Information Security
User Password Policy

|  |  |  |  |
| --- | --- | --- | --- |
| Policy ID |  | **Effective Date** | Date |
| Version | 1.0 | **Contact** |  |
| Scope | All Employees |  |  |

**Table of Contents**

1.0 Overview 1

2.0 Purpose 1

3.0 Scope 1

4.0 Composition & Distribution 1

5.0 Resets & Lockouts 2

6.0 UserID and Password Protection 2

7.0 Compromised Passwords 2

8.0 Related Policies 3

9.0 Policy Maintenance 3

# 1.0 Overview

Passwords are an important aspect of information security. A poorly chosen password may result in unauthorized access and/or exploitation of Firm Name resources. All users, including contractors and vendors with access to Firm Name systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

# 2.0 Purpose

This policy defines the requirements for establishing the password configuration settings and managing fixed passwords used on any Firm computer and communications system.

# 3.0 Scope

This policy applies to all Employees, Non-Partner Attorneys, Partner Attorneys, and External-Party Vendors who have or are responsible for an account on any system that resides in Firm Name’s environment, or managed systems in the cloud.

# 4.0 Composition & Distribution

Every user must have a single UserID, password, and two-form authentication for access to the Firm Name network.

1. All user network accounts must have a password that adheres to the following requirements:
	1. Minimum password length of 8 characters.
	2. Must include three of the following four;
		1. Uppercase alphabetic character
		2. Lowercase alphabetic character
		3. Numeric Character
		4. Special Symbol
	3. Cannot use one of the last four recently-used passwords (system will maintain a record of previously used passwords for prevention).
2. Users must not employ any password structure or characteristic that results in a password that is predictable or easily guessed including, but not limited to, derivatives of user IDs, common character sequences, or personal details.
3. Null passwords to network accounts are always prohibited.
4. Initial Passwords issued by a Network Administrator must be set to expire, forcing the user to choose another password before the next logon process is completed.
5. The Technology Service department must never share or reveal an initial password to anyone other than the authorized user.
6. UserIDs and passwords should not be communicated together in any form of electronic/physical communication.
7. A new user will construct their network password during computer orientation.
8. Passwords should not be displayed on the screen when being entered (Ex: \*\*\*\*\*\*\*\*)
9. It is recommended that users should not use the same password for Firm Name accounts as for other non- Firm Name accounts (i.e., personal)
10. Network passwords must be changed every 90 days.
11. Network UserIDs must also be assigned a security token for two-form authentication.
12. The initial two-form authentication PIN will be communicated during computer orientation.
13. A new user will define their two-form PIN during computer orientation.

# 5.0 Resets & Lockouts

1. All Firm systems that employ fixed passwords at log on must be configured to permit only five attempts to enter a correct password, after which the user ID is deactivated and can only be reset by Technology Services.
2. The requesting user must be positively identified before a password reset may be performed.
3. A reset can only be requested by the user needing the reset.
4. Password issued as a result of a requested reset must be a unique value, i.e. a string of characters that is not the same for all password resets.
5. The reset password can only be communicated to the user whose password is reset with an acknowledgement of receipt from user.
6. Once reset, the user should change the password from the reset password.
7. Passwords must not be inserted into email messages.

# 6.0 UserID and Password Protection

1. Passwords must not be written down and left in a place where unauthorized persons might discover them.
2. Passwords must not be shared with anyone. All passwords are to be treated as sensitive, confidential Firm information.
3. No unsupervised access to any Technology Systems under your network credentials to another employee is allowed.
4. Authorized users are responsible for the security of their passwords and accounts, and are responsible for all activities associated with their credentials or any activity originating from their system.
5. All virtual desktops should be logged out every night, and locked when unattended during the day.
6. Users must not provide their user-IDs and/or passwords to data aggregators, data summarization/formatting services, or any other third parties.

# 7.0 Compromised Passwords

In the event the Firm is suspect of compromise to its systems, password changes may be required.

1. Each user must immediately change his or her password if the password is suspected of being disclosed, or known to have been disclosed to an unauthorized party
2. In the event the Firm’s system that manages all network accounts is compromised, all network passwords must be immediately changed.
3. If a privileged user ID (i.e., system admin) has been compromised by an intruder or another type of unauthorized user, all passwords on that system must be immediately changed.
4. After either a suspected or demonstrated intrusion to a Firm Name system, the involved System Administrator must immediately notify the system's user community that an intrusion is believed to have taken place. The status of all passwords on that system must immediately be changed to expired, so that these passwords will be changed at the time that the involved users next log-in.

# 8.0 Related Policies

* Account Management
* Vendor Management

# 9.0 Policy Maintenance

The responsibility of ensuring this policy is kept current as needed for purposes of compliance with the Firm’s security requirements is assigned to the Security Team.

### Revision History

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Description | Revision Date | Review Date | Reviewer/ApproverName |
| 1.0 | Initial Version |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |