



a world class African city



TITLE	STANDARD FOR TRELLIX ENDPOINT LICENSES' RENEWAL, MAINTENANCE, AND SUPPORT	REFERENCE	REV
		CP_TSSTAN_187	1
		DATE:	AUGUST 2025
		PAGE:	1 OF 10

TABLE OF CONTENTS

FOREWORD..... 3

INTRODUCTION 4

1. SCOPE OF WORK..... 4

2. NORMATIVE REFERENCES 4

3. DEFINITIONS 5

4. TECHNICAL REQUIREMENTS 5

5. TRAINING 6

6. SUPPORT AND MAINTENANCE 6

7. DOCUMENTATION 7

8. QUALITY MANAGEMENT 8

9. HEALTH AND SAFETY 8

10.ENVIRONMENTAL MANAGEMENT 8

ANNEXURE A – BIBLIOGRAPHY 9

ANNEXURE B - REVISION INFORMATION 10

FOREWORD

This Request for Standard Services was prepared by the following Work Group member/s:

Mphethe Andries Mokoakoe	ICT Security
--------------------------	--------------

The work group was appointed by ICT Leadership, which at the time of approval comprised of the following members:

Lawrence Nengovhela	ICT Services
Humbulani Manyaga	ICT Services
Happiness Manzini	ICT Services
Sifiso Mtshali	ICT Services

Recommendations for corrections, additions or deletions shall be addressed to the:

General Manager: ICT
City Power Johannesburg (SOC) Ltd
P O Box 38766
Booyens
2016

1. INTRODUCTION

The objective of this document is to specify the intent of City Power to procure licenses for the Trellix Endpoint Security products, which include (Agent, Application Control, Data Exchange Layer (DXL), Threat Intelligence Exchange (TIE), Data Loss Prevention (DLP), Database Security, ePolicy Orchestrator - On-prem, Endpoint Security (ENS) – Platform, Firewall, Adaptive Threat Prevention, Threat Prevention, Web Control, Threat Intelligence, Trellix Client Proxy, Trellix Drive Encryption, and Advanced Threat Defense Appliances).

Trellix ePO (ePolicy Orchestrator) platform, Trellix ENS (Endpoint Security) licenses, and software licenses for Trellix Advanced Threat Defense (ATD) Appliances, along with associated support services. Trellix ePO provides centralized management for endpoint security products. Trellix ENS provides comprehensive endpoint protection against a wide range of threats, including malware, ransomware, and exploits. Trellix ATD provides advanced sandboxing and threat analysis to detect and prevent zero-day attacks and highly evasive malware.

The Advanced Threat Defense (ATD) set of appliances that City Power had bought in the past. The devices are currently not operational and hence not of any use to City Power as they are not licensed, and their support has also expired. This Trellix Advanced Threat Defense (ATD), formerly known as McAfee Advanced Threat Defense is a powerful security solution that will help the City Power ICT Security Team detect advanced, evasive malware and take immediate action to protect their systems.

2. SCOPE OF WORK

The scope of work shall include the following:

- A. The supply and installation of licenses for the Trellix Endpoint Security products and solution listed above.
- B. Installation and integration with other products and solutions.
- C. Assessment and the optimal configuration of the solution for the City Power environment.
- D. The licenses, support, and maintenance shall remain valid for the duration of the contract.

NB: All the solutions' deployment should adhere to the recommended best practices provided by the respective OEM.

3. NORMATIVE REFERENCES

The following documents contain provisions that, through reference in the text, constitute requirements of this specification. At the time of publication, the editions indicated were valid. All standards and specifications are subject to revision, and parties to agreements based on this standard are encouraged to investigate the possibility of applying the most recent editions of the documents listed below.

