| | | | |
|---|---|---|---|
| **Policy Domain** | **Password Policy** | **Creation Date** | 10th Feb 2021 |
| | | **Classification** | Internal |
| | | **Version** | 1.0 |
| | | **Doc. Owner** | IT Head |

| **Document Control** | | | |
|---|---|---|---|
| **Prepared By**<br>**Vineet Kumar Chawla**<br>**(Sr. Consultant IT)** | **Reviewed By**<br>**Maruti Divekar**<br>**(IT Head)** | **Checked By**<br>**B P Rauka**<br>**(CFO)** | **Approved By**<br>**Mukund Kabra**<br>**(Director)** |
| | | | |

**Document Modification History**

| SR # | Document | Version No. | Reviewed On | Checked On | Approved On | Effective Date | Authorized Signatory |
|---|---|---|---|---|---|---|---|
| 1. | Password Policy | 1.0 | 05TH Mar 21 | 10th Mar 21 | 10th Mar 21 | 11th Mar 21 | |
| 2. | | | | | | | |
| 3. | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

## Document Control

- This document is subject to version control and shall be managed by IT Head. Any request for amending this document shall be approved by Director. The IT Head shall review this document at least once in a year and/or when there is a significant change in technology adopted, business objectives, identified threats, legal environment, social climate and business processes.

- The document is available on Helpdesk Portal under Announcement and Server shared folder under AETL Policies and provided with HR Joining Kit, in non-editable pdf format and all the employees are expected to read and adhere to it. The approved and signed copies are available with IT Team, which can be used for audit purpose only. IT Team is responsible for maintaining updated copy of this document and its effective communication within Advanced Enzymes (AETL).

| | | | |
|---|---|---|---|
| **Policy Domain** | **Password Policy** | **Creation Date** | 10th Feb 2021 |
| | | **Classification** | Internal |
| | | **Version** | 1.0 |
| | | **Doc. Owner** | IT Head |

## Table of Contents

| | | | |
|---|---|---|---|
| **Policy Domain** | **Password Policy** | **Creation Date** | 10th Feb 2021 |
| | | **Classification** | Internal |
| | | **Version** | 1.0 |
| | | **Doc. Owner** | IT Head |

## 1. Overview

Passwords are an important aspect of computer and mobile device security. They are the first line of defense for user accounts. A poorly chosen password may result in a compromise of AETL Confidential Information subjected to hijack of network, leakage of customer information, confidential data which can result in a huge business and reputational loss of the organization.

## 2. Purpose

The purpose of this policy is to establish a standard for the creation of strong passwords, the protection of those passwords, and the frequency of change.

## 3. Scope

The scope of this policy includes all AETL employee who are assigned with user account and password are solely responsible and accountable for maintaining of confidentiality of this credentials.

## 4. Password Management

### 4.1 Domain User Password Policy

The Administrators user password should be changed and vaulted with Head of IT. Named users accounts having admin access rights are created for system administration and standard users are created to end users for their routine work.

- **Minimum Length** – 9 characters
- **Maximum Length** – Default (127 characters)
- **Complexity** - No dictionary words included. Passwords should use three of four of the following four types of characters:
  - Lowercase
  - Uppercase
  - Numbers
  - Special characters such as!@#$ %^&*(){} []
- **Password history** – 5 unique passwords before an old password may be reused
- **Maximum password age** – 90 days
- **Minimum password age** – 1 day
- **Account lockout threshold** – 5 failed login attempts
- Users are required to change their password on first login on domain.
- **Reset account lockout after** - The time it takes between bad login attempts before the count of bad login attempts is cleared. The recommended value is 15 minutes. This means if there are bad attempts in 15 minutes, the account would be locked.
- **Account lockout duration** - The administrator reset the account lockout so they are aware of possible break in attempts on the network.

- System should not be left unattended with the user logged on and no password protected screen saver active. Users should be in the habit of not leaving their computers unlocked. They can press the CTRL-ALT-DEL keys and select "Lock Computer" or Simply press Windows + L key to lock the computer.

### 4.2 SAP User Password Policy

The super admin user's password should be changed and vaulted with Head of IT. Named users accounts having basis admin access rights are created to manage the application and database support.

