ICT SERVICE LEVEL AGREEMENT MANAGEMENT POLICY (EXTERNAL SERVICE PROVIDERS/VENDORS)

TABLE OF CONTENTS

Glossary of Abbreviations

Abbreviation	Definition
COBIT	Control Objectives for Information and Related Technology
ICT	Information and Communication Technology
ISM	Information Security Manager
ISO	International Organization for Standardisation

Glossary of Terminologies

Terminology	Definition
Clauses	Contract terms and conditions.
Contract meetings	A scheduled meeting with a service provider/vendor with supporting evidence.
Cost structure	The methodology to calculate a service fee. It may include, but are not limited to, a fixed fee component, fee per deliverable, fee per usage of a product, etc.
Deliverables	The outcomes expected from a service provider. It may include, but are not limited to, documents, knowledge transfer, installed software, a service, etc.
Escalate	To formally inform another party in writing or through electronic communications asking for a course of action.
Intellectual property rights	Any copyrighted materials, patents, trademarks, industrial designs and geographical indications and names of origin registered by a third party. Also includes commercial secrets governed under a confidentiality agreement.
Performance reviews	Comparing expected and agreed performance against actual performance based on measurable outcomes.
Sub-contractors	A primary contractor entering into agreements with other entities to deliver the service of the primary contractor.

1. INTRODUCTION

The delivery of ICT services to the Municipality require specialist skills and varying capacity demands. The use of external service providers/vendors to provide ICT services can be a cost effective and reliable way of acquiring these skills at a reasonable cost and in the required timeframes. As a result, information security risks also extend across the supply chain and therefore service providers/vendors of ICT related services must be managed to ensure that these risks are controlled and mitigated where possible. ICT remains accountable for ICT services under the control of service providers/vendors. It is for this reason that the management of service providers/vendors is an important Municipal task to ensure that service providers/vendors deliver the agreed services within the agreed timeframes and cost.

2. LEGISLATIVE FRAMEWORK

The policy was developed with the legislative environment in mind, as well as to leverage internationally recognised ICT standards.

The following legislation, among others, were considered in the drafting of this policy:

- Constitution of the Republic of South Africa Act, Act No. 108 of 1996.
- Copyright Act, Act No. 98 of 1978.
- Electronic Communications and Transactions Act, Act No. 25 of 2002.
- Minimum Information Security Standards, as approved by Cabinet in 1996.
- Municipal Finance Management Act, Act No. 56 of 2003.
- Municipal Structures Act, Act No. 117 of 1998.
- Municipal Systems Act, Act No. 32, of 2000.
- National Archives and Record Service of South Africa Act, Act No. 43 of 1996.
- Promotion of Access to Information Act, Act No. 2 of 2000.
- Protection of Personal Information Act, Act No. 4 of 2013.
- Regulation of Interception of Communications Act, Act No. 70 of 2002.
- Treasury Regulations for departments, trading entities, constitutional institutions and public entities, Regulation 17 of 2005.

The following internationally recognised ICT standards were leveraged in the development of this policy:

- Western Cape Municipal Information and Communication Technology Governance Policy Framework, 2014.
- Control Objectives for Information Technology (COBIT) 5, 2012.

- ISO 27002:2013 Information technology — Security techniques — Code of practice for information security controls.
- King Code of Governance Principles, 2009.

3. OBJECTIVE OF THE POLICY

The objective of the policy is to ensure that ICT-related resource needs are met in an efficient and structured manner.

4. AIMS OF THE POLICY

The aim of this policy is to provide a set of principles, practices and functions for ICT service provider/vendor/vendor management that are aligned to national and international best practice frameworks. It is a requirement of the Municipal ICT Governance Policy to implement service provider/vendor management as an integral part of corporate governance within the Municipality.

5. SCOPE

This policy recognizes that municipalities are diverse in nature, and therefore adopts the approach of establishing and clarifying principles and practices to support and sustain the effective control of service level agreement management. The policy covers the supply of ICT hardware, software, services and personnel.

This policy is regarded as crucial to the operation and security of ICT systems of the Municipality. Municipalities must develop their own Service Level Agreement Management controls and procedures by adopting the principles and practices put forward in this policy.