COBIT: *Control Objectives for Information and Related Technology. It is a framework created by the ISACA (Information Systems Audit and Control Association) for IT governance and management*

KING IV: *Technology and Information Governance*

TOGAF: *The Open Group Architecture Framework is a framework for enterprise architecture that provides an approach for designing, planning, implementing, and governing an enterprise information technology architecture.*

POPI Act: *Protection of Personal Information Act, 2013*

GWEA: *Government Wide Enterprise Architecture framework*

4. DEFINITIONS

The definitions and abbreviations in the above document (Normative Reference) shall apply to this specification. In addition, the following terms and acronyms are used in this document:

Trellix ePO provides centralized management for endpoint security products.
Trellix ENS provides comprehensive endpoint protection against a wide range of threats, including malware, ransomware, and exploits.
Trellix ATD provides advanced sandboxing and threat analysis to detect and prevent zero-day attacks and highly evasive malware.

5. REQUIREMENTS

5.1 General Requirements.

City Power Johannesburg requires a robust and integrated cybersecurity platform to address the following challenges:

- 5.1.1 Increasing sophistication of cyber threats targeting critical infrastructure.
- 5.1.2 Need for unified management and visibility across all endpoints.
- 5.1.3 Requirement for advanced threat detection and analysis capabilities to combat evolving threats.
- 5.1.4 Overloaded security teams struggling with alert fatigue and manual investigations.
- 5.1.5 Need for consolidated reporting and executive dashboards to inform decision-making.

5.2 Technical Requirements

The solution should provide centralized control and management of endpoint security policies and deployments through ePO, streamlining operations. ENS offers multi-layered protection, including anti-malware, firewall, and web control, to secure endpoints effectively. ATD's sandboxing technology provides a crucial layer of defence against unknown threats by analysing suspicious files in a safe environment before they can impact the network. Integration between ePO, ENS, and ATD ensures a cohesive security posture, allowing for automated threat intelligence sharing and rapid response.

- 5.2.1 Sufficient licenses to cover all required endpoints and ATD appliances.
- 5.2.2 Integration with existing SIEM, SOAR, IAM, and ITSM platforms.
- 5.2.3 Executive dashboards and reporting for compliance and management oversight.
- 5.2.4 Adherence to industry best practices for endpoint security and threat detection.

6. TRAINING

- 6.1 City power requires the necessary training for system administrators.
- 6.2 The Service Provider shall clearly outline the layout of the recommended enhanced training.
- 6.3 The solution provider shall work closely with City Power's resources during the implementation in a live environment to ensure practical knowledge transfer.
- 6.4 Training shall be on-site and form part of the implementation process.
- 6.5 The Service Provider shall also be required to provide training to City Power technical representatives on the system when enhanced features and functionality become available as the system is upgraded at no cost.
- 6.6 The suppliers shall provide technical support on system and equipment queries for the duration of the contract as of the go-live date of the implemented solution at no cost.

7. SUPPORT AND MAINTENANCE

The Service Provider shall provide support and maintenance services on the proposed solution.

7.1 Support Desk

- 7.4.1 The Service Provider shall provide the Support Centre which shall be a single point of contact for the resolution of system problems.
- 7.4.2 Support requests shall be submitted by phone, email or on a support portal.
- 7.4.3 The Service Provider shall respond to all support requests.
- 7.4.4 The Support Centre shall be available for support requests on Monday to Friday from 08:00 AM – 5:00 PM (each "Business Day") and on Standby after-hours including weekends and public holidays.
- 7.4.5 The Support Centre shall be responsible to perform the following functions:
 - 7.4.5.1 Document all support all logged requests and issue a reference number for each incident.
 - 7.4.5.2 Monitor and manage the resolution of incidents from the initial support request to resolution.
 - 7.4.5.3 Route incidents to the appropriate resource for resolution.
 - 7.4.5.4 Perform problem diagnosis.
 - 7.4.5.5 Answer queries regarding the usage and performance of the system.
 - 7.4.5.6 Access the system remotely for diagnosis and correction of problems.
 - 7.4.5.7 Contact the City Power Representative at regular intervals to provide status and/or resolution of problems.

