

# IT Charter

---

**Version 3.0**  
**12<sup>th</sup> February 2020**

# Document History

---

Created by:	Eddy Lareine
Approved by:	Areff Salauroo

Release date	Version	Change Details	Reviewed by
22.10.19	1.0	Submitted for review	Legal Advisor
12.11.19	2.0	Apply changes submitted by legal advisor	Eddy Lareine
12.02.20	3.0	Submitted for review	Areff Salauroo

## Table of Contents

<b>1.0</b>	<b><i>What is the IT Governance Policy?</i></b>	<b>4</b>
1.2	Applicability	4
1.3	Responsibility	4
1.4	Ownership	5
1.5	Compliance	5
1.6	Communication	5
1.7	Updates to this policy	5
<b>2.0</b>	<b><i>Maturity</i></b>	<b>6</b>
<b>3.0</b>	<b><i>IT Strategy at La Sentinelle Group Level</i></b>	<b>8</b>
<b>4.0</b>	<b><i>Policy Statements</i></b>	<b>9</b>
4.1	Overview	9
4.2	Define IT Strategic Plan	10
4.3	Determine Technological Direction	11

# IT CHARTER

## 1.0 What is the IT Governance Policy?

This policy is a document that defines the mandatory or recommended principles and standards for consistent IT Management and IT Governance (including information security) in general. The purpose of this policy is to drive consistency with respect to the following high-level objectives:

- IT is used as an enabler to achieve business strategy and is leveraged to the maximum to improve sustainability, efficiency, reliability and automation within business processes;
- IT governance structures are clearly defined and followed, including the responsibilities at the Group and Operations level, and;
- Investments in IT related capital expenditures and operating expenditures are made diligently to ensure that value is sustained and to avoid quick obsolescence.
- IT infrastructure shall be designed in such a way as to ensure business continuity in all circumstances.
- IT Risk Assessments will be performed and performance measures will be implemented.

While this policy establishes the principles in general, the relevant operations and subsidiaries have the flexibility in defining the detailed processes and approach for implementation and adherence.

## 1.2 Applicability

This policy applies to all La Sentinelle Ltd operations and subsidiaries, (hereafter referred to as 'entities') which are custodians of Group information, information systems or information processing facilities.

Joint venture and associates shall be encouraged to adhere to the policies.

## 1.3 Responsibility

This policy is addressed to all personnel within the Group who own, develop, operate or use information systems or information processing facilities.

## 1.4 Ownership

This policy is sponsored by the Board of Directors and the Group Chief Executive Officer of the La Sentinelle Ltd Group. The Group Head of IT is responsible for maintaining the document on behalf of the Board of Directors and the Group Chief Executive Officer. All requests for information or clarifications pertaining to this document should be directed to the Group Head of IT of La Sentinelle Ltd.

## 1.5 Compliance

Compliance with the policy is required at all times. To allow for flexibility, the policy defines two types of compliance activities which may be performed to prevent and detect non-adherence. These activities can take the form of the following components:

- **Self-assessments:** Management of each operation, subsidiary, associate or joint venture performs self-assessments or health-checks at least every year or on an as required (ad-hoc) basis to determine the extent of adherence to the policy.
- **Independent verifications:** The Internal Audit function performs audits to detect instances of non-compliance and exceptions.

An IT Steering Committee will assess the risks and recommend follow-up actions. In case of unresolved and persisting deviations, the Steering committee will report to the CEO for further action. For internal audits, exceptions and deviations will be reported to the Audit Committee. It should be noted that some policy statements may be derived from regulatory requirements and thus directly impact compliance to law.

Taking into account that implementation of this initial version of the policy may take some time, a burn-in of six months (from the date of this current policy version) has been established during which it is expected that all concerned parties initiate procedures for implementation of relevant policy statements.

## 1.6 Communication

The Head of IT of La Sentinelle Ltd is responsible for communicating the policy to relevant stakeholders, including new versions following internal revisions to the content.