- **Minimum Length** – 9 characters recommended
- **Maximum Length** – Default
- **Password Complexity** – No dictionary words included. Passwords should use three of four of the following four types of characters:
  - ➢ Lowercase
  - ➢ Uppercase
  - ➢ Numbers
  - ➢ Special characters such as!@#$ %^&*(){} []
- Passwords are case sensitive, and the user name or login ID is not case sensitive.
- **Password history** - 5 unique passwords before an old password may be reused.
- **Maximum password age** – 90 days
- **Minimum password age** - 1 days
- **Account lockout threshold** - 5 failed login attempts
- Users are required to change their password on first login on domain.

### 4.3 E-mail User Password Policy

- **Minimum Length** – 9 characters
- **Maximum Length** – Default
- **Password Complexity** - No dictionary words included. Passwords should use three of four of the following four types of characters:
  - ➢ Lowercase
  - ➢ Uppercase
  - ➢ Numbers
  - ➢ Special characters such as!@#$ %^&*(){} []
- **Password history** – 5 unique passwords before an old password may be reused
- **Maximum password age** – 90 days
- **Minimum password age** – 1 day
- **Account lockout threshold** – 5 failed login attempts.
- Users are required to change their password on first login on domain.

### 4.4 IT Infrastructure Servers – Windows (Other than SAP Infra) Password Policy

The ADMIN user's password should be changed and vaulted with Head of IT. Named users accounts having Admin access rights are created to manage the physical servers and virtual servers.

- **Minimum Length** - 9 characters
- **Maximum Length** – Default (127 characters)
- **Minimum complexity** - No dictionary words included. Passwords should use three of the following four types of characters:
  - Lowercase
  - Uppercase
  - Numbers
  - Special characters such as!@#$ %^&*(){}[]
- Passwords are case sensitive, and the user name or login ID is not case sensitive.
- **Password history** - 5 unique passwords before an old password may be reused.
- **Maximum password age** – 90 days
- **Minimum password age** - 1 days
- **Account lockout threshold** - 5 failed login attempts
- Users are required to change their password on first login on domain.
- **Reset account lockout after** - The time it takes between bad login attempts before the count of bad login attempts is cleared. The recommended value is 15 minutes. This means if there are bad attempts in 15 minutes, the account would be locked.
- **Account lockout duration** - The administrator reset the account lockout so they are aware of possible break in attempts on the network.
- Servers should not be left unattended with the user logged on and no password protected screen saver active. Users should be in the habit of not leaving their computers unlocked. They can press the CTRL-ALT-DEL keys and select "Lock Computer".

### 4.5 IT Infrastructure Servers – SAP Infra (Linux/Windows/Database Severs) Password Policy

The ADMIN user's password should be changed and vaulted with Head of IT. Named users accounts having Admin access rights are created to manage the physical servers and virtual servers.

- **Minimum Length** - 9 characters
- **Maximum Length** – Default (127 characters)
- **Minimum complexity** - No dictionary words included. Passwords should use three of the following four types of characters:
  - Lowercase
  - Uppercase
  - Numbers
  - Special characters such as!@#$ %^&*(){}[]
- Passwords are case sensitive, and the user name or login ID is not case sensitive.
- **Password history** - 5 unique passwords before an old password may be reused.
- **Maximum password age** – 180 days
- **Minimum password age** - 1 days
- **Account lockout threshold** - 5 failed login attempts
- Users are required to change their password on first login on domain.

- **Reset account lockout after** - The time it takes between bad login attempts before the count of bad login attempts is cleared. The recommended value is 15 minutes. This means if there are bad attempts in 15 minutes, the account would be locked.
- **Account lockout duration** - The administrator reset the account lockout so they are aware of possible break in attempts on the network.
- Servers should not be left unattended with the user logged on and no password protected screen saver active. Users should be in the habit of not leaving their computers unlocked. They can press the CTRL-ALT-DEL keys and select "Lock Computer".

### 4.6 IT Infrastructure – Network

The SYSTEM/ ADMIN user’s password should be changed and vaulted with Head of IT. Named users accounts having admin access rights are created to manage the Network Devices.

- **Minimum Length** – 9 characters recommended
- **Maximum Length** – Default (set by OEM)
- **Minimum complexity** – No dictionary words included. Passwords should use three of four of the following four types of characters:
  - ➢ Lowercase
  - ➢ Uppercase
  - ➢ Numbers
  - ➢ Special characters such as!@#$ %^&*(){} [] are included
- Passwords are case sensitive, and the user name or login ID is not case sensitive.
- **Maximum password age** – 90 days
- **Minimum password age** – 1 (wherever possible)
- **Account lockout threshold** – 5 failed login attempts
- **Account lockout duration** – 30 minutes. The administrator reset the account lockout so they are aware of possible break in attempts on the network.

