Network 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

NETWORK SECURITY POLICY

1.0 Objective

The objective of this policy is to ensure the protection of information in networks and the protection of the supporting infrastructure.

2.0 Scope

This policy applies to all employees of La Sentinelle Ltd and contractual Third Parties of La Sentinelle Ltd who use IT facilities and equipment, or have access to, or custody of, customer information or La Sentinelle Ltd information.

3.0 References ISO 27001:2013

- **Network Controls – A.13.1.1**
  Networks shall be managed and controlled in order to be protect information in systems and application.

- **Security of Network Services – A.13.1.2**
  Security mechanisms, service levels and management requirements of all network services shall be identified and included in any network services agreement, whether these services are provided in-house or outsourced.

4.0 Policy Description

4.1 Network Controls

Below controls have been implemented by La Sentinelle Ltd to ensure the security of information in networks, and the protection of connected services from unauthorized access:

1. The IT Department of La Sentinelle Ltd has the operational responsibility for networks which is segregated from computer operations.

2. Responsibilities and procedures for the management of remote equipment, including equipment in user areas have been established.

3. Controls have been established to safeguard the confidentiality and integrity of data passing over LaSentinelle Ltd network. Availability of network services is maintained by a redundant network architecture.

4. Logging/monitoring of network activities with the use of a security monitoring appliance has been implemented to enable recording of security relevant actions.

5. Network management activities are closely coordinated both to optimize the service to the organization and to ensure that controls are consistently applied across the information processing infrastructure.

4.2 Security of Network Services

Security features, service levels, and management requirements of all network services are identified and included in any network services agreement. These include but are not limited to the following:

1. Security technology (encryption, authentication, network connection controls);
2. Technical parameters for connecting to service provider securely;
3. Procedure(s) for allowing access to required services where necessary;
4. Controls relating to data stored on Service Provider system such as personal data.

The ability of the network service provider to manage agreed services in a secure way is determined and regularly monitored, and the right to audit is also agreed. If security weaknesses are observed, additional controls to offset these are proposed.

Availability of network services is also ensured by resilience/fail-over of core equipment and service provider systems.

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 Network Security Policy Agreement

I have read and I understand the Network Security 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 : _____