUIREMENTS

The facility should cater for the following:

- Power:
  - Access to single phase power
  - Backup power if main building cannot provide
  - UPS per workstation would be advantageous

- Internet connectivity, if GSM: LTE (External aerial recommended)
  - To CCMS, httsp://ccms.co.za
  - To service provider's own IT systems
  - Minimum bandwidth of 5 Mbps (recommended 10 Mbps)

- Printing and scanning (Laser Jets are more reliable). It's critical that lodgement officers have easy access to a reliable multi-function printers (MFP). Each claimant often has multiple documents which requires scanning, and this process normally takes the longest to do, thereafter the scanned pdf files need to be available to lodgement officer's workstation for CCMS uploading.

6. SITE READINESS SIGN-OFF

A. FACILITY IDENTIFICATION

B. EQUIPMENT AND FUNCTIONALITY SIGN OFF

Item	Tested component	Confirmed working Yes/No
1	**Facility infrastructure**	
	Power stable	
	Internet connectivity	
	CCMS connectivity	
2	**Lodgement CCMS Workstation #1 allocation**	
2.1	OS = WIN 10	
2.2	Fingerprint reader allocated and functional	
2.3	Signature pad installed and functional	
2.4	Workstation camera external available and functional	
2.5	CCMS connectivity	
2.6	Lodgement Transactions tested	
2.7	Printer scanner functional Can scanned documents be access by lodgement station/stations	
3	**Lodgement CCMS Workstation #2 allocation**	
3.1	OS = WIN 10	
3.2	Fingerprint reader allocated and functional	
3.3	Signature pad installed and functional	
3.4	Workstation camera external available and functional	
3.5	CCMS connectivity	
3.6	Lodgement Transactions tested	

Item	Tested component	Confirmed working Yes/No
3.7	Printer scanner functional Can scanned documents be access by lodgement station/stations	
4	**Lodgement CCMS Workstation #3 allocation**	
4.1	OS = WIN 10	
4.2	Fingerprint reader allocated and functional	
4.3	Signature pad installed and functional	
4.4	Workstation camera external available and functional	
4.5	CCMS connectivity	
4.6	Lodgement Transactions tested	
4.7	Printer scanner functional Can scanned documents be access by lodgement station/stations	

C. READINESS SIGN OFF

Service Provider Technical	Name of Engineer:	Signature:	Date:
Service Provider Management	Name of Manager:	Signature:	Date:
Tshiamiso Trust Management	Name of Manager:	Signature:	Date: