Password Management Policy

Document Name :	Password Management Policy
Version :	1.0
Version Date :	10/06/2022
Modified By :	Marc MARTINEZ
Creation Date :	27/05/2022
Created by :	Marc MARTINEZ
Approved by :	Marc MARTINEZ
Confidentiality Level :	INTERNAL

Modification History

	Date	Author	Commentary
1.0	10/06/2022	Marc MARTINEZ	Creation of the document

Introduction

This document aim to provide a robust Password Management Policy to ensure the security of the systems and of the tools used to develop said systems.

Content

The following instriuctions are to be followed by the developpement team.

The password we were handed were either extremely shorts or rather easy to social engineer.
Most of them did not actually work enither.

The passwords we managed to get by either brute forcing the services or doing "social engineering" were default passwords in the most case.

To secure the system we consider we should use a strict password reglement.

The passwords on this project needs to be :

- 14 characters longs at least

- Use alphabetic letters, numbers and symbols

- Users should refrain from using words from a dictionnary

- Users should use randomly generated passwords

Passwords must be changed every 3 months, at most.

This password policy also need to be implemented in the logins screens for the clients, meaning they have to be asked to choose a password that is compliant to this policy.

Required Budget

- Half a day (0.5) of man-hour (400€) per semester or major avancement to make sure that the Developpement Team follow these instructions.