Asset 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

Table of Tables

ASSET POLICY

1.0 Objective

The objective of this policy is to identify organizational assets and define appropriate protection responsibilities by ensuring that

i. Every information asset has an owner and that the nature and value of each asset is fully understood;
ii. The boundaries of Acceptable Use are clearly defined for anyone who has access to the information asset.
iii. Each information asset receives an appropriate level of protection in accordance with its importance to the organization.

2.0 Scope

This policy applies to all employees of La Sentinelle Ltd.

3.0 References

3.1 References to ISO 27001:2013

- **Inventory of assets - A.8.1.1**

  Assets associated with information security and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.

- **Ownership of assets – A.8.1.2**

  Assets maintained in the inventory shall be owned.

- **Acceptable Use of Assets – A.8.1.3**

  Rules for the acceptable use of information and assets associated with information and information processing facilities shall be identified, documented and implemented.

- **Classification of Information – A.8.2.1**

  Information shall be classified in terms of its legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification.

- **Labelling of Information – A.8.2.2**

  An appropriate set of procedures for information labeling shall be developed and implemented in accordance with the information classification scheme adopted by the organisation.

- **Handling of Assets – A.8.2.3**

  Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organization.

3.2 References to Policies and Forms

- Disposal and Destruction Policy
- Acceptable Use Policy
- HR Policy
- Asset Inventory Form
- Asset Owner Form

4.0 Glossary of Terms

- **Asset –** anything that has value to La Sentinelle Ltd.
- **Owner** - an individual or entity that has approved management responsibility for controlling the production, development, maintenance, use and security of the assets. The term 'owner' does not mean that the person actually has property rights to the asset, but they are responsible and/or accountable for it.

5.0 Policy Description

5.1 Inventory of assets

La Sentinelle Ltd has identified the following categories of assets:

- **Hardware**: includes computers, servers, laptops, printers…
- **Software**: includes application systems, operating systems, development tools…
- **Paper**: includes HR Records, invoices, user manuals, files, publications…
- **Electronic data**: includes all databases on electronic media, all information on electronic media
- **Extension services:** includes Air conditioners, generators, UPS…
- **Telecommunications Equipment:** includes Routers, Switches, Firewall….
- **People:** includes employees, customers, cleaners…
- **Company Image**: Goodwill

All assets of the organisation are identified and listed in an ***Asset Inventory Form.*** Information available in ***Assets Inventory*** form is as follows:

- Asset Identification
- Asset Description
- Name & Brand (where applicable)
- Location
- Assigned Owner

5.2 Ownership of Assets

- Employees and/or Head of Departments are designated as Asset Owners and must abide to rules implemented by Management regarding the ownership and acceptable use of the assets. Each asset is assigned to nominated owners who are responsible and accountable for the appropriate protection of the asset.

- In case of assets whose use is widespread, e.g. software and telecommunications equipment, the respective Head of Department is treated as the asset owner. Routine tasks may be delegated, e.g. to a custodian looking at the asset on a daily basis, but the responsibility and accountability remains with the owner.

- The owner will have to acknowledge receipt of the asset and take responsibility for the asset.

- The assets assigned to an owner will be listed in the **'Asset Owner Form'** which will be updated as and when necessary. This form (kept in 3 copies) will need to be signed by the owner. The original will be in the Personal file of the Asset Owner with the HR Department, one copy will be submitted to the Asset Owner and one copy will be kept with the IT and/or Finance Department.

- Responsibilities of asset owners will include inter-alia:

  (a) Monitoring compliance with protection requirements affecting their assets;

  (b) Appropriate classification and protection of the information assets;

  (c) Authorizing access to information assets in accordance with the classification and business needs;

5.3 Classification of Information

- Information asset classification is critical to ensure that the organisation's information assets have a level of protection corresponding to the sensitivity and value of the information.

- Information is available either in physical (hard copy) or electronic records. Physical records (which include all forms of paper records and documents) contain information directly readable by anyone. Electronic records contain information that requires electronic device to read the information.

- All employees who create a new information asset (e.g a report, database, procedure, and proposal) must ensure that the information asset is classified in line with the Information Classification Guidelines below (Table 1.0).

