Network Access Policy

Version 3.0

12th February 2020

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 ACCESS POLICY

1.0 Objective

The objective of this policy is to establish the rules for the access and use of La Sentinelle Ltd network infrastructure and to prevent unauthorized access to the company's networked services in order to preserve the confidentiality, integrity and availability of information.

2.0 Scope

This policy applies to all employees of La Sentinelle Ltd and Third Parties who use the company's networked services.

3.0 References ISO 27001:2013

- **Access Control Policy – A.9.1.1**
  An access control policy shall be established, documented and reviewed based on business and security requirements.

- **Access to Networks and Network Services – A.9.1.2**
  Users shall only be provided with access to the network and network services that they have been specifically authorised to use.

- **User Registration and De-Registration – A.9.2.1**
  A formal user registration and de-registration procedure is implemented to enable assignment of access rights.

- **Review of User Access Rights – A.9.2.5**
  Asset owners shall review users' access rights at regular intervals.

- **Removal or Adjustment of Access Rights – A.9.2.6**
  The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.
- **Network Controls – A.13.1.1**
  Networks shall be managed and controlled, in order to protect information in systems and applications.

4.0 References to Policies and Forms

- Password Policy
- Logical Access Policy
- Physical Access Policy
- User Registration and De-Registration Form
- Computer Services Request Form
- Network Access Request Form

5. Definitions

Network Equipment – Routers, Switches, Firewalls

IPS – Intrusion Prevention System

ACS – Access Control Server

Remote Access – Any access to La Sentinelle Ltd Corporate network through a non-La Sentinelle Ltd controlled network, device, or medium.

DMZ – Demilitarized Zone

VPN – Virtual Private Network

VLAN – Virtual Local Area Network

6.0 Policy Description

6.1 Access to Networks and Use of Network Services

The following measures have been implemented so that users are only provided with access to the services that they have been specifically authorised to use:

a) Users are restricted to networks and network services which they are allowed to access as per the ***User Registration Form (Ref….)*** *or* ***Network Access Request Form (Ref…..)*** approved by user's manager or responsible party upon employment. Any access change requires filling of a new ***Network Access Request Form*** to be filled in and submitted to the IT Department.

b) Network Equipment are configured with the appropriate security restrictions wherever applicable.

c) IPS have been deployed to reinforce security as they provide a means for monitoring and react to potential intrusion threats.

d) Systems that are accessed from outside La Sentinelle Ltd network via private WAN or VPN tunnel are secured accordingly via firewalls and VPN access will be monitored regularly.

e) La Sentinelle Ltd may block, restrict or limit application traffic as needed to ensure adequate bandwidth for priority applications and ensure use of resources is for the sole use of La Sentinelle Ltd business.

f) Computer network users are permitted to use only those network (IP) addresses issued by the IT Department of La Sentinelle Ltd. Selecting an IP address at random to configure a computer network device is prohibited; specific static addresses may be requested from IT Department of La Sentinelle Ltd. The use of private IP addressing behind firewalls and proxy servers, as well as the use of network address translation (NAT) is prohibited without authorization from Head of IT Department.

g) Non-IT Staff or Contractors are not allowed to:

1. Extend or re-transmit network services by installing a router, switch, hub, or wireless access point to La Sentinelle Ltd network;
2. Install network hardware or software that provides network services;
3. Alter network hardware in any way;
4. Download, install, or run security programs or utilities that reveal weaknesses in the security of a system;

5. Run password cracking programs, packet sniffers, network mapping tools, or port scanners;

6.2 User Authentication for External Connections

Access by remote users is strictly controlled and secured by appropriate authentication methods.

a) Control is enforced via password authentication or public/private keys with strong passwords. For information on creating a strong password, see the ***Password Policy.***

b) Users are not allowed to provide or share their login or password to anyone including family members.

c) Users with remote access privileges must ensure that their computer or workstation, which is remotely connected to La Sentinelle Ltd Group's corporate network, is not connected to any other network at the same time.

d) All hosts that are connected to La Sentinelle Ltd internal networks via remote access technologies must use up-to-date anti-virus software. Third party connections must comply with requirements as stated in the ***Third Party Policy.***

6.3 Equipment Identification in Networks

Equipment identification is a means to authenticate connections from specific locations and equipment. An identifier attached to the equipment is used to indicate whether this equipment is permitted to connect to the network. An equipment naming convention is used for equipment identification.

6.4 Remote Diagnostic and Configuration Port Protection

Physical and logical access to diagnostic and configuration ports of all IT equipment is controlled and defined by the ***Physical Access Policy*** and ***Logical Access Policy*** respectively.

Whenever there is a need for remote access by Third Parties, a management approval and authorisation process is followed as per ***Third Party Policy***. Reason for remote access as well as expected duration should be specified. An administrator should monitor the remote access and keep a record of all applicable logs for traceability.

6.5 Segregation in Networks

While segregating the organization’s networks, the network team of La Sentinelle LTD makes sure that:

1. Departments or the different business units of the La Sentinelle Ltd Group are separated from each other, such that if one network is compromised, it will be much harder for the attack to be extended to other groups of networks within the company and it also prevents access to the other departments or business units.
2. Each group/department/ business unit is separated into logical broadcast domains, each protected by a defined security perimeter.
3. A RADIUS server is used to establish authentication schemes and secure transmission tunnels for the communications from outside La Sentinelle Ltd networks (LAN/WAN) where applicable.
4. There are secure gateways (VLANs/routers/firewalls) configured with the appropriate access control rules between logical domains.
5. VLANs are implemented with access control rules to segregate networks in a switched network environment
6. Wireless networks are logically segregated from internal networks such that an unauthorized user cannot access La Sentinelle Ltd’s internal network and have limited access to requested service only.
7. Internal Servers are grouped in a separate DMZ (through a firewall). All traffics going in and out are inspected and filtered.
8. Additionally where software/application development is concerned, development and test environments domains are separated.
9. Network monitoring traffic and network administration traffic are logically segregated from other network traffic.

6.6 Network Connection and Routing Control

The network access rights of users are maintained and updated as required by the ***Logical Access Policy.*** The connection capability of users are restricted through network equipment that filter traffic by means of pre-defined rules as follows:

a) The Internet and Intranet Firewalls are configured such that they restrict access to business applications hosted in the core network from outside its boundaries.

b) Access control lists are configured on routers and switches to control incoming and outgoing traffic across the boundaries of the core network as per the Logical Access Control Policy.

c) All connections to the network by Third Parties are restricted according to the specific requirements of the third parties as per the ***Third Party Policy .***

d) It is ensured that connections to the network by Third Parties are controlled and restricted using Access Control List and Network Address Translation where source and destination are specified.

Routing controls are based on positive source and destination address checking mechanisms. Security gateways are used to validate source and destination addresses at internal and external network control points.

7.0 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 and may be held in breach of contract, and as such, may be subject to grievances or penalties allowed by such contract.

8.0 Network Access Policy Agreement

I have read and I understand the Network 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 : ____