7.2 City Power's responsibilities. shall be responsible for the following functions:

City Power shall provide 1st line support, which entails the following:

- 7.2.1 Response to End-user queries regarding the usage or performance of the system.
- 7.2.2 Resolve system problems with support from the Service Provider where necessary.
- 7.2.3 Swap defective Hardware components using spare parts.
- 7.2.4 Hand over complex system problems to the Service Provider through the Support Desk.
- 7.2.5 File a support request with the Support Desk for software and hardware support.

**STANDARD FOR TRELLIX ENDPOINT
LICENSES' RENEWAL, MAINTENANCE, AND
SUPPORT**

REFERENCE
CP_TSSTAN_187
PAGE 7

REV
1
OF 10

- 7.2.6 Inform and update the service provider of all information related to the encountered software or hardware problem.

7.3 ON-SITE SUPPORT

On-site support shall be the responsibility of the service provider. The support shall be linked to the SLA.

7.4 SYSTEM MAINTENANCE

- 7.4.1 The Service Provider shall perform on-site routine system maintenance once every week, the weekly site visits shall include but not be limited to the following:
- 7.4.2 General routine checks of the system status.
- 7.4.3 Resolving system alarms.
- 7.4.4 Routine tests the of the equipment's performance against the relevant equipment specifications.

7.5 SOFTWARE UPGRADE

- 7.5.1 The Service Provider shall be responsible for providing software upgrades as may be required to fix bugs; introduce added functionality; and keep the system fully functional.
- 7.5.2 Upgrades shall be made available either on-premises or via a VPN connection.

**7.6 INCIDENT MANAGEMENT
PRIORITY AND RESPONSE TIMES**

TABLE: A PRIORITY LEVEL RATING OF ALL SUPPORT QUERIES IS AS PER TABLE BELOW:

PRIORITY	DESCRIPTION	CONDITION
1	Critical	Total system failure
2	High	Unavailability of major system functionality
3	Medium	Unavailability of minor system functionality
4	Low	All configurations and minor ad hoc programming on request
5	Configuration and programming	Includes all configurations and minor ad hoc programming on request

TABLE B RESPONSE TIMES SHALL BE AS FOLLOWS:

PRIORITY	RESPONSE TIME	COMMENCEMENT	FEEDBACK	MAXIMUM TIME TO REPAIR
1	½ HR	1 HR	ON SITE	4 HOURS
2	1 HRS	2 HRS	ON SITE	5 HOURS
3	2 HRS	3 HRS	ON SITE	6 HOURS
4	6 HRS	8 HRS	DAILY	12 HOURS
5	24 HRS	36 HRS	DAILY	48 HOURS

8. DOCUMENTATION

The Service Provider/s shall provide all documentation required that includes but is not limited to manuals, licenses, and catalogues. Documentation shall be in both hard and soft copy.

9. QUALITY MANAGEMENT

A quality management system/plan shall be set up to assure quality during manufacture, installation, removal, transportation, and disposal. Guidance on the requirements for a quality management system may be found in the following standards: ISO 9001:2015. The details shall be subject to an agreement between the purchaser and the supplier.

10. HEALTH AND SAFETY

A health and safety system/plan shall be set up to ensure proper management and compliance during manufacture, installation, removal, transportation, and disposal. Guidance on the requirements of a health and safety plan shall be found in ISO 45001:2018 standards. The details shall be subject to an agreement between City Power and the Supplier.

11. ENVIRONMENTAL MANAGEMENT

An environmental management system/plan shall be set up to ensure the proper environmental management and compliance is adhered to during manufacturing, installation, removal, transportation, and disposal. Guidance on the requirements for an environmental management system shall be found in ISO 14001:2015 standards. The details shall be subject to an agreement between City Power and the Supplier. This is to ensure that the asset created conforms to environmental standards and City Power SHERQ Policy.

ANNEXURE A – BIBLIOGRAPHY

None

ANNEXURE B - REVISION INFORMATION

DATE	REV. NO.	NOTES
September 2024	0	First issue
August 2025	1	Second issue General editing