The policy covers the following elements of service level agreement management of external service providers/vendors:

- Agreement with service providers/vendors/vendors;
- Service management; and
- Change control.

6. BREACH OF POLICY

Any failure to comply with the rules and standards set out herein will be regarded as misconduct and/or breach of contract. All misconduct and/or breach of contract will be assessed by the Municipality and evaluated on its level of severity. Appropriate disciplinary action or punitive recourse will be instituted against any user who contravenes this policy. Actions include, but are not limited to:

- Revocation of access to Municipal systems and ICT services;
- Disciplinary action in accordance with the Municipal policy; or

- Civil or criminal penalties e.g. violations of the Copyright Act, 1978 (Act No. 98 of 1978).
- Recourse against the service provider in terms of the contract terms.

7. ADMINISTRATION OF POLICY

The ICT Manager or service provider/vendor is responsible for maintaining the policy. The policy must be reviewed by the ICT Steering Committee on an annual basis and any changes approved by the Council.

8. AGREEMENTS WITH SERVICE PROVIDERS/VENDORS

8.1 Over and above the default government terms and conditions, the following terms and conditions must be defined in all ICT service provider/vendor contracts:

(a) A description of the ICT services and how they will be delivered;

(b) The monthly fees and deliverables attached to the fees;

(c) The cost structure and payment schedule;

(d) The period of the contract, renewal and termination clauses;

(e) Availability, reliability and capacity of person/s responsible for delivering the service;

(f) Confidentiality and non-disclosure;

(g) In the case of software development:

- Who owns the program as well as the ideas and processes that makes it a valuable piece of software within the Municipal environment;
- Who is responsible for testing and ensuring that users are completely satisfied, as well as who is responsible for ensuring that users are able to use the software successfully;
- Who is responsible for, and how, the software will be maintained in the future;

(h) Which data the service provider/vendor may have access to, who owns the data, and how the data must be protected in line with the ICT Security Controls Policy;

(i) The responsibilities of both parties for ICT disaster recovery;

(j) Municipality's involvement in service provider/vendor processes, as well as the right to send its own audit team;

(k) Service Provider/Vendor service reporting;

(l) How the service provider/vendor will ensure that the resources/skills are available for the duration of the agreement;

(m) Skills transfer to the Municipality;

(n) Monitoring of critical systems in real-time and providing appropriate alerts to the ICT Manager.

(o) The security requirements of the person(s) delivering the ICT service in line with the ICT Security Controls Policy as well as the ICT Operating System Security Controls Policy;

(p) Should the service provider/vendor store or process personal information on behalf of the Municipality, the contract must state that the information must be protected in line with the ICT Security Controls Policy.

(q) Restrictions on the use of sub-contractors;

(r) In the event of a security breach affecting personal information, the service provider/vendor must notify the Municipality immediately;

(s) Penalties or discounts for non-performance against service levels;

(t) The process to terminate the agreement, without disrupting the ICT service to the Municipality; and

(u) Monthly status meeting.

8.2 The ICT Manager must ensure that service providers/vendors produce reports that include, but not limited to, the following information:

- Service level performance statistics, with failures and consequences;
- Major events;
- Incidents logged and resolution;
- Capacity usage and growth trends;
- Change requests and status; and
- Details of charges and invoices.

8.3 The agreement with the service provider/vendor must indicate the response time from the service provider/vendor based on the level of impact. The table below contains an example:

Impact	Description	Service level
Priority 1	The whole Municipality affected Extensive financial impact	2 hours

Impact	Description	Service level
Priority 2	More than half of Municipality affected Single department affected Significant financial impact	4 hours
Priority 3	Single user affected by an incident Limited financial impact	24 hours
Priority 4	Enhancement or new capability Service request from a user	To agreed timelines

Table 1 : Example service level determined by impact

8.4 All ICT contracts must be stored centrally in the Municipal archive. Ideally contracts must also be stored in electronic form in a contract management system where they are easily accessible to those managing the service.

9. SERVICE MANAGEMENT

9.1 The ICT Steering Committee must nominate the ICT Manager as the service manager for each ICT contract. The ICT Steering Committee may nominate any other Municipal employee to manage the service of ICT-related contracts if the contract is outside of the ICT Manager's scope of responsibility e.g. a financial or human resources system.

