
TABLE OF CONTENTS

FOREWORD

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

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

Mphethe Andries Mokoakoe	Information Communication Technology

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

Humbulani Manyaga	Information Communication Technology
Happiness Manzini	Information Communication Technology
Khathu Muambadzi	Information Communication Technology

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

Research and Development General Manager
City Power Johannesburg (Pty) Ltd
P O Box 38766
Booysens
2016

INTRODUCTION

City Power hereby requires the services of an ICT Security Services Partner (Managed Security Service Provider) that has expertise in the provisioning of ICT security solutions and services. The implemented solution must prevent malicious attacks, information leaks, and business disruptions resulting from cyberattacks. These services are requested from experienced and certified/accredited ICT Service Providers. Systems that are not adequately protected are prone to cyber threats and attacks. City Power's ICT Security infrastructure requires the latest solutions to augment or replace our current endpoint security.

1. SCOPE OF WORK

The Appointed Service Provider must provide ICT Security Services that shall cover and protect all Workstations and Servers located in Reuven Head Office and all our Depots. We have a Data Centre located in Reuven that hosts our virtual environment and physical servers. We also have a Roodepoort DR Data Centre. We have 1600 users with laptops and computers working from City Power offices or working from home. There are over 400 servers hosted on both Data Centres.

The Service Provider shall ensure Licensing of all software, provide support and maintenance for all ICT requirements, and ensure a secure working environment.

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

2. 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*

3. 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:

Term	Meaning
ICT	Information and Communication Technology
SLA	Service Level Agreement
IT	Information Technology
DR	Disaster Recovery
IPS	Intrusion Prevention
SCCM	System Centre Configuration Manager
MAOS	Management of Outage and Supply
ITIL	Information Technology Infrastructure Library
SOC	Security Operation Centre
AAA	Authentic Authorization Accounting
SIEM	Security Information and Event Management
TACACS/RADIUS	Access Control Security Protocols
NAC	Network Admission Control
ISE	Identity Service Engine
NAT	Network Address Translation
NGFW	Next Generation Firewall
URL	Uniform Resource Locator
GB	Giga Byte
GBPS	GB per second
3DES	3-pass Digital Encryption Standard
AES	Advanced Encryption Standards
IPsec	Internet Protocol Security
CMDB	Configuration Management Database
VPN	Virtual Private Network
IoT	Internet of Things
OT	Operational Technology

4. REQUIREMENTS

4.1 General Requirements

The following requirements should be considered in the proposal to strengthen City Power security:

4.1.1 Endpoint Protection for Windows, MacOS, and Linux
4.1.2 Data Loss Prevention
4.1.3 Email Security and Mail Filtering
4.1.4 Advanced Threat Prevention
4.1.5 Host Intrusion Prevention Systems
4.1.6 Network Intrusion Prevention Systems
4.1.7 Endpoint web control and firewall
4.1.8 Database Security
4.1.9 Threat Intelligence Exchange
4.1.10 Shadow IT and IoT security
4.1.11 IoT and OT security
4.1.12 Backup Security
4.1.13 DNS Security
4.1.14 Multifactor Authentication

4.2 Technical requirements

4.2.1 Endpoint Protection for Windows, MacOS, and Linux

A solution (may also include XDR/MDR – Extended Detection and Response/Managed Detection and Response solution) that converges endpoint device security functionality into a single product that delivers Centralized Management, antivirus, anti-spyware, application control, Host Intrusion prevention system, Endpoint web control, Endpoint firewall, OT endpoint security, Crypto Guard anti-ransomware, Rollback Remediation, machine learning and Dynamic Application Containment.

4.2.2 Data Loss Prevention.

Data Leak Prevention solution that includes Device Types Control, Ports Secured, Network Communications Monitoring, Clipboard Control, Data Categorization, Content Discovery and Filtering, Encryption Integration, and Cloud storage monitoring.

4.2.3 Email Security and Mail Filtering

Email Security solution that has Anti-Spam, Phishing protection, Inbound Email Filtering, Outbound Filtering, Malware detection, Impersonation Protection, Attachment Protection suspicious contents blocking.

4.2.4 Adaptive Threat Prevention

Advanced Threat Defense Appliances are designed to analyze suspicious files for malware and sandboxing for dynamic analysis of file behaviour.

4.2.5 Database Security

Real-time Database protection, Database vulnerability, protection against SQL injection, and Database Activity Monitoring.

4.2.6 DNS Security

A solution that offers DNS-layer security, malicious IP blocking, selective web inspection, and app visibility/control to block malware, easily enforce content web filtering, and enable secure cloud adoption.

4.2.7 Multifactor Authentication

This solution provides secure and flexible user authentication. It uses adaptive MFA, offers password-less sign-in, provides login analytics, and automatically routes users to their correct identity provider.

4.2.8 Network Intrusion Prevention Systems/Network Detection and Response

An application (including firewalls) that protects the network against stealthy attacks and monitors east-to-west traffic.

4.3 **Enhancements**

The Service Provider shall provide enhancements, support, and maintenance services for existing and future ICT Security solutions. Below enhancements shall be provided as and when needed.

4.3.1 Forensic services as and when required.

4.3.2 ICT risk detection and treatment services.

4.3.3 Penetration testing.

5. TRAINING

5.1 City power requires the necessary training for system administrators.

5.2 The Service Provider shall clearly outline the layout of the recommended enhanced training.

5.3 The solution provider shall work closely with City Power’s resources during the implementation in a live environment to ensure practical knowledge transfer.

5.4 Training shall be on-site and form part of the implementation process.

5.5 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.

5.6 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.

6. SUPPORT AND MAINTENANCE

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

6.1 Support Desk

6.1.1 The Service Provider shall provide the Support Centre which shall be a single point of contact for the resolution of system problems.
6.1.2 Support requests shall be submitted by phone, email or on a support portal.
6.1.3 The Service Provider shall respond to all support requests.
6.1.4 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.
6.1.5 The Support Centre shall be responsible to perform the following functions:
6.1.5.1 Document all support all logged requests and issue a reference number for each incident.
6.1.5.2 Monitor and manage the resolution of incidents from the initial support request to resolution.
6.1.5.3 Route incidents to the appropriate resource for resolution.
6.1.5.4 Perform problem diagnosis.
6.1.5.5 Answer queries regarding the usage and performance of the system.
6.1.5.6 Access the system remotely for diagnosis and correction of problems.
6.1.5.7 Contact the City Power Representative at regular intervals to provide status and/or resolution of problems.

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

City Power shall provide 1st line support which entails the following:
6.2.1 Response to End-user queries regarding the usage or performance of the system.
6.2.2 Resolve system problems with support from the Service Provider where necessary.
6.2.3 Swap defective Hardware components using spare parts.
6.2.4 Hand over complex system problems to the Service Provider through the Support Desk.
6.2.5 File a support request with the Support Desk for software and hardware support.
6.2.6 Inform and update the service provider of all information related to the encountered software or hardware problem.

6.3 ON-SITE SUPPORT

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

6.4 SYSTEM MAINTENANCE

6.4.1 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:
6.4.2 General routine checks of the system status.
6.4.3 Resolving system alarms.
6.4.4 Routine tests of the equipment's performance against the relevant equipment specifications.

6.5 SOFTWARE UPGRADE

6.5.1 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.
6.5.2 Upgrades shall be made available either on-premises or via a VPN connection.

6.6 INCIDENT MANAGEMENT

PRIORITY AND RESPONSE TIMES

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

7. 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 copies.

8. 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.

9. 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.

10. 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 Technical requirements changes and general editing