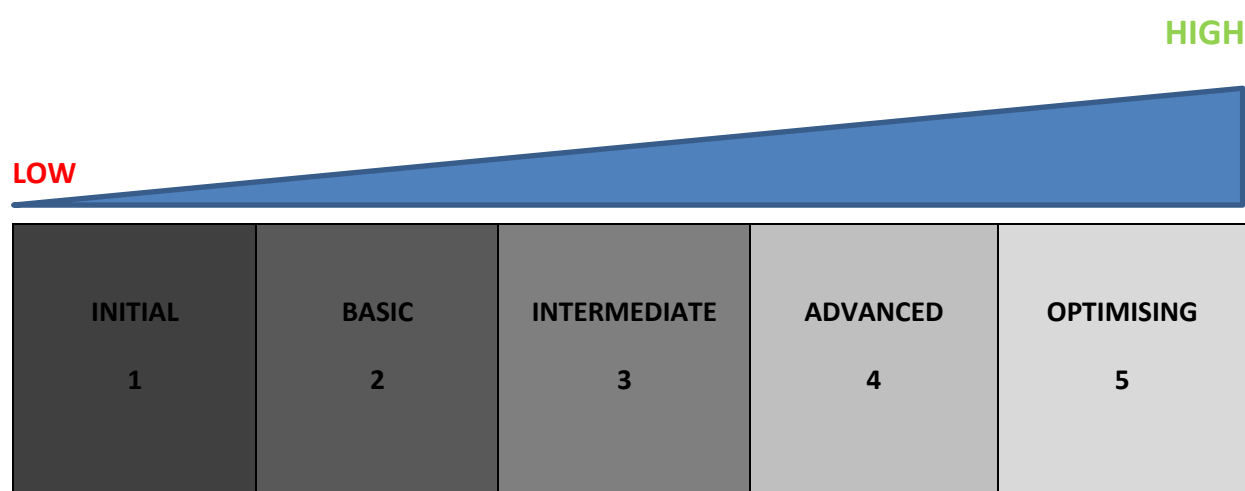
## 1.7 Updates to this policy

The contents of this policy will be reviewed annually by the ICT (or any other instances to be defined) and updated accordingly to reflect any changes in the IT environment.

## 2.0 Maturity

La Sentinelle Ltd recognises that its operations and subsidiaries have varying levels of maturity in terms of IT processes and supporting IT environments. To provide a pragmatic framework for implementation and adherence to the policy, different maturity levels have been defined to ensure that implementation remains realistic and practical.

IT maturity can be assessed using the Innovation Value Institute (IVI) IT Capability Maturity Framework™ (CMF) which is derived from the generic Capability Maturity Model. The IT CMF provides a blueprint for incremental improvement across four macro-capabilities (namely Managing IT as a Business, Managing the IT Budget, Managing IT for Business Value and Managing the IT Capability) measured on five maturity levels as illustrated below:



Illustrative qualitative criteria for each maturity level are provided below:

Maturity Level	Illustrative Criteria
<ul style="list-style-type: none"><li>Initial</li></ul>	<ul style="list-style-type: none"><li>Ad-hoc and undocumented processes for management of IT</li><li>Inadequate resources to support information systems and IT infrastructure</li><li>Frequent occurrence of IT related incidents</li><li>No interaction with Business Holders</li><li>No formalized project management approach</li><li>IT projects and information systems are owned by IT function</li></ul>
<ul style="list-style-type: none"><li>Basic</li></ul>	<ul style="list-style-type: none"><li>Basic IT services are delivered</li><li>Some IT and business interactions formalised</li></ul>
<ul style="list-style-type: none"><li>Intermediate</li></ul>	<ul style="list-style-type: none"><li>IT and business interaction formalised for all critical processes</li><li>Buy-in from business during IT projects and initiatives</li><li>Transparent IT investment decision</li></ul>
<ul style="list-style-type: none"><li>Advanced</li></ul>	<ul style="list-style-type: none"><li>Benefits from IT investments are monitored, quantified and communicated</li><li>Practices and outcomes well above industry average</li></ul>
<ul style="list-style-type: none"><li>Optimising</li></ul>	<ul style="list-style-type: none"><li>Value-centric IT management</li><li>State-of-the-art practices and outcomes</li><li>Continuous improvement within IT processes</li></ul>

For the purpose of implementation of this policy, each operation, department and subsidiary, should be assessed against the qualitative criteria above and categorised in one of the above mentioned five maturity levels. As per standard Statement of Applicability rule, justification criteria for compliance or non-compliance will be required.

### 3.0 IT Strategy at La Sentinelle Group Level

Irrespective of the maturity level of any entity within La Sentinelle Group, business strategy must dictate and drive any investment in IT. The ability to translate strategic business objectives into pragmatic technologically strategic plans provides competitive advantage in leveraging IT to deliver enhancements in customer experiences, gains in efficiency, reliability and integrity of processes (through automation) and meaningful management information that prompts appropriate decision making. This approach allows IT to be a business enabler and the IT function to be a trusted advisor providing both innovative technologies and value-added solutions.

