Password Policy

1. Objective

The objective of this Password Policy is to define the rules governing the creation, use, management, protection, and lifecycle of passwords and other authentication secrets used to access **Arido Software** (hereafter referred to as “the Organization”) information systems, applications, services, and infrastructure. This policy is intended to support secure authentication practices, reduce the risk of unauthorized access, and protect the confidentiality, integrity, and availability of organizational information.

2. Scope

This policy applies to all employees, contractors, consultants, temporary personnel, and third parties who are authorized to access the organization’s information assets. It applies to all passwords and password-based access mechanisms used for workstations, laptops, servers, applications, databases, network devices, cloud services, collaboration platforms, administrative consoles, and any other systems owned by, managed by, or used on behalf of the organization.

3. Definitions

- **Password**: secret string of characters used to authenticate a user or account.
- **Passphrase**: longer password composed of multiple words or elements intended to improve security and memorability.
- **Authentication information**: any secret or controlled information used to verify identity, including passwords, PINs, tokens, cryptographic keys, or equivalent credentials.
- **Privileged account**: account with elevated permissions capable of changing configurations, administering systems, bypassing normal controls, or accessing restricted functions or data.
- **Multi-factor authentication (MFA)**: authentication method that requires two or more independent factors, such as something the user knows, something the user has, or something the user is.
- **Special characters**: non-alphanumeric symbols used for punctuation, formatting, or technical purposes, such as !, @, #, $, %, &, *.

4. Roles and Responsibilities

All users are responsible for protecting their passwords and any other authentication information assigned to them. Users shall comply with this policy, maintain the confidentiality of their credentials, and report any suspected compromise immediately.

IT Managers are responsible for implementing and maintaining the technical controls necessary to enforce this policy. This includes configuring password parameters in systems under their control, ensuring secure password reset processes, protecting password storage and transmission, managing privileged account controls, and reviewing exceptions where technically justified and formally approved.

Management is responsible for approving this policy, ensuring that adequate resources are available for its implementation, and supporting compliance through governance, oversight, and disciplinary action where necessary. Management shall also ensure that this policy is communicated to relevant personnel and remains aligned with business and security requirements.

5. Password Creation Rules

Passwords shall be strong, difficult to guess, and appropriate for the sensitivity of the system or information being protected.

Any password must contain

- At least 8 characters.
- Should satisfy three (3) out of the four (4) of the following:
    - Lowercase characters.
    - Uppercase characters.
    - Numbers (0-9).
    - Special characters

In addition, the following guidelines should be followed when manipulating a password:

- Passwords shall not be based on easily obtainable personal information such as names, birthdays, telephone numbers, usernames, company names, or predictable keyboard patterns.
- Common passwords and previously compromised password combinations shall not be used.

- Default passwords supplied by vendors, installers, or administrators shall be changed immediately before the system is placed into operational use.
- Temporary passwords issued during onboarding, reset, or recovery processes shall be unique, non-guessable, and changed upon first use.

6. Password Usage Rules

Passwords are personal secret authentication information and shall be kept confidential at all times. Users shall not share passwords with any other person, including colleagues, supervisors, IT personnel, external providers, or family members. Passwords shall not be written down in unsecured locations, stored in plain text, or embedded in unprotected files, emails, scripts, or documents.

The same password shall not be reused across distinct systems, applications, services, or external sites. Work-related passwords shall not be reused for personal services, and personal passwords shall not be used for organizational systems. Users shall use only the accounts assigned or authorized for them and shall not attempt to access systems by using another person’s credentials.

7. Password Management and Lifecycle

The organization adopts a risk-based approach to password rotation. Standard user passwords shall not be rotated periodically by default solely because time has elapsed. Password changes shall be required in any of these cases:

- There is evidence or suspicion of compromise
- After a security incident when a password has been exposed
- When an account has been misused
- When a shared or emergency credential has been disclosed beyond authorized personnel

When an employee changes role or leaves the organization, access rights shall be reviewed and accounts shall be modified, disabled, or removed in a timely manner. Where a departing user knows shared, service, emergency, or other non-personal credentials that remain active, those credentials shall be changed without undue delay.

8. Transmission and Storage of Authentication Information

Passwords and other authentication information shall never be transmitted in clear text over unsecured channels. Email, chat, tickets, documents, and scripts shall not be used to distribute

passwords. Temporary passwords shall be communicated through protected channels and, where possible, separately from usernames or activation instructions.

Passwords shall not be stored in plain text. Systems and applications shall store passwords only in protected form using approved hashing or cryptographic techniques appropriate to the technology in use. Password entry fields shall be masked so that characters are not displayed openly during entry. Administrative personnel shall not retrieve, view, or disclose user passwords; instead, reset mechanisms shall be used.

9. Privileged Accounts

Multi-factor authentication shall be enforced for privileged access wherever technically feasible. Privileged accounts shall be used only for administrative activities and not for routine day-to-day tasks such as email or general web browsing. Emergency or break-glass credentials shall be tightly controlled, logged, and changed immediately after use.

10. Security Incidents Related to Passwords

Any user who suspects that a password has been disclosed, guessed, stolen, intercepted, reused without authorization, or otherwise compromised shall report the matter immediately through the designated security or IT channel. The affected password shall be changed without delay, and the associated account shall be reviewed for suspicious activity.

IT Managers shall ensure that password-related incidents are assessed and handled in accordance with the organization’s incident management process.

11. Compliance and Violations

Compliance with this policy is mandatory for all personnel and relevant third parties within scope. Violations of this policy may result in disciplinary action, restriction or removal of access rights, contractual action, and any other measures deemed appropriate under applicable employment terms, contractual conditions, and internal disciplinary processes.