# Equipment Security 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

# EQUIPMENT SECURITY POLICY

## 1.0 Objective

The objective of this policy is: -

(i) To provide guidance in order to prevent loss, damage, theft or compromise of assets and interruption to La Sentinelle Ltd operations and activities;

(ii) To protect equipment from physical and environmental threats.

## 2.0 Scope

This policy applies to all La Sentinelle Ltd employees, trainees, sub-contractors or Third Parties, with a Company-Owned equipment. This policy also applies to both on-site and off-site equipment taking into account the different risks of working outside La Sentinelle Ltd premises.

## 3.0 References to ISO 27001:2013

- **Equipment Siting and Protection - A.11.2.1**

  *Equipment shall be sited and protected to reduce the risks from environmental threats and hazards and opportunities for unauthorized access.*

- **Supporting Utilities – A.11.2.2**

  *Equipment shall be protected from power failures or other disruptions caused by failures in supporting utilities.*

- **Cabling Security – A.11.2.3**

  *Power and telecommunications cabling carrying data or supporting information services shall be protected from interception or damage.*

- **Equipment Maintenance – A.11.2.4**

  *Equipment shall be correctly maintained to ensure its continued availability and integrity.*

- **Removal of Assets – A.11.2.5**

*Equipment, information or software shall not be taken offsite without prior authorisation.*

- **Security of Equipment and Assets off-Premises – A.11.2.6**

  *Security shall be applied to off-site assets taking into account the different risks of working outside the organisation's premises.*

## 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

It is important to protect equipment so as to reduce the risk of unauthorised access to information and subsequent loss or damage. Suitable equipment siting is identified within La Sentinelle Ltd premises. La Sentinelle Ltd takes appropriate actions to protect equipment which is taken off-site. Supporting facilities such as electrical supply and cabling infrastructure are maintained to ensure their proper functioning and to reduce risk from failure.

### 5.1 Equipment Siting and Protection

Equipment is sited to reduce the risks from unauthorized access, physical access and environmental threats. Equipment is sited in secure areas to minimize unauthorized access. This includes servers, laptops, notebooks, personal computers, external hard disks and pen drives. All laptops and notebooks shall be equipped with security cables; this decreases the risk of potential theft. Photocopiers, faxes and scanners are sited, whenever possible, in a viewing angle of the open space to prevent unauthorized persons having access to information.

Sensitive equipment, including servers and telecommunication devices, is sited in physically secured Data Centres. These locations are accessible to authorized personnel only, as per the **Physical Access Policy.**

Access to these sites is restricted to authorized employees and Third parties, where applicable, in accordance with ***Physical Access Policy.*** External maintenance personnel, suppliers and cleaners are always accompanied by La Sentinelle Ltd authorized staff, whenever they are required to access these physically secured locations.

The Data Centres are equipped with fire alarms, smoke detectors and fire extinguishers. The main information processing zone is equipped with cameras and a heat detector. Sensors to detect flooding, humidity, high temperatures are also available in the data centres.

It is ensured that flammable products such as chemicals are not stored in the Data Centres. For limiting risk of fire due to paper documents, the filing room of La Sentinelle Ltd is located in a zone separated from processing equipment. The filing room and store are locked when unattended.

Smoking is strictly forbidden in the security perimeters. Eating and drinking are not allowed in secure areas, unless authorized by management.

Air-conditioners located in the security perimeters of the Data Centres are maintained by external professionals. They are inspected periodically, as agreed between both parties. Preventive service maintenance is also performed by the supplier. Whenever the temperature in the Data Centre reaches the maximum tolerated limit (due mainly to faulty air-conditioners), an alarm is activated to notify this non-conformity. Corrective actions are promptly taken to remedy this situation.

La Sentinelle Ltd buildings are equipped with lightning protection facilities. The equipment is maintained by professional service providers.

## 5.2 Supporting Utilities

It is ensured that equipment is protected from power failures and other disruptions due to failures of supporting utilities. All critical equipment are connected to an Uninterrupted Power Supply (UPS). La Sentinelle Ltd ensures that all UPS are covered by a valid maintenance agreement.

The following aspects of the UPS units are inspected every three months or in line with the service level agreement (SLA) by selected professional suppliers:

- output voltages and earthing
- printed circuit boards with special solvent cleaner
- voltages at given test points in the equipment
- batteries
- electronic components

La Sentinelle Ltd building where the Data Centre is hosted, is equipped with a generator which provides alternate electrical power during power failures. An adequate supply of fuel is available to ensure that the generator can perform for a prolonged period. In case the autonomy of the generator and UPS are about to be reached, all servers and communications equipment are manually switched off.