Inherently derived from the vision and mission statements of the company, the high-level strategic objectives of La Sentinelle Ltd, can be summarised along the following themes:

- Deliver a higher return on investment.
- Advance position and reputation with stakeholders (such as customers, employees, the authorities and regulators, suppliers, business partners, the community)
- Grow the capabilities of the Group sustainably and continue to capitalise on the long-term growth opportunities available, both in existing businesses and future ventures
- Implement a leaner operating environment and a culture based on a continuous pursuit of excellence and talent management

The following are the IT imperatives which are derived from the strategic objectives through a top-down approach:

- Established IT governance structures at La Sentinelle Group and subsidiary levels.
- Controlled cost on IT expenditures by leveraging centralized procurement and continually improving the process.
- Technology capabilities built for flexibility to handle scalable requirements.
- Use and application of standardised and value-for-money technologies.
- Use of autonomous IT platforms to allow for easy plug-in or separation in the event of acquisitions or divestitures respectively.
- Uniform access to information with easy integration of information through a common platform.
- IT due diligence during transactions to obtain a clear view of the value of IT.
- Interdepartmental synergies and knowledge sharing, whenever applicable.



## 4.0 Policy Statements

### 4.1 Overview

This policy is structured around specific domains relevant to the context of La Sentinelle Group, all its operations, subsidiaries, and with the IT imperatives as detailed in section 3 above.

The domain areas have been aligned to COBIT (Control Objectives for Information and Related Technology) wherever relevant and customised to the needs of La Sentinelle Group, all its operations, subsidiaries, associates and joint ventures, as applicable. For each domain, the high-level objectives and applicable control statements are provided. Further, for each control statement, the following has been added to determine their priority and applicability to each maturity level:

- The following convention has been used to indicate the applicability of each control statement:

<b>Must (M)</b>	Indicates mandatory compliance. Non-compliance requires an approved exception.
<b>Should (S)</b>	Indicates a recommendation, something that should be implemented wherever possible. Non-compliance requires an approved request.
<b>“-“ (-)</b>	Indicates the control statement is not applicable. Non-compliance requires an approved request as stated in each Policy document.

- **Responsibility:** Whether implementation of control should be performed by the Group, managed locally by each entity (i.e. subsidiaries,) or both.
- **Importance:** From high, moderate to low, the importance denotes the significance of each control and assists in defining a prioritised plan for implementation and compliance reviews.

## 4.2 Define IT Strategic Plan

### Objectives

In the context of La Sentinelle Group, IT strategic planning is required to manage and direct all IT resources in line with the Group or entity level business strategies and priorities, with a focus on standardisation as far as possible within the Group and cost optimisation. Optimal value should be derived and realised from IT investments.

### Control Statements

(Maturity Level – 1=Initial; 2=Basic; 3=Intermediate; 4=Advanced; 5=Optimising)

DESCRIPTION	RESPONSIBILITY	IMPORTANCE	MATURITY LEVEL				
			1	2	3	4	5
1.1 Establish processes of two-way education and involvement in strategic planning to achieve business and IT alignment and integration.	Group & Entity	High	-	M	M	M	M
1.2 Continually assess the current capabilities and performance of IT functions within the Group and identify future requirements based on business objectives and priorities.	Group & Entity	High	-	S	M	M	M
1.3 Create strategic plan(s) that defines, in cooperation with relevant stakeholders, how IT goals will contribute to the Group's strategic objectives.	Group & Entity	High	-	-	S	M	M
1.4 Assess the value of IT during due diligences as part of acquisition and divestiture transactions, taking into consideration the following key components where relevant: <ul style="list-style-type: none"> <li>Enterprise Applications</li> <li>Specialised Applications (Industry Specific)</li> <li>Office Productivity Applications</li> <li>Hardware (mainframes, servers, storage, end-user devices)</li> <li>Network and telecommunication (data, voice and mobile)</li> <li>Infrastructure software (operating systems, middleware, security, compliance, database management systems)</li> <li>IT organisation (size, structure, capabilities, location outsourcing, skill, experience)</li> <li>Suppliers/vendors (vendor viability, licenses and conditions, contract termination fees)</li> <li>IT culture (governance, mission, innovation, adaptability, communication)</li> <li>IT operations (IT operating and capital budgets, security &amp; risk management, disaster recovery, business continuity, current and planned projects, data centre/server room)</li> </ul>	Group & Entity	High	S	M	M	M	M

