**Password Policy**

# Introduction

Passwords are a way of identifying a user based on the credential provided. They form a common means of validating a user’s identity to access an information system or service. Improper management and use of passwords can result in security breach.

# Scope

Betala Stock Broking Limited needs to ensure that passwords are managed effectively and are not misused by users. This policy addresses the effective password management. It applies to all staff present at Betala Stock Broking Limited and using their facilities.

# Responsibilities

|  |  |
| --- | --- |
| **Designation** | **Role** |
| Information Security Manager | Ensuring that this policy is implemented effectively. |
| Information Security Officer | Enforcing the policy. |
| System Administrator | Applying password settings as per the policy. |
| Network Administrator | Applying password settings for network devices. |
| Manager-HR | Ensure that all users and staff at Betala Stock Broking Limited are aware of this policy. |
| All Users | Should be aware of the policy and follow the password guidelines. |

# Policy

## One time passwords

The system administrator gives a temporary password or initial password when creating a new user account. Users must change their passwords after first successful login attempt. Where possible, systems must be configured to force a user to change their initial passwords when they log on for the first time.

## Password settings

#### Password Length and Composition

Passwords used should be at least 8 characters in length. The combination of characters used should be a mix of alphabets, numbers and special characters. Users should not choose passwords which can be easily guessed, like names or part of names, dictionary words, phone numbers, dates or common words.

#### Password History

Password history should be set to 5. This will prevent the re-use of the last 5 passwords.

#### Password Age

Password age must be set to 30/45 days. A reminder must be given to the user, 7 days prior to the expiry of the passwords. Failure to change the passwords before expiry will result in the account getting locked / disabled.

#### Account Lockout

Where possible, systems must be configured to lock the user’s account if there have been more than 3 invalid login attempts. For the reactivation of locked user accounts, the user should report to helpdesk and provide his/her date of birth and Betala Stock Broking Limited employee code. Or the user can appear in person and show the ID card to helpdesk.

## Password Management

### Administrator Passwords

* All system passwords must be kept in a sealed envelope and under the custody of the Information Security Officer.
* For users requiring administrative privileges for carrying their job functions; necessary privileges must be granted to their user-id after getting due approval from heads and ISO
* If, for any reason the sealed envelope is to be opened to access the password, the Information Security Officer must authorize the same. A log to that effect must be made in the sealed envelope. After the required task is complete, the system / network administrator must change the password and hand over the same in a sealed envelope to the Information Security Officer. This must also be logged in the **Error! Reference source not found.**.

### Password reset

If in case users forgot their passwords they can call the IT helpdesk to reset their passwords, who in turn will provide a temporary password which must to be changed by the user after first you. The user should provide his/her date of birth and Betala Stock Broking Limited employee code to helpdesk or the user can appear in person to helpdesk and show the ID card to helpdesk.

### Default Passwords

The operating system, application and database vendors provide default user-ids and passwords. Where feasible, the system administrator must disable all such default user-ids and change the default password that is set by the manufacturer of the product.

## Passwords of Network Devices

Passwords of network devices such as firewalls and routers should be changed as per point 4.2 of this policy document. The password for these devices should be with the Network Administrators. These passwords must also be placed in a sealed envelope and handed over to the Information Security Officer. When-ever the sealed envelope is opened and a new envelope given, an entry must be made in the **Error! Reference source not found.**.

## Automated Log-on

Use of passwords in automated logon processes should be avoided. Passwords should not be included in automated logon processes; batch processes or hard coded in applications unless there is a business need for the same. For such inclusions, authorization of the Information Security Officer should be taken.