Laptop 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

LAPTOP POLICY

1.0 Objective

The objective of this policy is to

1. Ensure that employees are fully aware of the security measures with respect to company owned laptops;
2. Provide guidance for appropriate actions and measures that must be taken by all employees who have been issued with a company owned laptop, in order to ensure the physical security of the laptop and the protection of company information contained therein.

2.0 Scope

This policy applies to all La Sentinelle Ltd employees who have been assigned with a company owned laptop.

3.0 References

3.1 References to ISO 27001:2013 Controls

- **Information Security Awareness, Education and Training – A.7.2.2**

  All employees of the organisation and where relevant, contractors shall receive appropriate awareness, education and training and regular updates in the organisation's policies and procedures, as relevant to the job function.

- **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.

- **Return of Assets – A.8.1.4**

  All employees and external party users shall return all of the organisation's assets in their possession upon termination of their employment, contract or assignment.

- **Handling of Assets – A.8.2.3**

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

- **Management of Removable Media – A.8.3.1**

  Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organisation.

- **Disposal of Media – A.8.3.2**

  Media shall be disposed of securely when no longer required, using formal procedures.

- **Physical Media in Transit – A.8.3.3**

  Media containing information shall be protected against unauthorised access, misuse or corruption during transportation.

- **Use of Secret Authentication Information – A.9.3.1**

  Users shall be required to follow the organisation's practices in the use of secret authentication information.

- **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 unauthorised access.

- **Secure Disposal or re-Use of Equipment – A.11.2.7**

  All items of equipment containing storage media shall be verified to ensure that any sensitive data and licenses software has been removed or securely overwritten prior to disposal or re-use.

- **Unattended User Equipment – A.11.2.8**

  Users shall ensure that unattended equipment has appropriate protection.

- **Management of Removable Media – A.12.3.1**

  Back-up copies of information, software and system images shall be taken and tested regularly in accordance with an agreed back-up policy.

- **Reporting Information Security Events – A.16.1.2**

  Information security events shall be reported through appropriate management channels as quickly as possible.

- **Compliance with Legal and Contractual Requirements – A.18.1**

  To avoid breaches of any legal, statutory, regulatory and contractual obligations related to information security and of any security requirements.

3.2 References to Policies & Forms

- Asset Policy
- Acceptable Use Policy
- Disposal and Destruction Policy
- Password Policy
- Compliance Policy
- Laptop Financed by Company Policy

4.0 Policy Description

Laptops are assigned to employees depending on their specific job function and/or organisational hierarchy. Laptops are the property of La Sentinelle Ltd and accordingly the company reserves the right to monitor a laptop at any time. The primary purpose of a laptop is to conduct official business.

Procurement of Laptops

- Procurement of laptops should be approved by the respective Head of Departments, Head of IT Department and Finance Department of the company.
- All laptop configurations and technical specifications must be approved by The IT Department of La Sentinelle Ltd, prior to procurement.

Financing of Laptops

- 100% by La Sentinelle Ltd – Laptops remain the property of La Sentinelle Ltd and are assigned to employees as company owned asset.
- Company: Employee in the ratio of 2:1 – La Sentinelle Ltd bears 2/3 of the costs and employee bears 1/3 of the cost of the laptop. The employee share is borne by the company which is subsequently deducted in monthly instalments from employee's salary. In such cases, the laptop owner is the employee. However, La Sentinelle Ltd keeps a lien on the laptop for a period of three (3) years.

All La Sentinelle Ltd computer systems face information security risks. Laptops are an essential business tool but their very portability makes them particularly vulnerable to theft or physical damage. Furthermore, the fact that they are often used outside La Sentinelle's premises increases the threats from people who are external to La Sentinelle Ltd and who may not have its interests at heart.

Appropriate measures are therefore taken when using laptops to ensure their physical security and the confidentiality, integrity and availability of sensitive information contained on these devices.

The guidelines listed below with regards to laptops and laptop users are by no means exhaustive and employees are therefore expected to take all necessary measures to ensure safeguarding of both the physical asset and most importantly the information that they contain given the nature of La Sentinelle Ltd business and sensitive information that are dealt with. Loss of sensitive information is deemed more serious than the loss of the physical asset itself.

4.1 User Responsibilities and Physical Security

- All employees assigned a laptop by La Sentinelle Ltd are responsible for the physical security of their laptops at all times and for protecting the information contained therein.

- Laptops must always be carefully looked after to minimise the risk of loss, theft, unauthorised use or tampering.

- Laptops must not be left in an unattended car, or left visible in unattended cars or in an unsecured area.

- Laptops need to be stored securely and/or kept close to the owner/user at all times especially in public places.

- Laptops must be stored in a physically secure location when not in use, e.g. Users should ensure that laptops are locked in safes in hotel rooms, deposit boxes or locked in suitcases during their absence instead of leaving them unattended in a hotel room.

- Laptops should always be kept in possession of the user (employee) and within sight whenever possible or secured with a laptop security cable in the office.

- Laptops should be carried and stored in padded laptop bags to reduce the risk of accidental damage.

- Users of laptops may not load, download or distribute pirated/unlicensed software from any source, nor any inappropriate images or videos.

- Users of laptops should not store any authentication credentials such as passwords, tokens or any other items necessary to access information, with the laptop at any time.

- Users (employees) should treat all laptops and authentication credentials with the same care as they would treat their valued possessions.

- Users (employees) will be held accountable for unauthorised or illegal use of company owned laptops.

- Laptops are provided for official business use to authorized employees, who should ensure that they are not to be used by others such as family members, friends or other colleagues.

- Users are not authorised to change any system configuration on their laptops. La Sentinelle Ltd authorised IT personnel are the sole administrators and as such all administrator rights on laptops are granted exclusively to La Sentinelle Ltd IT System Administrators.