### 4.3 Determine Technological Direction

#### Objectives

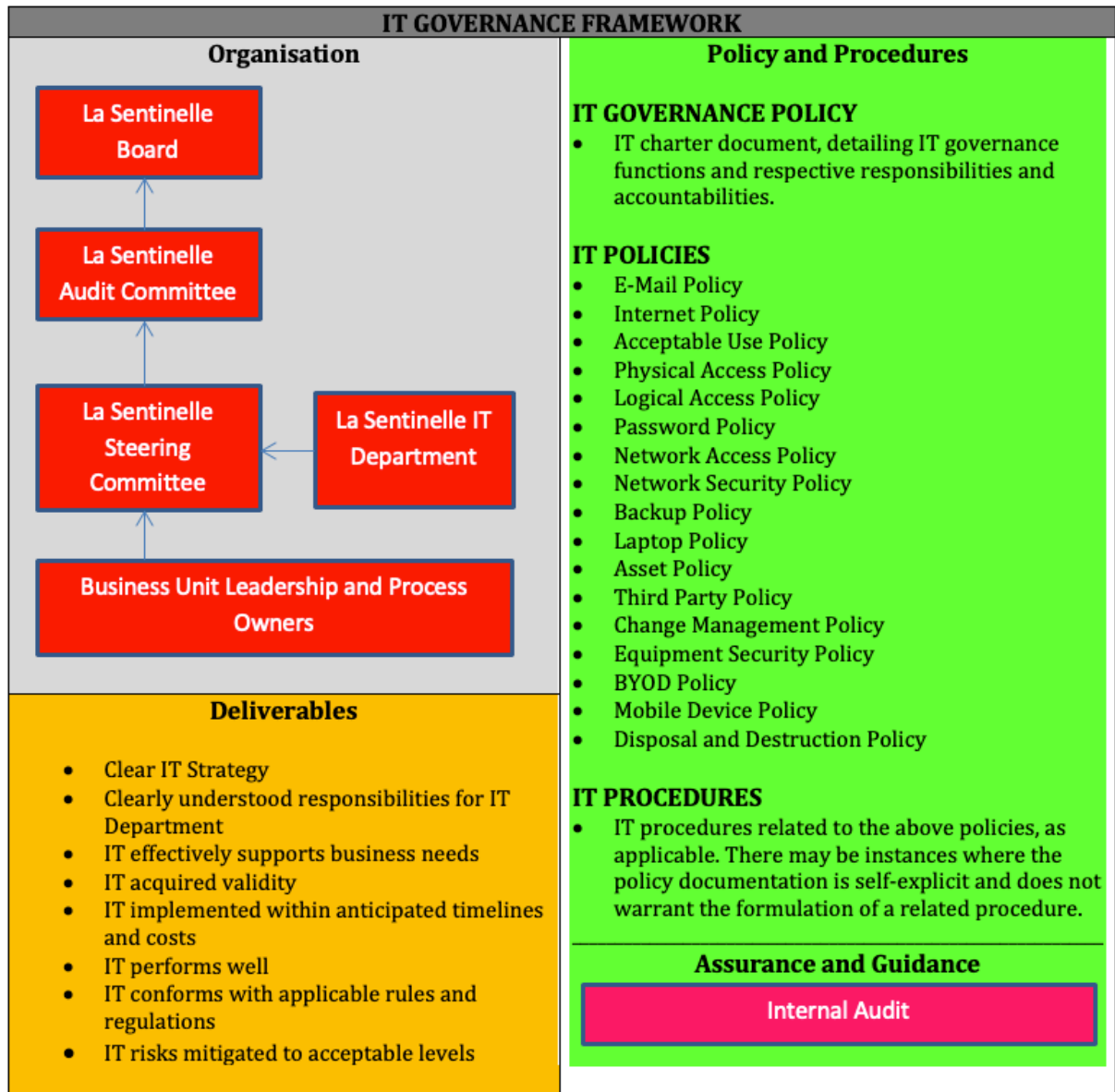
Given the complexity and fast-changing nature of IT, architectures are important for defining the technological direction intended to support evolution and change as per requirements. There are generally three overall end goals namely business and IT alignment (fit for purpose), risk management (reduced likelihood of failures) and resource management (cost effectiveness and value for money).

#### Control Statements

(Maturity Level – 1=Initial; 2=Basic; 3=Intermediate; 4=Advanced; 5=Optimising)

DESCRIPTION	RESPONSIBILITY	IMPORTANCE	MATURITY LEVEL				
			1	2	3	4	5
1.5 Analyse existing and emerging technologies, and plan which technological direction is appropriate to realise the IT strategy, support business processes and introduce innovative techniques.	Group & Entity	Moderate	-	-	M	M	M
1.6 Establish standards on the selection of technology and measure compliance with these standards, to provide consistent, effective, interoperable (within the Group) and secure technological solutions Group wide. Indicative components which should be covered by standards are:  <ul style="list-style-type: none"> <li>Hardware (desktop, laptop, server)</li> <li>Infrastructure software (operating system, database management systems, firewalls, routers)</li> <li>Business applications (e.g. Enterprise Resource Planning software)</li> </ul>	Group & Entity	High	S	M	M	M	M

## APPENDIX A - IT GOVERNANCE FRAMEWORK



### Legend



**Organisation / Policy & Procedures / Deliverables / Assurance and Guidance**