# Cyber 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

# CYBER SECURITY POLICY

## 1.0 Objective

The objective of this policy is to preserve the security of our data and technology infrastructure. The more we rely on technology to collect, store and manage information, the more vulnerable we become to severe security breaches. Human errors, hacker attacks and system malfunctions could cause great financial damage and may jeopardize our company's reputation.

## 2.0 Scope

This policy applies to all our employees, contractors, volunteers and anyone who has permanent or temporary access to our systems and hardware.

## 3.0 Policy elements

Confidential data is secret and valuable. Common examples are:

- Unpublished financial information
- Data of customers/partners/vendors
- Customer lists (existing and prospective)

All employees are obliged to protect his data. This policy will give the employees of La Sentinelle instructions on how to avoid security breaches.

## 4.0 Policy Description

### 4.1 Protect personal and company devices

When employees use their digital devices to access company emails or accounts, they introduce security risk to our data. We advise our employees to keep both their personal and company-issued computer, tablet and cell phone secure. They can do this if they:

- Keep all devices password protected.
- Choose and upgrade a complete antivirus software.

- Ensure they do not leave their devices exposed or unattended.
- Install security updates of browsers monthly or as soon as updates are available.
- Log into company accounts and systems through secure and private networks only.

We also advise our employees to avoid accessing internal systems and accounts from other people's devices or lending their own devices to others.

When new hires receive company-issued equipment they will receive instructions for:

- Installation of security updates of browsers
- Using secure private networks (VPN)

They should follow instructions to protect their devices and refer to our Systems and Network Administrator if they have any questions.

## 4.2 Keep e-mails safe

E-mails often host scams and malicious software (e.g. worms.) To avoid virus infection or data theft, we instruct employees to:

- Avoid opening attachments and clicking on links when the content is not adequately explained (e.g. "watch this video, it's amazing.")
- Be suspicious of clickbait titles (e.g. offering prizes, advice.)
- Check email and names of people they received a message from to ensure they are legitimate.
- Look for inconsistencies or give-aways (e.g. grammar mistakes, capital letters, excessive number of exclamation marks.)

If an employee isn't sure that an e-mail they received is safe, they can refer to our Systems and Network Administrator.

## 4.3 Manage passwords properly

Password leaks are dangerous since they can compromise our entire infrastructure. Not only should passwords be secure so they won't be easily hacked, but they should also remain secret. For this reason, we advice our employees to:

- Choose passwords with at least eight characters (including capital and lower-case letters, numbers and symbols) and avoid information that can be easily guessed (e.g. birthdays.)

- Remember passwords instead of writing them down. If employees need to write their passwords, they are obliged to keep the paper or digital document confidential and destroy it when their work is done.

- Exchange credentials only when absolutely necessary. When exchanging them in-person isn't possible, employees should prefer the phone instead of email, and only if they personally recognize the person they are talking to.
- Change passwords at regular intervals, recommended after every three to four months and to avoid re-using or cycling old passwords.
- Change temporary passwords at the first log-on.
- Not to include passwords in any automated log-on process.
- Not to share individual user passwords.
- Not to use same password for business and non-business purposes.

Employees should also refer to the Password Policy.

## 4.4 Additional measures

To reduce the likelihood of security breaches, we also instruct our employees to:

- Turn off their screens and lock their devices when leaving their desks.
- Report stolen or damaged equipment as soon as possible to HR/ IT Department.
- Change all account passwords at once when a device is stolen.
- Report a perceived threat or possible security weakness in company systems.
- Refrain from downloading suspicious, unauthorized or illegal software on their company equipment.
- Avoid accessing suspicious websites.

Employees should also comply with the Internet Usage Policy

Our Systems and Network Administrator should:

- Install firewalls, anti-malware software, e-mail Gateway security and access authentication systems.
- Arrange for security training to all employees.
- Inform employees regularly about new scam emails or viruses and ways to combat them.
- Investigate security breaches thoroughly.
- Follow this policies provisions as other employees do.

### 4.5 Remote employees

Remote employees must follow this policy's instructions too. Since they will be accessing our company's accounts and systems from a distance, they are obliged to follow all data encryption, protection standards and settings, and ensure their private network is secure.

We encourage them to seek advice from our Systems and Network Administrators.

## 5.0 Enforcement

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 Cyber Security Policy, and consent to adhere to the rules outlined therein.

**Name** : _____

**Signature** : _____

**Date** : _____