Third Party Policy

Version 3.0

12th February 2020

Rue des Oursins, 21731, Baie du Tombeau I T : +(230) 206 8200 I F : +(230) 247 1010 I E : corporate@lasentinelle.mu

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

THIRD PARTY POLICY

1.0 Objective

The objective of this policy is to:

i. maintain the security of La Sentinelle Ltd's information and information processing facilities that are accessed, processed, communicated to, or managed by external parties;

ii. To implement and ensure an appropriate level of information security and service delivery in line with Third Party Service Delivery Agreements.

iii. To maintain an agreed level of information security and service delivery in-line with supplier agreements.

2.0 Scope

All employees including temporary employees, suppliers, contractors, consultants and all personnel affiliated with Third Parties that use or provide services to La Sentinelle Ltd must adhere to this policy.

Definition of Third Parties – *include but are not limited to suppliers, auditors, maintenance staff, trainees, hardware & software contractors, consultants, customers, visitors, security personnel, emergency personnel, etc..*

3.0 References

3.1 References to ISO 27001:2013

- **Information Security Policy in Supplier Relationships – A.15.1.1**

  Information security requirements for mitigating the risks associated with supplier's access to the organisation's assets shall be agreed with the suppliers and documented.

- **Addressing Security Policy for Supplier Relationships – A.15.1.2**

  All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate or provide IT infrastructure components for the organisation's information.

- **Information and Communication Technology Supply Chain – A.15.1.3**

  Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain.

- **Monitoring and Review of Supplier Services – A.15.2.1**

  Organisations shall regularly monitor, review and audit supplier delivery.

- **Managing Changes to Supplier Services – A.15.2.1**

  Changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls shall be managed, taking account of the criticality of the business information and processes involved and the re-assessment of the risks.

- **Confidentiality or Non-Disclosure Agreements – A.13.2.4**

  Requirements for confidentiality or non-disclosure agreements reflecting the organisation's needs for the protection of information shall be identified, regularly reviewed and documented.

3.2 References to Forms & Agreements

- Computer Services Request Form
- Third Party Agreement
- Third Party Computer Connection Request Form
- Confidentiality and Non-Disclosure Agreements
- Business Continuity Plan

4.0 Policy Description

4.1 Identification of Risks Related to External Parties

The risks to La Sentinelle Ltd's information and information processing facilities from business processes involving external parties are assessed when the external party submits the **Computer Services Request Form**. The identification of risks related to external party access takes into account the following issues:

a) The information processing facilities an external party is required to access;
b) The type of access the external party will have to the information and information processing facilities such as physical access, logical access, network access and whether the access is taking place on-site or off-site remote access;
c) The value and sensitivity of the information involved, and its criticality for business operations;
d) The controls necessary to protect information that is not intended to be accessible by external parties;
e) The external party personnel involved in handling La Sentinelle Ltd's information;
f) How the external parties authorised to have access can be identified, the authorisation verified, and how often this needs to be reconfirmed;
g) The different means and controls employed by the external party when storing, processing, communicating, sharing and exchanging information;
h) The impact of access not being available to the external party when required, and the external party entering or receiving inaccurate or misleading information;
i) Practices and procedures to deal with information security incidents;
j) Legal and regulatory requirements and other contractual obligations relevant to the external party;
k) How the interests of any other stakeholders may be affected by the arrangements.

Access by external parties to La Sentinelle Ltd's information is not provided until the appropriate controls have been ensured and where feasible, a contract has been signed, defining the terms and conditions for the connection or access and the working environment.

Appendix AA below shows risks associated with external parties and measures taken to eliminate or mitigate these risks accordingly.

4.2 Addressing Security When Dealing with Customers and Suppliers

Before giving customers and/or suppliers access to La Sentinelle Ltd's information or assets, all identified security requirements are addressed. The following terms are considered:

a) Asset protection;
b) Description of the product or service to be provided;
c) The different reasons, requirements, and benefits for customer and/or supplier access;
d) Access control policy;
e) Arrangements for reporting, notification, and investigation of information inaccuracies, security incidents and security breaches;
f) A description of each service to be made available;
g) The target level of service and unacceptable levels of service;
h) The right to monitor, and revoke, any activity related to La Sentinelle Ltd's assets;
i) The respective liabilities of La Sentinelle Ltd and the customer and/or supplier;
j) Responsibilities with respect to legal requirements;
k) Intellectual property rights and protection of any collaborative work.

4.3 Addressing Security in Third Party Agreements

Agreements with Third Parties involving accessing, processing, communicating or managing La Sentinelle Ltd's information or information processing facilities, or adding products or services to information processing facilities cover all relevant security requirements. The following terms are considered for inclusion in the Third Party Agreement in order to satisfy the identified security requirements:

a) Controls to ensure asset protection;
b) User and Administrator training in methods, procedures and security;
c) Ensuring user awareness for information security responsibilities and issues;
d) Provision for the transfer of personnel, where appropriate;
e) Responsibilities regarding hardware and software installation and maintenance;
f) A clear reporting structure and agreed reporting formats;
g) A clear and specified process for Change Management;
h) Access control policy – Logical and Physical;
i) Arrangements for reporting, notification, and investigation of information security incidents and breaches;
j) A description of the product or service to be provided, and a description of the information to be made available along with its security classification;
k) The target level of service and unacceptable levels of service;
l) The definition of verifiable performance criteria, their monitoring and reporting;
m) The right to monitor and revoke any activity related to La Sentinelle Ltd's assets;
n) The right to audit responsibilities defined in the agreement;
o) The establishment of an escalation process for problem resolution;
p) Service continuity requirements;
q) The respective liabilities of the parties to the agreement;
r) Responsibilities with respect to legal matters;
s) Intellectual property rights and protection of any collaborative work;
t) Involvement of the Third Party with Subcontractors;
u) Conditions for renegotiation/termination of agreements.

