BYOD (Bring Your Own Device) 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

BYOD POLICY (Bring your own Device)

1.0 Objective

The objective of this policy is to establish La Sentinelle Ltd guidelines for employee use of personally owned electronic devices for work-related purposes.

2.0 Scope

This policy applies to all La Sentinelle Ltd employees who have been authorized to use their personal electronic devices for work-related purposes. Formal authorisation for use of personal owned devices, should be obtained by the employee, in writing from La Sentinelle Ltd Head of Human Resources and the Head of IT Department.

Personal electronic devices include personally owned cellphones, smartphones, tablets, laptops and computers.

The use of personal devices is limited to certain employees and may be limited based on compatibility of technology.

3.0 References to IS0 27001:2013

- **Mobile Device Policy - A.6.2.1**

  A policy and supporting security measures shall be adopted to manage risks introduced by using mobile devices.

4.0 Policy Description

Employees of La Sentinelle Ltd may have the opportunity to use their personal electronic devices for work purposes when authorized in writing, in advance, by the Employee and La Sentinelle Ltd Management – Head of Human Resource and Head of IT. Personal electronic devices include personally owned cellphones, smartphones, tablets, laptops and computers.

The use of personal devices is limited to certain employees at the discretion of La Sentinelle Ltd and may also be limited based on compatibility of technology.

4.1 Device Protocols

To ensure the security of La Sentinelle Ltd's information, authorized employees are required to have anti-virus and mobile device management (MDM) software installed on their personal mobile devices. This MDM software will store all company-related information, including calendars, e-mails and other applications in one area that is password-protected and secure. La Sentinelle Ltd's IT department must install this software prior to allowing use of the personal device for work purposes.

Employees may store company-related information only in this area. Employees may not use cloud-based apps or backup that allows company-related data to be transferred to unsecure parties. Due to security issues, personal devices may not be synchronized with other devices in employees' homes. Making any modifications to the device hardware or software beyond authorized and routine installation updates is prohibited unless approved by La Sentinelle Ltd Head of IT. Employees may not use unsecure Internet sites.

4.2 Restrictions on Authorized Use

Employees whose personal devices have camera, video or recording capability are restricted from using those functions anywhere in the building or on company property at any time unless authorized in advance by La Sentinelle Ltd Management.

While at work, employees are expected to exercise the same discretion in using their personal devices as is expected for the use of company devices. La Sentinelle Ltd policies pertaining to harassment, discrimination, retaliation, trade secrets, confidential information and ethics, apply to employee use of personal devices for work-related activities.

Excessive personal calls, e-mails or text messaging during the workday, regardless of the device used, can interfere with employee productivity and be distracting to others. Employees must handle personal matters on non-work time and ensure that friends and family members are aware of the policy. Exceptions may be made for emergency situations and as approved in advance by management. Managers reserve the right to request employees' cellphone bills and use reports for calls and messaging made during working hours to determine if use is excessive.

Nonexempt employees may not use their personal devices for work purposes outside of their normal work schedule without authorization in advance from management. This includes reviewing, sending and responding to e-mails or text messages, responding to phone calls, or making phone calls.

Employees may not use their personal devices for work purposes during periods of unpaid leave without authorization from La Sentinelle Ltd Management. La Sentinelle Ltd reserves the right to deactivate the company's application and access on the employee's personal device during periods of leave.

An employee may not store information from or related to former employment on the company's application.

Employees' family and friends should not use personal devices that are used for company purposes.

4.3 Security

Employees using personally-owned devices and related software for network and data access will, without exception, use secure data management procedures. All devices that are able to store data must be protected by a strong password in line with the company's Password Policy.

All users of personally-owned devices must employ reasonable physical security measures. End users are expected to secure all such devices whether or not they are actually in use and/or being carried. This includes, but is not limited to, passwords, encryption, and physical control of such devices whenever they contain enterprise data.

Any non-business computers used to synchronize with these devices will have installed up-to-date Anti-Virus and Anti-Malware software deemed necessary by La Sentinelle Ltd's IT department.

Passwords and other confidential data as defined by La Sentinelle Ltd, are not to be stored unencrypted on mobile devices.

Any device that is being used to store La Sentinelle Ltd data must adhere to the authentication requirements of La Sentinelle Ltd's IT department. In addition, all hardware security configurations must be pre-approved by La Sentinelle Ltd's IT department before any enterprise data-carrying device can be connected to the organizational network.

4.4 Privacy/Company Access

No employee using his or her personal device should expect any privacy except that which is governed by law. La Sentinelle Ltd has the right, at any time, to monitor and preserve any communication that use La Sentinelle Ltd networks in any way, including data, voice mail, telephone logs, Internet use and network traffic, to determine proper use.

Management reserves the right to review or retain personal and company-related data on personal devices or to release the data to government agencies or third parties during an investigation or litigation. Management may review the activity and analyze use patterns and may choose to publicize these data to ensure that La Sentinelle Ltd's resources in these areas are being used according to this policy. Furthermore, no employee may knowingly disable any network software or system identified as a monitoring tool.

4.5 Lost, Stolen, Hacked or Damaged Equipment

Employees are expected to protect personal devices used for work-related purposes from loss, damage or theft. In an effort to secure sensitive company data, employees are required to have "remote-wipe" software installed on their personal devices by the IT department prior to using the devices for work purposes. This software allows the company-related data to be erased remotely in the event the device is lost or stolen. Wiping company data may affect other applications and data.

La Sentinelle Ltd will not be responsible for loss or damage of personal applications or data resulting from the use of company applications or the wiping of company information. Employees must immediately notify La Sentinelle Ltd Management – Head of Human Resource and Head of IT, in the event their personal device is lost, stolen or damaged. If IT is unable to repair the device, the employee will be responsible for the cost of replacement.

Employees may be subject to disciplinary action up to and including termination of employment for damage to personal devices caused willfully by the employee.

4.6 Termination of Employment

Upon resignation or termination of employment, or at any time on request, the employee may be asked to produce the personal device for inspection. All company data on personal devices will be removed by IT upon termination of employment.

5.0 Enforcement

Employees who have not received authorization in writing from La Sentinelle Ltd authorised management and who have not provided written consent will not be permitted to use personal devices for work purposes. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6.0 Employee Declaration

I have read and I understand the above BYOD Policy, and consent to adhere to the rules outlined therein.

Name : _____

Signature : _____

Date : _____