### 4.7 Generic User Password Guidelines

Password requirements should ensure making the password too difficult may actually decrease security if users decide the rules are impossible or too difficult to meet. If passwords are changed too often, users may tend to write them down or make their password a variant of an old password which an attacker with the old password could guess. The following password requirements have been set by the IT department unless not defined explicitly:

- **Minimum Length** – 9 characters recommended.
- **Maximum Length** – Default (127 characters)
- **Password Complexity** – No dictionary words included. Passwords should use three of four of the following types of characters:
  - ➢ Lowercase
  - ➢ Uppercase
  - ➢ Numbers
  - ➢ Special characters such as!@#$ %^&*(){} []

- Passwords are case sensitive and the user name or login ID is not case sensitive.
- **Password history** – 5 unique passwords before an old password may not be reused.
- **Maximum password age** – 90 days
- **Minimum password age** – 1 days
- **Account lockout threshold** – 5 failed login attempts
- **Account lockout duration** – The administrator reset the account lockout so they are aware of possible break in attempts on the network. The account will be unlocked after 30 minutes.
- System should not be left unattended with the user logged on and no password protected screen saver active. Users should be in the habit of not leaving their computers unlocked. They can press the CTRL-ALT-DEL keys and select "Lock Computer" or Simply press Windows + L key to lock the computer.

**Guidelines for secure use of password are enumerated below for ready reference.**

- Never write passwords down;
- Never send a password through email to others, except for initial communication by IT Service Desk;
- Never include a password in a non-encrypted stored document;
- Never tell anyone your password;
- Never reveal your password over the telephone;
- Never hint at the format of your password;
- Never reveal or hint at your password on a form on the internet;
- Never use the "Remember Password" feature of application programs such as Internet Explorer, your email program, or any other program;
- Never use your corporate or network password on an account over the internet which does not have a secure login where the web browser address starts with https:// rather than http://
- Report any suspicion of your password being broken to your IT dept.
- If anyone asks for your password, refer them to your IT Dept.
- Don't use common acronyms as part of your password
- Don't use common words or reverse spelling of words in part of your password
- Don't use names of people or places as part of your password
- Don't use part of your login name in your password
- Don't use parts of numbers easily remembered such as phone numbers, social security numbers, or street addresses
- Be careful about letting someone see you type your password.

## 5. Enforcement

Since password security is critical to the security of the organization and everyone, employees that do not adhere to this policy may be subject to disciplinary action up to and including dismissal.

## 6. Policy Review

The policy will be reviewed on yearly basis or if there is any major change in IT infrastructure to incorporate changes if any.

IT Head will be responsible for reviewing the policy and communicating the changes made therein.

## 7. Roles & Responsibility Matrix (RACI)

| Role<br>Activity | IT Head | ISMS Steering Committee | Internal Users | External Users | Exempted |
|---|---|---|---|---|---|
| Authoring of this document | RA | RA | - | - | - |
| Approval of this document | I | CI | - | - | - |
| Sign-off of this document | CI | CI | - | - | - |
| Application of this document | RA | RA | RA | RA | - |
| | | | | | |

| | |
|---|---|
| R | Responsible |
| A | Accountable |
| C | Consulted |
| I | Informed |

## 8. Roles and Responsibilities

Roles and their specific responsibilities for the defined policy are as under:

- **IT Head**
  - Shall assist in risk assessment and identify security controls,
  - Shall perform document review and version control.

- **Network, Applications, Server IT Administrators**
  - Shall be responsible for maintaining adequate security of passwords.
  - Shall reset, disable, lock passwords.

- **User**
  - Shall use passwords judiciously.
  - Always ensure security of username and passwords.

## 9. Risk for Non-Compliance

Risks arising due to non-compliance with this policy include, but not limited to:

- Unauthorized data access.
- Fraudulent transactions in SAP.
- Change of Network and systems settings.
- Misuse of Servers & other IT Infrastructure.

## 10. ISMS Steering Committee Members

1. Mukund Kabra (Director)
2. B. P. Rauka (CFO)
3. Maruti Divekar (IT Head)

## 11. AETL IT Helpdesk Contact Details

- Logging an online support request: **http://192.168.2.7:8080**
- Email: **it.helpdesk@advancedenzymes.com**
- Telephone: **022 41703234**