Fire alarm systems are installed at the Data Centres. The systems are inspected once every four months or inline with the service level agreement (SLA) with the respective suppliers. The following preventive maintenance services are offered under the maintenance contract with our supplier:

- check and cleaning of smoke and heat detectors;
- check and cleaning of sounders and callpoints;
- fire alarm panel circuits test;
- bells and sounders test;

Fire extinguishers located at the Data Centres are serviced twice in a yearr or in line with the service level agreement (SLA) with the applicable service provider. La Sentinelle Ltd

management ensures that the staff has obtained appropriate training for using this equipment in case of fire fighting.

All supporting utilities are regularly tested and, whenever applicable, stress tested. Service Level Agreements (SLAs) are periodically monitored to ensure conformity to agreement.

## 5.3 Cabling Security

Power and telecommunications cabling carrying data and supporting information services are protected from interception or damage. Cabling is secured with the appropriate infrastructures (cable raceways, conduit and wiring ducts). Wherever possible, network wiring is separated from all other wiring (example, electrical wiring), so as to enable protection and monitoring and to reduce the danger of accidental electronic interference.

Equipment and cables are clearly labeled in order to minimize handling errors, such as accidental patching of wrong network cables. Wherever there is a risk for rodent damage, armoured cables are installed.

The following controls are enforced:

- Network access points are disabled whenever they are not in use.
- Incoming and outgoing communication lines are hidden from view and are adequately protected against damage.
- Access to patch panels and cable rooms are restricted to authorized persons only.
- Regular reviews of cables conditions are performed by the La Sentinelle Ltd IT team.

## 5.4 Equipment Maintenance

Equipment is correctly maintained to ensure its continued availability and integrity. Maintenance of equipment is performed in-house whenever expertise is available , otherwise it is sub-contracted to external parties. Priority is given to companies who supplied the equipment. The criticality of the equipment is an important factor in the award of the contract. Therefore, when entering into an agreement with sub-contractors, the response and intervention times are carefully assessed and agreed by both parties. Equipment is maintained in accordance with the supplier's recommended service intervals and specifications.

Only authorized personnel are allowed to carry out repairs and services on any equipment. A list of authorized maintenance personnel is recorded in the ***Maintenance Personnel Form.***

Whenever in-house expertise is available, equipment which falls under the responsibility of La Sentinelle Ltd IT department, whether on-site or off-site, is maintained by the IT staff or Service Provider, as applicable. This applies to equipment such as servers, PCs, notebooks, telecommunication equipment.

A maintenance log book is kept for recording faults reported and all preventive and corrective maintenance performed on the equipment. Prior to repairs, whether by personnel on site or external to La Sentinelle Ltd, backup and deletion of sensitive data are performed.

It is also ensured that all requirements imposed by insurance policies are complied with.

## 5.5 Removal of Assets

Management authorization is required prior to taking any equipment or information asset outside La Sentinelle Ltd premises. Spot checks may be carried out to detect unauthorized removal of property. Such spot checks will be carried out in accordance with the relevant legislation and regulations.

Employees, contractors and Third Party users who have the authority to exercise off-site, removal of assets are clearly identified. Equipment is recorded when taken off-site and recorded when returned. The Removal of Assets process Flow is illustrated in Appendix A.

Whenever applicable, time limits for equipment removal are set and returns checked for compliance.

## 5.6 Security of Equipment & Assets Off-Premises

Security is applied to off-site equipment taking into account the different risks of working outside La sentinelle Ltd premises.

A formal record for the authorisation to move company owned equipment off-premises, whether temporarily or permanantly, is obtained prior to the equipment removal. This applies to (but not limited to) the following:

- Loan/Lease of equipment to employees
- Sending equipment to suppliers for repairs
- Employees using equipment for off-site services
- Permanent off-site equipment such as antennas or PABX

Personnel who have been issued laptops, PenDrives, External Harddrives, Personal Computers, Mobile Phones are under moral obligation of not leaving the equipment unattended while off-premises in line with the Asset Policy and Acceptable Use Policy. Screen savers and password protections are enabled to prevent unauthorised access.

Manufacturers' instructions for protecting equipment need to be observed at all times, for example protection against exposure to environmental threats and hazards. It is ensured that the employee/customer responsible for the equipment implements adequate safety procedures against theft. In case of theft of equipment off-premises, a report is lodged with the police and insurance company.

Suitable controls are applied to personnel of La Sentinelle Ltd who carries equipment for home-working. They are not allowed to lend the equipment to family members or friends for personal use to avoid misuse or damage. Personnel issued with laptops, Pen Drives, External Hard drives, Personal Computerss, Mobile Phones are made aware of precautions to be taken on how to protect the equipment and have signed La Sentinelle Ltd's ***Acceptable Use Policy.***

Whenever applicable, an adequate insurance cover is established to provide protection to off-site equipment.

## 6.0 Enforcement

This Equipment Security Policy is communicated to all employees during communication meetings, awareness and training sessions. Spot checks and internal audits are carried out in order to ensure that La Sentinelle Ltd's employees, trainees and applicable Third Parties comply with this policy.

Appendix A - *Removal of Assets Business Process Flow*