9.2 The ICT Manager must ensure that the services received from service providers/vendors are dependent on contact meetings and performance reviews. The amount of time and effort spent managing service providers/vendors must be equal to their importance to the Municipality. The following table is a broad guideline of the categories of service providers/vendors and the level of service management required by this policy:

Categories of service providers/vendors	Description	Example
Strategic	This is a significant agreement that involves a lot of participation by the ICT Manager. This agreement is often long term and involves sharing of Municipal data. This agreement would require monthly contact and service reviews. The contract and SLAs must be reviewed twice a year.	ICT outsourcing Supply of network services

Categories of service providers/vendors	Description	Example
Tactical	This is a significant agreement that would normally be managed by the ICT Manager. This agreement would require monthly contact and service reviews. The contract and SLAs must be reviewed twice a year.	Hardware maintenance and repair End-user support services
Operational	This type of agreement is for the supply of operational products and services and would normally be managed by the ICT Manager. This agreement would require quarterly contact and service reviews. The contract and SLAs must be reviewed once a year.	Internet hosting service provider
Commodity	This type of agreement is for the supply of low-value and readily available products and services. The agreement is normally managed by ICT staff and the normal supply chain management controls would suffice.	Personal computers Printer consumables

Table 2 : Categories of service providers

9.3 The ICT Manager is responsible to review the ability of the service provider/vendor to continue delivering the service in the near future as well as dealing with contract disputes and renewals.

9.4 The ICT Manager must inform the ICT Steering Committee on a monthly basis of known service delivery failures on Strategic and Tactical contracts. The ICT Manager must escalate continued service delivery failures to the ICT Steering Committee at their next scheduled meeting.

9.5 The ICT Manager must deal with known service delivery failures on Operational contracts on a quarterly basis.

9.6 The ICT Manager must communicate unsatisfactory performance by service providers/vendors in writing compelling the service provider/vendor to perform according to the contract.

9.7 If any dispute arises, the process is to first attempt to reach an amicable agreement. Secondly, the parties can go for mediation. Thirdly, the matter may be settled in a South African court of law.

9.8 Termination of the contract must be considered, as stipulated in the general conditions of contract, for reasons such as delayed deliveries, failing to perform any other contractual obligation or if the service provider/vendor has engaged in corrupt and fraudulent practises and insolvency.

9.9 Contract termination may be effected if allowed for in the contractual conditions and if both parties agree to the termination in writing.

9.10 The ICT Steering Committee may enforce discounts or penalties from service providers/vendors if the contract conditions provide for this.

9.11 The ICT Manager is responsible to ensure that ICT service provider/ vendor environments are audited.

10. CHANGE CONTROL

10.1 The ICT Manager must ensure that agreements are kept up to date with changes to the ICT service.

10.2 The ICT Manager must ensure that the introduction of a new service provider/vendor and a major change to an existing agreement must be controlled through the change control process defined in the ICT Security Controls Policy.

10.3 The ICT Manager must ensure that service providers/vendors follow the change control process defined in the ICT Security Controls Policy for changes to the ICT environment.

11. ANNEXURE A: IMPLEMENTATION ROADMAP

No	Action	Month 1	Month 2	Month 3	Month 4	Month 5	Month 6	Month 7 - 9
1	Identify all ICT contracts							
2	Allocate ICT Contract Managers to all ICT contracts							
3	Identify ICT service providers/vendors that process personal information							
4	Review all ICT contracts against prescribed minimum terms							
5	Commence management of ICT contracts (Continuous)							

12. ANNEXURE B: REFERENCES

BS ISO/IEC 27002: Information technology - Security techniques - Code of practice for information security controls. (2013). Geneva: BSI Standards Limited.

Control Objectives for Information Technology (COBIT) 5. (2012). Illinois: ISACA.

King Code of Governance for South Africa. (2009). Institute of Directors in Southern Africa.

Local Government: Municipal Finance Management Act, No. 53. (2003). Republic Of South Africa.

Local Government: Municipal Structures Act 117. (1998). Republic of South Africa.

Local Government: Municipal Systems Act 32. (2000). Republic of South Africa.

Protection of Personal Information Act, No. 4. (2009). Republic of South Africa.