- Users should keep a record of the laptop – Serial number, asset identification details, badge number, brand, configuration details, etc and contact information details needed in an emergency situation, to report if laptop is lost or stolen.

- Users are recommended to use strong passwords on laptops to keep them secure from unauthorised access, as per ***Password Policy.***

- Users must ensure that Password-protected screensaver is automatically activated when laptops are not in use or are unattended.

4.2 Incident Reporting and Compliance

- A security incident is defined as an issue that comes to the attention of any staff, which breaches the policies of La Sentinelle Ltd. This includes the loss of control, compromise, unauthorized disclosure, unauthorized possession, and/or unauthorized access of the organisation's information, whether physical, electronic, verbal or recording.
- All incidents or breaches must be reported immediately or as soon as possible to the Head of IT of La Sentinelle Ltd at **eddy.lareine@lasentinelle.mu or 57271543**
- Damage to, including suspected tampering or loss of a laptop or mobile device must be reported to the Head of IT of La Sentinelle Ltd at **eddy.lareine@lasentinelle.mu or 57271543.** The IT Department is responsible to make an immediate assessment of damage incurred, which will include a review of the security of the laptop, associated passwords, to determine whether security may have been compromised.

Loss or theft of a laptop must be reported by the user through their Head of Departments and Head of Human Resource/Capital to the Head of IT Department. The loss or theft of a laptop will also be reported to the police department and the insurance company and the user should cooperate and provide all the necessary information to the Police and to the insurance company.

4.3 Virus Protection

- Viruses are a major threat to La Sentinelle Ltd and laptops are particularly vulnerable if their anti-virus software is not kept up-to-date. Anti-virus software is installed on all laptops and automatic updates are enabled when connecting to La Sentinelle Ltd network.
- Users are made aware through training and awareness sessions, of the possibility of laptops being infected by computer viruses through email attachments. It is strongly recommended not to open email attachments from unknown senders. Files downloaded to computers from sources such as CD/DVD, USB hard disks and memory sticks, network files, email attachments or files from the Internet are virus-scanned.
- Users must ensure that their laptop is connected to La Sentinelle Ltd network at least once weekly to ensure that security, anti-virus and other updates are deployed to their laptop as applicable. Exception is made to employees on overseas travel, who should nevertheless ensure that they connect to La Sentinelle Ltd network as soon as they are back from their trip, while taking all the necessary measures while travelling.
- Any security incidents (such as virus infections) are to be promptly notified to La Sentinelle Ltd IT Department on **it.helpdesk@lasentinelle.mu or 57478514.**

4.4 Training and Awareness

- Training and awareness sessions are held with users to sensitize them against risks and laptop security. The following are covered through these sessions: -

    - User responsibility through increased user awareness of the risks, application of this Laptop Policy and compliance.
    - Physical security both within office premises and external to the company premises, including while travelling.
    - Data protection – use of passwords, restricting access to sensitive company information, anti-virus updates, backups, etc.

- Users are given appropriate instructions, when issued with a laptop, on the use of the security functionality and the responsibility for safeguarding the laptop.

- Users are recommended to contact the IT Department of La Sentinelle Ltd at **it.helpdesk@lasentinelle.mu or 57478514** for any further guidance regarding laptops.

4.5 Other Controls

- **Unauthorized software** - It is not allowed to download, install or use software programs unless authorised by Head of IT Department of La Sentinelle Ltd. Unauthorized software could introduce serious security vulnerabilities into La Sentinelle Ltd networks. Software packages that permit the computer to be 'remote controlled' (e.g. PC anywhere) and 'hacking tools' (e.g. network sniffers and password crackers) are explicitly forbidden on La Sentinelle Ltd equipment unless they have been explicitly authorised by Head of IT Department of La Sentinelle Ltd or legitimate business purposes.
- **Backups** - Laptop owners must ensure that data contained on their laptops are periodically backed up. If the laptop is stolen, lost or damaged, or if it simply malfunctions, backups can be transferred on a new equipment to ensure availability of data as per *Backup Policy.*
- **Laws, regulations and policies** - All employees of La Sentinelle Ltd must comply with relevant laws, regulations and policies applying to the use of laptops/computers and information.
- **Termination** – Head of Departments and Head of Human Resources must inform La Sentinelle Ltd Head of IT at **it.helpdesk@lasentinelle.mu** whenever an employee is terminated and/or leaves the organisation, to arrange for return of all company assets, including company laptops and all peripherals, in custody of employees.
- **Disposal of Laptops** – Prior to disposal of laptops, the IT Department must ensure that all storage media have been removed and destroyed, and laptops are subsequently disposed of securely as per the **Disposal and Destruction Policy.**

5.0 Security Procedures for Employees using Laptops

On receipt of their laptops, users are required to sign the declaration issued by the IT Department of La Sentinelle Ltd, accepting that they will comply with the security procedures and acknowledging that they are responsible for the physical security of the laptop as well as the information stored on them.

6.0 Enforcement

Any breach of this policy will be treated as a security incident and like other allegations of wrongdoing at La Sentinelle Ltd. Allegations of misconduct will be adjudicated according to established procedures. Sanctions for non-compliance to La Sentinelle Ltd's Laptop Policy may include, but are not limited to, one or more of the following:

- Disciplinary action according to applicable La Sentinelle Ltd policies;
- Termination of employment; and/or
- Legal action according to applicable laws and contractual agreements.

7.0 Laptop User Agreement

I have read and I understand La Sentinelle Ltd Laptop Policy and its related contents. I understand that if I violate the rules explained herein, I may face legal or disciplinary action according to applicable laws or company policy.

Name : _____

Signature : _____

Date : _____