CITADEL
SERVICING CORPORATION

PASSWORD SECURITY POLICY

2022

5. PASSWORD SECURITY POLICY

POLICY STATEMENT

All users who have been authorized to access Citadel Servicing Corporation systems, applications and data must establish, maintain, and safeguard their user password(s) according to the password standards established by Citadel Servicing Corporation .
Authorized personnel for each system are the only individuals who may add, remove, or change password requirements for any system or user account.

5.1. OVERVIEW

Passwords are utilized to securely access company systems and provide a front line of protection to those systems and data. All individuals/entities who logically access Citadel Servicing Corporation ’s systems, applications, and data, have a responsibility to safeguard these systems by ensuring their passwords remain within policy guidelines, are kept strictly confidential, and secure.

This policy establishes the standards by which all user passwords will be managed and maintained for all systems. To ensure a high level of identification, access, and authentication security, passwords must adhere to a minimum set of established standards. This policy elaborates on password requirements in alignment with Information Security Policies.

5.2. PURPOSE

The purpose of this policy is to define the authorities and procedures for creating, changing, and safeguarding passwords. This policy is used to govern strong password generation, management, and security as well as educate users on password standards and usage as part of the methodology that verifies the identity and privileges of persons with access to the Citadel Servicing Corporation ’s systems.

5.3. SCOPE

This policy applies to all company computer systems and facilities, including those managed for Citadel Servicing Corporation . This policy applies to all employees, partners, contractors, consultants, other workers and third parties with access to company information assets and facilities.

This policy applies to all accounts and controls within the IT environments that access, operate, and manage Citadel Servicing Corporation IT and business resources.

5.4. OVERSIGHT RESPONSIBILITIES

- Information Security Office Responsibilities — The Information Security Office, consisting of leadership representing IT, Compliance & Risk, HR, and Legal departments, is responsible for establishing and maintaining organization-wide information security policies, standards, guidelines, and procedures.
- Management Responsibility — Management is primarily responsible for decision-making relating to Information Security, including the allocation of sufficient resources. Specialists and advisors play an important supporting role ensuring the proper design, function, and consistent use of established controls.
- Compliance — Compliance ensures that the company and its employees comply with relevant laws and regulations.

5.5. POLICY REQUIREMENTS

A. Complex Passwords — All user-chosen passwords must contain at least three of the four following criteria:

- Contain at least one uppercase letter (A through Z)
- Contain at least one lowercase letter (a through z)
- Contain at least one number (0 through 9)
- Contain at least one non-alphabetic character (e.g., special characters “! @ # $ %”)

B. Null Passwords Always Prohibited — At no time, may any Systems Administrator or Security Administrator enable any user ID that permits password length to be 0 / null / blank password.

C. Password Restrictions and Limitations — The following restrictions and limitations will be imposed on account passwords used on Citadel Servicing Corporation systems and its network:

- Passwords will not contain the user’s account name.
- Users will not be allowed to reuse a password from the last five (5) passwords used.
- Passwords will expire every sixty (90) days for user accounts.
- User accounts will automatically lockout after five (5) consecutive incorrect attempts.

5.5.1. Length

A. Minimum Password Length — All passwords must have a minimum length. The following standard will be used for setting password length:

- All user accounts will be a minimum of eight (8) character passwords with 2 special characters.
- The length must always be checked automatically at the time that users construct or select their password.

5.5.2. Distribution

A. Initial Passwords — Are issued by an Administrator and coded with forced expiration. This requires the user to choose another password before the next logon process is completed.

B. Password Sharing — Passwords must never be shared or revealed to anyone other than the authorized user.

C. Disclosure of Passwords — Security Administrators must disclose passwords to a user providing two pieces of definitive evidence substantiating his or her identity only if a new user ID is being assigned.

Any temporary passwords must be given to users in a secure manner; the use of non-approved third parties or unprotected (clear text) electronic mail messages will be avoided. Temporary passwords must be unique to an individual and not be guessable. Users must acknowledge receipt of password.

5.5.3. Resets

A. Password Resets – Identification — The requesting user must be positively identified by IT Personnel or approved by the Human Resources manager before a password reset may be performed. The user can also perform their own password reset through Citadel Servicing Corporation ’s self-service portal.

B. Password Resets – Unique Value — Passwords 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 previous password resets).

C. **Fixed Password Change Confirmation** — All fixed password resets or changes must be promptly confirmed, so the authorized user can readily detect and report any fraudulent or abusive behavior. The password itself must not be transmitted – only the fact that it was changed.

5.5.4. Compromised Passwords

A. **Password Changes after System Compromise** — If a multi-user computer system employs fixed passwords as its primary access control mechanism, all passwords on that system must be changed immediately after evidence of system compromise has been discovered, and all users must change their fixed passwords on other machines, if the passwords on the compromised machine are also used on these other machines.

B. **Password Changes after Privileged User ID Compromise** — If a privileged user ID has been compromised by an intruder or another type of unauthorized user, all passwords on that system must be immediately changed.

C. **Passwords Set to Expired after Intrusion** — After either a suspected or demonstrated intrusion to an Citadel Servicing Corporation computer 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.

5.5.5. Changes

A. **Required Password Changes** — All users must be automatically required to change their passwords at least once every sixty (60) days.

B. **Password Reset after Lockout** — All users must limit the number of attempts to enter the correct login credentials or password to a maximum of five (5) attempts, after which the user ID will be temporarily disabled and can only be reset by the Help Desk staff after authenticating the user’s identity.

C. **Masking Password Changes** — Whenever user-chosen passwords or encryption keys are specified, they must be entered twice and masked such that the user cannot see what was typed.

D. **Password Security** — The system will ensure password hashes are encrypted in storage and during transmission to prevent the compromise of user passwords.

E. **Password Change Interval Synchronization** — The fixed password change interval must be synchronized across all computer and network platforms at Citadel Servicing Corporation .

F. **User Notification of Changed Password** — Whenever a fixed password is changed, the involved user must be promptly notified of that fact using a communications system other than the one to which the password applies. This notification must be accompanied by instructions to immediately contact the Help Desk if the authorized user did not initiate the change.

5.5.6. Display

A. **Password Display and Printing** — The display and printing of passwords, when end users enter them, must be masked, suppressed, or otherwise obscured so that unauthorized parties will not be able to observe or subsequently recover them.

5.5.7. Default Passwords

For any systems (e.g., routers, firewalls) that are pre-configured with vendor-supplied default passwords, those passwords will be changed to conform and align with the corporate password security policy to ensure compliance and security of the corporate network.

5.6. ENFORCEMENT

All users (employees, contractor, part-time and temporary workers) and those employed by others to perform work for the organization, or who have been granted access to IT assets or facilities, are covered by this policy and must comply with its associated policies, procedures, standards and guidelines.

Failure to comply with this policy and associated guidelines may result in suspension of use privileges or other disciplinary actions up to and including termination and/or legal action.