[organization logo]

[organization name]

**PASSWORD Standard FOR WINDOWS SYSTEMS**

|  |  |
| --- | --- |
| Code: | POLICY-GELDCORP-EN-PASSWORD |
| Version: | 1 |
| Date of version: | 03/28/2020 |
| Created by: | Emily Williams, Security Advisor | GeldCorp LLC |
| Approved by: |  |
| Confidentiality level: | INTERNAL USE ONLY |

**Change history**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Created by** | **Description of change** |
| 03/28/2020 | 1.0 | Emily Williams | Initial Draft of Policy |
| 03/29/2020 | 1.1 | John Business | Approved Policy |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Table of contents**

[1. Purpose, scope and users 3](#_Toc270000142)

[2. Reference documents 3](#_Toc270000143)

[3. User obligations 3](#_Toc270000144)

[4. User password management 4](#_Toc270000145)

[5. Validity and document management 4](#_Toc270000146)

# Purpose

The purpose of this document is to prescribe to align with our Password Policy

Reference Password Policy Document

# Scope

This document is applied to Any of GeldCorp’s Systems, workplaces, or other company-owned/operated assets.

# Users

Users of this document are anyone who accesses windows systems

# Reference documents

* ISO/IEC 27001 standard, clauses A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.3
* Information Security Policy
* Password Policy Doc

# Password Requirements

* strong passwords must be selected, in the following way:
  + using at least twelve characters
  + using at least one numeric character
  + using at least one uppercase and at least one lowercase alphabetic character
  + using at least one special character
  + a password must not be a dictionary word, dialectal or jargon word from any language, or any of these words written backwards
  + passwords must not be based on personal data (e.g. date of birth, address, name of family member, etc.)
  + the last three passwords must not be re-used
* password must be changed every 3 months
* password must be changed at first log-on to a system
* passwords must not be stored in an automated log-on system (e.g. macro or browser)
* passwords used for private purposes must not be used for business purposes

# User password management

When allocating and using user passwords, the following rules must be followed:

* by signing the Statement of Acceptance of ISMS Documents, users also accept the obligation to keep passwords confidential, as prescribed by this document
* each user may use only his/her own uniquely allocated username
* each user must have the option to choose his/her own password, where applicable
* the temporary password used for first system log-on must be unique and strong, as prescribed above
* temporary passwords must be communicated to the user in a secure manner, and user’s identity must be previously checked
* the password management system must require the user to change the temporary password at first log-on to the system
* the password management system must require the user to select strong passwords
* the password management system must require the users to change their passwords every three months
* if the user requests a new password, the password management system must determine the identity of the user by [specify how]
* the user has to confirm the receipt of the password by [specify how]
* the password must not be visible on the screen during log-on
* if a user enters an incorrect password three consecutive times, the system must block the user account in question
* passwords created by the software or hardware manufacturer must be changed during initial installation
* files containing passwords must be stored separately from the application's system data

# Validity and document management

This document is valid as of [approval date].

The owner of this document is [Job Title of whoever approves], who must check and, if necessary, update the document at least once a year.

When evaluating the effectiveness and adequacy of this document, the following criteria must be considered:

* number of incidents related to misuse of passwords by unauthorized persons
* number of incidents related to inadequate handling of passwords

[Approver’s job title]

[Approver’s name]

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

[Approver’s Signature]