Password Policy

Version 5.0

7th June 2021

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
18.01.21	4.0	Add Windows Security Baselines	Areff Salauroo
07.06.21	5.0	Modify Windows Security Baselines	Areff Salauroo

Table of Contents

PASSWORD POLICY

1.0 Objective

The objective of this policy is to set a standard for creating, protecting, and changing passwords in order to ensure that they are strong, secure, and protected.

2.0 Scope

This policy applies to all employees of La Sentinelle Ltd who have or are responsible for a computer account, or any form of access that supports or requires a password, on any system that resides at any La Sentinelle Ltd facility, has access to La Sentinelle Ltd network infrastructure, or stores any non-public La Sentinelle Ltd information and/or data.

3.0 References ISO 27001:2013

- **Management of Secret Authentication Information of Users – A.9.2.4**
  The allocation of secret authentication information shall be controlled through a formal management process.

- **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.

- **Secure Log-on Procedures – A.9.4.2**
  Where required by the access control policy, access to systems and applications shall be controlled by secure log-on procedures.

- **User Access Provisioning – A.9.2.2**
  A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.

- **Password Management System – A.9.4.3**
  Password management systems shall be interactive and shall ensure quality passwords.

Rue des Oursins, 21731, Baie du Tombeau I T : +(230) 206 8200 I F : +(230) 247 1010 I E : corporate@lasentinelle.mu

4.0 Policy Description

Passwords are a critical component of information and network security. Passwords serve to protect user accounts. However, a poorly chosen password, if compromised, could put the entire network and information systems at risk. As a result, all employees of La Sentinelle Ltd are required to take appropriate steps to ensure that they create strong, secure passwords and keep them safeguarded at all times.

4.1 Management of Secret Authentication Information of Users

The allocation of passwords is controlled through a formal management process.

- Users who are granted logical access, through User Registration are required to sign this Password Policy to accept compliance to this policy and to accept that they will keep personal passwords confidential and group passwords solely within the members of the group.
- When users are required to maintain their own passwords, they are initially provided with a secure temporary password, which they are forced to change immediately on first log-on.
- When users are issued temporary passwords after they forget their passwords, controls are implemented to ensure authentication of the user prior to issue of password.
- Temporary passwords are communicated to users in a secure manner, the receipt of which they acknowledge. Passwords are not sent in e-mails or unprotected (clear text).
- Temporary passwords are unique to an individual and are not guessable.
- Passwords are not stored on computer systems in an unprotected form.
- Default vendor passwords are altered following installation of systems or software.

4.2 Use of Secret Authentication Information

Users are required to follow good security practices in the selection and use of passwords. Users are advised to: -

- Keep passwords confidential. No employee is to give, tell, or hint their password to another person, including IT staff, administrators, superiors, other co-workers, friends, and family members, under any circumstances.
- Avoid keeping a record of passwords in any media – hardcopy or softcopy, unless this can be stored securely in accordance with an approved storage method – a-controlled access safe in hardcopy form or in an encrypted file if in electronic form.
- Change passwords whenever there is an indication of possible system or password compromise.
- Select quality passwords which: -
    1. Are easy to remember for the user
    2. Have a minimum length of eight characters
    3. Not based on anything somebody else can easily guess or obtain using person related information, e.g. names of family members, date of birth, default user identity, phone numbers, address
    4. Are not vulnerable to dictionary attacks, i.e. words which do not exist in dictionaries
    5. Free of consecutive identical, all numeric or all alphabetic characters
    6. Contain at least a combination of alphabets (Upper and Lower case), numbers and special characters
    - 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.

The IT Department may attempt to crack or guess users' passwords as part of its ongoing security vulnerability auditing process. If a password is cracked or guessed during one of these audits, the user will be required to change his or her password immediately.

One technique for creating strong passwords is to use pass phrases, selecting the first character of each word in the phrase, mixed with some numbers and

special characters, e.g. a pass phrase such as 'Sunday is my favourite day of the week' and a password '7SimF!Dotw%'.

4.3 Secure Log-on Procedures

Access to operating systems, are controlled by a secure log-on procedure in order to disclose minimum information about the system and to avoid giving any unauthorised user any assistance. Systems are configured according to the following guidelines: -

- System or application identifiers are not displayed until the log-on process has been successfully completed.
- A general notice warning that computer must only be accessed by an authorised user is displayed.
- No help messages are provided during log-on procedure that could assist an unauthorised user.
- Log-on information is validated only after completion of all input data. No indication is given on specific incorrect data.
- On critical systems, the number of unsuccessful log-on attempts, have been restricted to three attempts, except for systems which does not have this feature, following which the user profile is disabled.
- Passwords are not displayed on the screen when they are input.
- Passwords are not transmitted in clear text over the network.

4.4 User Access Provisioning

Users are issued a unique identifier or user ID for their personal and sole use so that activities on the network or systems can be traced back to the user. Regular user activities are not performed from privileged accounts, e.g. Administrator. The use of a shared user ID for a group of users or a specific job is used only in exceptional cases, where the need to the business is beneficial and justified.

4.5 Password Management System

A password management system is implemented in order to ensure quality passwords. The following controls apply: -

- Individual User IDs and passwords are allocated to users in order to maintain accountability.
- Temporary passwords are issued in a secure manner and users are required to change the temporary password, at the first log-on.
- Choice of quality passwords is enforced, as per section 4.2 of this policy.

- Passwords changes are enforced.
- Users are allowed to select and change their own passwords, as per guidelines in section 4.2 of this policy.
- Passwords are not displayed on the screen when being input.
- Passwords are stored and transmitted in encrypted or secured form.
- In critical systems, password expiry has been implemented.
- Blank passwords are not allowed.
- Inactive sessions are shut down after a defined period of inactivity. Sessions are disconnected from the application and network, necessitating a new log-on for re-connection.

4.6 Active Directory (AD)

Windows Security Baselines recommendations have been used to configure 'Store passwords using reversible encryption', 'Reset Account lockout counter after' and 'Account lockout duration'.

Auditors' recommendations have been used to configure 'Enforce password history'.

The password has been set to never expires as it impacts on our business production if the number of days is set between 1 and 999. It is an added complexity for staffs working on production floor and hence, as result was slowing down the production.

- 'Account lockout duration' value has been set to 15 minutes
- 'Reset Account lockout counter after' value has been set to 15
- 'Account lockout threshold' value has been set to 3
- 'Enforce password history' value has been set to 4
- 'Maximum password age' value has been set to 90
- 'Store passwords using reversible encryption' value has been set to Disabled

5.0 Enforcement to Password Policy

Any employee found to have violated this policy may be subject to disciplinary action that may lead to termination of employment. A violation of this policy by a temporary worker, contractor or vendor may result in the termination of their contract or assignment with La Sentinelle Ltd.

6.0 Password User Agreement

I have read and I understand the Password Policy and its related contents. I understand that I must comply to 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 : _____