Table 1.0 below shows ***Information Classification Guidelines***

Information Category	Description	Examples
SECRET	Class of information that is extremely sensitive and/or business critical and therefore needs to be protected as strongly as possible against unauthorized access.	• Organization's strategic plans • Board minutes • System security information (e.g. Passwords) • Credit card information • Legal documents
CONFIDENTIAL	Class of information that is sensitive and/or business critical and therefore needs to be protected to a reasonable extent. It is intended for limited distribution within the organization or to specially designated Third Parties, on a need-to-know ('default deny') basis.	• Budget Files • Financial Proposals • Financial Statements • Minutes of Meetings • Employee records • Business Plans
INTERNAL USE	Class of information that is intended for general use by the employees and, if necessary, by selected Third Parties such as clients, suppliers or contractors.	• Client files • Suppliers File • Fax • Mails • Memos • Quality/Security Manual
PUBLIC USE	Class of information that has been officially sanctioned by the organization for external publication to selected groups or the general public or is already in the public domain	• Press Releases • Newspapers • Magazines • Marketing Materials • Website • Newsletters

Table 1 - Information Classification Guidelines

- The classification of information can also change over time. Generally, as information becomes outdated it becomes less sensitive. In such case, the owner of the information will redefine the classification level of the information.

5.4 Labelling of Information & Handling of Assets

- The following procedures establish basic rules for handling, labelling, transmission, and storage of information in order to protect information from unauthorised disclosure or misuse.

5.4.1 Secret Information

When transferring secret information, the restrictions of the information owner must govern the transfer. The information user must enforce these restrictions, e.g. by only forwarding information to authorized recipients, and must adhere to all applicable policies that cover transfer issues.

At a minimum, the asserted identity of the user must be verified according to applicable policies.

- Access to secret information must be kept to a minimum and limited to authorized personnel only. Hardcopies of secret information must be securely stored if not in use and access to secret information must be duly logged and monitored.
- Information classified as secret must not be printed on printers that are openly accessible. Printers must be attended if secret information is being printed.
- Hardcopies of secret documents must not be duplicated using photo-copiers or other technical means. Secret information stored digitally must not be duplicated except as required for back up purposes by authorized asset owners.
- Secret information must never be sent over unencrypted communication channels. Secret documents in particular must never be sent over unencrypted fax-lines.
- It is the responsibility of the information user in possession of secret information to ensure that proper disposal occurs. When secret information is no longer required, the documents must be securely destroyed in a verifiable way **as per La Sentinelle's "Disposal and Destruction Policy".**
- All spoken communications involving secret information must be conducted in a way that minimizes the risk of disclosure to unauthorized parties.

5.4.2 Confidential Information

When transferring confidential information, the restrictions of the information owner must govern the transfer. The information user must enforce these restrictions, e.g. by only forwarding information to authorized recipients, and must adhere to all applicable policies that cover transfer issues. At a minimum, the user must verify the identity of the recipient in accordance with applicable policies.

- Access to confidential information must be kept to a minimum and limited to authorized personnel only. Hardcopies of confidential information must be securely stored if not in use.

- Information classified as confidential must not be printed on printers that are openly accessible. Printers and photo-copiers must be attended if confidential information is being printed or copied.

- It is the responsibility of the information user in possession of confidential information to ensure that proper disposal occurs. When confidential information is no longer required, the documents must be securely destroyed, **as per La Sentinelle's "Disposal and Destruction Policy".**

- All spoken communications, including telephone calls, involving confidential information must be conducted in a way that minimizes the risk of disclosure to unauthorized parties.

5.4.3 Internal Information/Office Use

- When transferring internal information, the restrictions of the information owner must govern the transfer. The information user must enforce these restrictions, e.g. by only forwarding information to authorized recipients.

5.4.4 Public Information

- Restrictions related to the handling of public information must be observed. The formal release of public information must be restricted to authorized individuals only.

