Physical Access 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

PHYSICAL ACCESS POLICY

1.0 Objective

The objective of this policy is to prevent unauthorized physical access, damage and interference to the organisation's information and information processing facilities.

2.0 Scope

This policy applies to all Employees, Trainees and Third Parties who have access to La Sentinelle Ltd physical premises and information processing facilities.

3.0 References to ISO 27001:2013

- **Physical Security Perimeter – A.11.1.1**
  Security perimeters shall be defined and used to protect areas that contain, either sensitive or critical information and information processing facilities.

- **Physical Entry Controls – A.11.1.2**
  Secure areas shall be protected by appropriate entry controls to ensure that only authorised personnel are allowed access.

- **Securing Offices, Rooms and Facilities – A.11.1.3**
  Physical security for offices, rooms and facilities shall be designed and applied.

- **Protecting Against External and Environmental Threats – A.11.1.4**
  Physical protection against natural disasters, malicious attack or accidents shall be designed and applied.

- **Working in Secure Areas – A.11.1.5**
  Procedures for working in secure areas shall be designed and applied.

- **Delivery and Loading Areas – A.11.1.6**
  Access points such as delivery and loading areas and other points where unauthorised persons could enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorised access.

4.0 Policy Description

1. La Sentinelle Ltd operates from the following physical premises: -
    i. Head Office located at Riche Terre/Baie du Tombeau
    ii. A secondary office located at Port Louis.

2. Information processing facilities are present in both premises, with the Data Centre in the Head Office and the Disaster Recovery Centre in Port Louis.

3. All facilities including information processing facilities are physically protected in proportion to the criticality or importance of their respective functions.

4. Physical access to La Sentinelle Ltd premises is controlled as follows: -
    a. Security Cards at entrance of the premises, log the name of all visitors and car/vehicle registration numbers in their log books and issue a visitor's pass to visitors. The visitor's badge must be worn by visitors and remain visible at all time while they are present in the premises.
    b. Receptionists in the reception area at entrance, confirm purpose and appointment with concerned stakeholder of La Sentinelle Ltd. Visitor is either escorted to meeting place by receptionist or the visitor is met by the concerned stakeholder in the reception area and escorted in the building/office premises.
    c. On departure from the premises, the visitor's badge is returned to the security guards, who then record the time the car leaves the premises.
    d. After office hours and non-working days, the security guards authorize access to premises to employees, in case any urgent intervention is required. All movements are recorded in the log books in the custody of the security guards.

5. Entry controls are set to secure physical areas of La Sentinelle Ltd and to ensure that only authorised personnel are allowed access to these areas.

6. Data Centers are equipped with Access Control Systems using both Fingerprints and HID Cards. Access Control is managed using IVMS Software. The system administrator of IVMS is also La Sentinelle Ltd IT Department System Administrator.

7. A Log Book (Data Centre Intervention Form) is maintained in both Data Centers to record the following, by all persons entering the said secured premises: -
    a. Date
    b. Time In / Time Out

c. Name of Person
d. Reason for accessing the secured zone
e. Nature of Intervention

This log book is reviewed periodically by the Head of IT of La Sentinelle Ltd for monitoring purposes.

8. Servers and communication equipment are secured in the Data Centres, access to which is controlled by an Access Control System. Only authorised employees of La Sentinelle Ltd have access to these secured perimeters. A List (Physical Access Authorisation Form) is maintained by La Sentinelle Ltd IT Department to record the authorized staff members of La Sentinelle Ltd, who have access to the Data Centres.

9. Access to information resources facilities are granted only to La Sentinelle Ltd support personnel and contractors whose job responsibilities require access to that facility.

10. Access to Data Centres is limited to staff of IT Department and Maintenance Staff of La Sentinelle Ltd.

11. Any other third party requiring access in the Data Centres, e.g. hardware/software suppliers, are always accompanied by an authorized staff of IT Department.

12. Cleaning personnel are always accompanied in the data Centres by an Authorised IT staff.

13. Photographic, video, audio and other recording activities are not allowed within secure areas, unless formal authorization has been obtained by authorized La Sentinelle Ltd Management Team.

14. All requests for authorisations to secured perimeters of La Sentinelle Ltd, need to be approved by the Head of IT and/or Head of Human Resources.

15. The Head of IT who is responsible for the information resources and technology facility must review access records and visitor logs for the facility on a periodic basis and investigate any unusual access.

16. On termination or suspension of employees who have access to secured perimeters, the Head of the Human Resources Department shall immediately inform the Head of IT, so

that the access is immediately revoked both on the Access Control System and the Physical Access Forms are amended accordingly.

17. Lost or stolen access cards and/or keys must be reported to the Head of IT who is responsible for the information resources and technology facility.

18. The Data Centres are equipped with sensors for controlling humidity, temperature and flooding. SMS alerts are sent to members of the IT Department as per Authorised list of employees having access to the Data Centre.

19. Air Conditioners in the Data Centres are installed in redundancy to minimize the risk of excessive temperature in case of faulty air conditioner.

20. Data Centre at Head Office is equipped by CCTV cameras. Recordings are monitored by the Head of IT and are kept for a period of one month.

21. A UPS (Uninterruptible Power Supply) is installed to ensure electric supply in case of electrical outage (sustainable for a period of 15-20 minutes depending on the load) and to protect the servers and other equipment from electrical surcharge in case of electrical fluctuations. In case of power cut the generator will ensure electrical supply.

22. Data Centres are also equipped with fire extinguishers and fire alarms. Maintenance of fire extinguishers and fire alarms, are ensured by and under the responsibility of the Maintenance team of La Sentinelle Ltd.

23. La Sentinelle Ltd complies with occupational safety and health legal provisions in accordance with the Mauritian legislation. The purpose is to optimize work efficiency, to prevent accidents and eliminate work hazards, to promote and maintain safety standards and to create awareness. Fire drills are done between 2-3 times per year by the Health and Safety Department, applicable to all persons in the premises. Fire drills can be planned or unplanned. Emergency exits are used during fire drills for evacuation.

24. Deliveries are done in specific zones in the physical premises and access to the physical premises is recorded by the security guards as per control @4 above. All IT delivery is done through the Reception area and suppliers are always escorted in the office premises.

5.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action that may lead to and including termination of employment. A violation of this policy by a temporary worker, contractor, vendor or third party may result in the termination of their contract or assignment with La Sentinelle Ltd.

6.0 Physical Access Policy Agreement

I have read and I understand the Physical Access Policy and its related contents. I understand that I must comply with the instructions and guidelines given therein and if I violate the rules explained herein, I may face legal or disciplinary action according to applicable laws or company policy.

Name : _____

Signature : _____

Date : _____