Rue des Oursins, 21731, Baie du Tombeau I T : +(230) 206 8200 I F : +(230) 247 1010 I E : corporate@lasentinelle.mu

4.4 Service Delivery

La Sentinelle Ltd ensures that the security controls, service definitions and delivery levels included in **Third Party Agreements** are implemented, operated and maintained by the Third Party in line with the agreement. Service delivery includes the agreed security arrangements, service definitions and aspects of service management.

It is also ensured that the Third Party maintains sufficient services capability together with workable plans designed to ensure that agreed service continuity levels are maintained following major service failures or disaster in line with La Sentinelle Ltd **Business Continuity Plan.**

4.5 Monitoring and Review of Third Party Services

Monitoring and review of Third-Party services ensures that the information security terms and conditions of the agreements are being adhered to, and that information security incidents and problems are managed properly. This involves a service management relationship and process between La Sentinelle Ltd and the Third Party to:

a) Monitor service performance levels to check adherence to the agreements, identify shortfalls and agreeing how they should be rectified;
b) Review service reports produced by the Third Party and arrange regular progress meetings as required by the agreements;
c) Provide information about information security incidents and review of this information by the Third Party and La Sentinelle Ltd to take appropriate corrective actions;
d) Review Third Party audit trails and records of security events, operational problems, failures, tracing of faults and disruptions related to the service delivered;
e) Resolve, manage and mitigate any identified problems and/or risks.

5.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment as per La Sentinelle Ltd HR Policy.

6.0 User Agreement

I hereby acknowledge that I have read and I understand the Third Party Policy of La Sentinelle Ltd. I agree to abide by this policy and ensure that persons working under my supervision shall abide by these policies. I understand that if I violate such rules, I may face disciplinary action.

Name : _____

Signature : _____

Date : _____

7.0 Appendix AA – Common controls applicable to Third Parties

External party	Potential risks	Measures taken	Policy/Control
Auditors (Internal Auditors, External Auditors e.g. Financial, Quality, …..)	Access to all documents and Release of confidential information	Sign Non-Disclosure Agreement Sign Confidentiality Agreement	Non-Disclosure Agreement Confidentiality Agreement
Maintenance Staff/Personnel (	Accidental access to confidential information (reports, on screen, fax, print out ...) Access and usage of IT equipment	Always accompanied by staff Visits must be scheduled Clear Desk Policy - Confidential documents to be secured and not left unattended Access to restricted areas in line with Physical Access Policy Automatic screen locking/ password Compliance to requirements of Third Party Policy	Non-Disclosure Agreement Physical Access Policy Third Party Agreement
Trainees	Accidental access to confidential information (reports, on screen, fax, print out ...) Release of confidential information	Access given only on a need-to-know basis Controlled Access to restricted zones – Physical Access Logical access on a need to have basis	Physical Access Policy Logical Access Policy Non-Disclosure Agreement Confidentiality Agreement Third Party Agreement

	Intellectual property act	Monitoring Confidential agreement and/or confidentiality clause included in all contractual agreements e.g. Trainee contract Protection of company's Intellectual Property	
Contractors – Hardware , Software Suppliers	Access to confidential and sensitive information Access to infrastructures and networks -Remote -On site Access to Systems and sensitive data	Access to information strictly restricted on a "Need to have/need to know" basis; Always accompanied by staff; Visits must be scheduled; Clear desk policy/ Confidential documents to be secured and not left unattended Automatic screen locking/ password Sign Non-Disclosure Agreement Confidentiality Agreement and/or confidentiality clause included in all contractual agreements	Physical Access Policy Logical Access Policy Non-Disclosure Agreement Confidentiality Agreement Third Party Agreement
Consultants	Access to confidential and sensitive information	Always accompanied by staff Visits must be scheduled	Physical Access Policy Logical Access Policy Non-Disclosure Agreement

	Access to infrastructures and networks -Remote -On site Access to Systems and sensitive data	Clean desk policy/ Confidential documents to be secured and not left unattended Automatic screen locking/ password Sign Non-Disclosure Agreement Controlled Access rights on a need to have basis	Confidentiality Agreement Third Party Agreement
Customer –Internal - External	Accidental access to confidential information (reports, on screen, fax, print out ….) Access to restricted areas (e.g. server room) Access and usage of IT resources Access to network	Always accompanied by staff Visits must be scheduled Clear desk policy/ under lock Automatic screen locking/ password Always accompanied by staff Controlled Access rights on a need to have basis	Physical Access Policy Logical Access Policy Non-Disclosure Agreement Confidentiality Agreement Third Party Agreement
Visitors	Accidental access to confidential information (reports, on screen, fax, print out ….) Access to restricted areas Access and usage of IT equipment	Always accompanied by staff Visits must be scheduled Clear desk policy Automatic screen locking/ password	Physical Access Policy