5.5 Classification of Information & Impact on Organisation

Table 2.0 below shows the Classification of Information & Impact on Organisation

Classification	Definition	Impact	Labelling Standard
Secret information	Is the most confidential and sensitive information for La Sentinelle Ltd. Distribution of Secret information must be restricted **to a very small group of identified and authorized people**. A very small portion Of La Sentinelle Ltd Information is Secret.	Unauthorized disclosure would have ***severe negative impact*** on La Sentinelle Ltd, its shareholders, business partners, employees and/or its customers.	Secret must be labelled where possible.
Confidential information	Is the second highest level of Information Classification Distribution of Confidential information must be restricted **to a small group of people.**	Unauthorized disclosure would have ***significant negative impact*** to La Sentinelle Ltd, its shareholders, business partners, employees and/or its customers.	Confidential must be labelled where possible.
Internal Use information	Is the most common classification of La Sentinelle Ltd information. Distribution of Internal information is normally restricted **to larger groups of people**.	Unauthorized disclosure could have ***limited negative impact*** to La Sentinelle Ltd, its shareholders, business partners, employees and/or its customers	All information without an information classification must be treated as Internal Use information.
Public information	Is not confidential and is intended **for general use inside and outside La Sentinelle Ltd**	It must be released by the information owner followed by an authorized function for public release.	All information without an information classification must be treated as Public information.

Table 2 - Classification of Information

5.6 Handling of Information

Table 3.0 below shows Handling of Information

Classification	Storage	Disposal	Copying
Secret information	Secret Information must be kept in secured place to which only authorized personnel will gain access. For example an archive room with fingerprint access or locked safes or cupboards. Information kept on database must be well protected with passwords or encrypted access.	Secret information which is no longer required should be destroyed or erased depending if the information is in hard copy or soft copy **as per the Disposal and Destruction Policy.**	Information tagged as 'Secret' is not allowed to be either viewed or copied unless by authorized personnel only. Any extra or spoilt copy must be destroyed as per **Disposal and Destruction Policy**.
Confidential information	Confidential information (paper or removable media) should be stored in a locked enclosure when not in use. Media should not be left unattended on a desk. Electronic storage requires access controls and file protection mechanisms such as passwords, locking systems, etc.	Confidential information which is no longer required should be disposed of in the same way as secret information **as per the Disposal and Destruction Policy.**	Information tagged as 'Confidential' is not allowed to be copied except by authorized personnel. Any extra or spoilt copy must be destroyed as per **Disposal and Destruction Policy**.
Internal Use information	Internal Use Information should be stored safely whether in archive room or in locked cupboards and should be available to anyone on a need to know basis.	Information can be disposed by tearing and/or erasing or shredding.	No degree of restriction, duplication allowed if necessary but information should be kept inside office bounds unless proper authorization is given.
Public information	As Public Information is freely available to anyone, it does not require any safe storage.	Information can be disposed by tearing and/or erasing or shredding.	No degree of restriction, duplication allowed

Classification	Transmission			
	Electronic Mail	Manual Transmission	Fax	Telephone/ Tele-Conference
Secret information	Secret information should not be sent by email.	Information must be sent in person or through authorised employees but must be sealed in a plain envelope clearly marked, "To be Opened by Addressee Only ", thus safeguarding from attempts to read the information. Acknowledgement of receipt should be requested.	Secret information should not be sent by fax.	The identity of the recipient must be confirmed. Discussions must not take place in a public place or where conversation can be overheard. Messages should not be left on answering machines since these can be replayed by unauthorized persons.
Confidential information	May be sent through La Sentinelle Ltd's email system but to restricted persons with a business need-to-know.	Information must be sent through trusted sources but must be sealed in a plain envelope clearly marked, "To be Opened by Addressee Only ", thus safeguarding from attempts to read the information.	Authorized only from La Sentinelle Ltd Fax machines. The sender must ensure that the destination is correct and receipt acknowledged by the recipient.	Only to La Sentinelle Ltd employees and others with a business need-to-know so that it is ensured conversations are with trusted individuals.
Internal Use Information				
Public information	No restrictions	No restrictions	No restrictions	No restrictions

Table 3 - Handling of Information-Transmission

6.0 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.

7.0 User Agreement

I hereby acknowledge that I have read and I understand the Asset 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 legal or disciplinary action according to applicable laws or organizational/departmental policy.

Name : _____

Signature : _____

Date : _____