Acceptable Use 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

ACCEPTABLE USE POLICY

1.0 Objective

The objective of this policy is to ensure that employees, contractors and Third Parties are aware of the appropriate and acceptable use of company assets.

Definition of Asset: *Anything that has value to the organization. An asset extends beyond physical goods or hardware, and includes software, information, people, and reputation.*

2.0 Scope

This policy applies to all La Sentinelle Ltd employees, contractors and Third Parties and to all assets owned by the company and/or entrusted to or made accessible to La Sentinelle Ltd employees, contractors or Third Parties in the execution of their duty or contractual agreements.

3.0 References

3.1 References to ISO 27001:2013

- **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.

3.2 References to Policies

- Password Policy
- E-Mail Policy
- Internet Policy
- Mobile Device Policy

4.0 Policy Description

4.1 General Use and Ownership

- Information Resources (Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP) are strategic assets of La Sentinelle Ltd and must be treated and managed as valuable resources. La Sentinelle Ltd provides these resources to its employees for the purpose of assisting them in the performance of their job-related duties. These systems are to be used for business purposes in serving the interests of the company, and of its clients and customers in the course of normal operations

- Employees are responsible for exercising good judgment regarding reasonableness of personal use.

- While La Sentinelle's network administration desires to provide a reasonable level of privacy, users should be aware that the data/information created on the corporate systems and resources remains the property of La Sentinelle Ltd.

- It is recommended that any information that users consider sensitive or vulnerable be protected by strong passwords in line with the **Password Policy.**

4.2 Unacceptable Use

- Under no circumstances is an employee authorized to engage in any activity that is illegal under local or international laws while utilizing La Sentinelle Ltd's owned resources.

  The list below is by no means exhaustive, but attempts to provide a framework for activities which fall into the category of unacceptable use.

4.2.1 Professional Conduct

- La Sentinelle's resources **must not** be used in a manner that is false, unlawful, offensive or disruptive. Users **must not** use technology assets to intentionally view, download, store, transmit, retrieve or communicate any material that:

    1. Is harassing or threatening;
    2. Is obscene, pornographic or sexually explicit;
    3. Is defamatory;
    4. Is discriminatory in reference to race, age, gender, sexual orientation , religious or political beliefs, national origin, health or disability;
    5. Is untrue or fraudulent;
    6. Is illegal or promotes illegal activities;
    7. Is intended for personal benefit;
    8. Facilitates Internet gaming or gambling;
    9. Contains offensive humour.

4.2.2 Security and Proprietary Information

- Users (i.e. employees, contractors and Third parties) **must not** attempt to access any data, documents, email correspondences and programs contained on La Sentinelle's systems to which they are not authorized.
- Users must respect the confidentiality of other users' information and **must not** attempt to :

    1. Access Third Party systems without prior authorization by the system owner;
    2. Obtain other users' login names or passwords;
    3. Defeat or breach computer or network security measures;
    4. Intercept or access electronic files or communication of other users without approval from an Authorised Management representative of LSL;
    5. Peruse the files or information of another user without specific business need to do so or prior approval from the owner of the files or information.

- Users must not share their account(s), passwords, Personal Identification Numbers (PIN), Security Tokens, or similar information or devices used for identification and

authorization purposes. Users are responsible for the security of their passwords and should ensure that they are changed regularly as per the **Password Policy**.

- Users **must not** leave their PCS, laptops and workstations unattended. They must be secured with a password protected screensaver with the automatic activation feature set at 5 minutes or less or by logging off when the host is unattended.
- Systems administrators and authorized users **must not** divulge remote connection details or other access points of La Sentinelle Ltd's IT resources or infrastructure to anyone, without proper formal authorization from La Sentinelle's IT Head or anyone duly authorized by the latter.

4.2.3 Data Integrity

- Users **must not** knowingly destroy, or change the data stored in La Sentinelle's information systems in such a way as to compromise or reduce the accuracy, integrity or reliability of the data.

4.2.4 Operational Efficiency

- Users **must not** engage in any activity that may degrade the performance of Information Resources; deprive an authorized user access to La Sentinelle Ltd resources; obtain extra resources beyond those allocated; or circumvent La Sentinelle Ltd computer/network security measures.

- Users **must not** operate or use information assets in a manner likely to impair the availability, reliability, or performance of La Sentinelle Ltd business processes and systems, or unduly contribute to system or network congestion.

4.2.5 Software Installation, Downloads, Security

- Users **must not** download, install or run security programs or utilities such as password cracking programs, packet sniffers, or port scanners that reveal or exploit weaknesses in the security of La Sentinelle Ltd IT resources unless formal instructions having been received from the IT head or anyone duly authorized by the latter.
- Users **must not** make unauthorized copies of copyrighted or La Sentinelle Ltd owned software.
- Users **must not** use non-standard shareware or freeware software without the approval the IT head or anyone duly authorized by the latter..

4.2.6 Email and Communication Activities

- Use of e-Mail - Personal use of e-mail is allowed on a limited and reasonable basis. La Sentinelle Ltd may monitor e-mails on a random basis or in case of any business need E-mail messages and attachments **shall not** include offensive content. *(*Refer to the ***Email Policy).***
- Access to the Internet from La Sentinelle Ltd owned resources must adhere to all applicable policies. Employees **must not** allow unauthorised persons to access La Sentinelle Ltd's IT systems and/or other related resources. (Refer to ***Internet Policy).***

4.2.7 Mobile Computing

- When using mobile computing and communicating facilities, e.g. notebooks, tablets, laptops, and mobile phones, special care must be taken to ensure that business information is not compromised. Care must be taken when using mobile computing facilities in public places, meeting rooms and other unprotected areas outside of the La Sentinelle Ltd's premises. Protection must be in place to avoid unauthorised access to or disclosure of the information stored and processed by these facilities. Suitable protection must be given to the use of mobile facilities connected to networks. Remote access to business information across public network using mobile computing facilities must only take place after successful identification and authentication, and with suitable access control mechanisms in place. (Refer to ***Mobile Device Policy).***

4.3 Security

- Users must report any weaknesses identified in La Sentinelle Ltd's network security to the appropriate IT staff. Weaknesses in computer security include unexpected software or system behaviour, which may result in unintentional disclosure of information or exposure to security threats.

- Users must report any incidents of possible misuse or violation of this Acceptable Use Policy to the Head of IT, Head of Operations and/or Head of Human Resources of La Sentinelle Ltd.

5.0 Enforcement

Violation of this policy may result in disciplinary actions that may include:

i. Termination for employees and temporary staff;
ii. Termination of contractual agreements and/or assignments in the case of contractors, consultants or Third Parties.

6.0 User Acceptance

I have read and understood the Acceptable Use Policy and agree to abide by the requirements laid down therein:

Name : _____

Signature : _____

Date : _____