USER ACCESS AND ACCOUNT MANAGEMENT POLICY

2022

4. USER ACCESS AND ACCOUNT MANAGEMENT POLICY

POLICY STATEMENT

All computer users within the Citadel Servicing Corporation corporate network who access corporate information systems and assets will be subject to guidelines and standards regarding access to corporate information systems in order to secure and protect the information assets of the corporate network.

In order to fully protect the confidentiality, integrity and availability of corporate and client data created, stored and transmitted by Citadel Servicing Corporation , access to Citadel Servicing Corporation system resources is granted to individuals who are approved by Citadel Servicing Corporation management.

It is the policy of Citadel Servicing Corporation that each user of Citadel Servicing Corporation IT resources be assigned a unique identity to securely authenticate to the system that the user has been authorized to access it. This unique identity is part of an overall process of identification and authorization designed to ensure that access is granted only to properly authorized individuals.

4.1. OVERVIEW

Citadel Servicing Corporation employs IT systems to perform and execute its business operations. Access to these systems is formally approved, managed, and reviewed to ensure that data systems and/or contents thereof can only be accessed by authorized individuals. Only individuals that have been identified, authenticated, authorized and approved by the company may be granted access to corporate systems and data.

Citadel Servicing Corporation has information access management policies and procedures in place that grant different levels of access to corporate and/or client data while limiting the minimum necessary rights for a person to perform their duties. The company will take reasonable and appropriate steps to ensure that individuals and/or entity identities are validated and true prior to accessing corporate/client data systems.

4.2. PURPOSE

The purpose of this policy is to prevent unauthorized access and specify the requirements for creation, administration, use, revision and removal of access to Citadel Servicing Corporation IT systems and data through an established set of standards pertaining to minimum requirements, authentication, authorization, and management of accounts and all attributes associated therein.

The company will take reasonable and appropriate steps to ensure that the corporate network is installed with technical safeguards to control and restrict access to corporate/client data systems to persons, entities and software programs that are authorized to have such access in accordance with corporate access policies.

Access will be restricted on a business need-to-know basis with defined control requirements for the secure management of accounts on Citadel Servicing Corporation computer and communications systems.

4.3. SCOPE

The policy applies to all employees, contractors, consultants, temporary employees, and other entities at Citadel Servicing Corporation including all personnel affiliated with third parties.

This policy applies to all company computer systems and facilities, including those managed for company customers and to all accounts and controls within the IT environments that access, operate, and manage company IT and business resources.

4.4. 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.

4.5. POLICY REQUIREMENTS

Accounts within Citadel Servicing Corporation follow established account management procedures to ensure role-based privileges, separation of duties, access validations, auditing capabilities, and that only authorized personnel have access to information. User Access is established based upon levels defined by Management. Information Owners will approve access privileges. Users will be granted the minimum access rights required to perform their daily job duties. Access will be granted on a business need-to-know basis. Users that require either elevated or special access must have additional upper management approval to gain access.

All computer users within the Citadel Servicing Corporation corporate network accessing corporate information systems and assets, whether remote or on-premises, will be subject to the following:

A. Each user will have a uniquely assigned login name and password to access corporate computer systems and resources, issued and managed by an authorized systems administrator in IT Operations. If a system is hosted Software outside of Citadel Servicing Corporation in the Cloud or other non-Citadel Servicing Corporation managed Computer Systems, a network login is required and will be issued and maintained by the IT Operations, in addition to the specific application systems access which may be issued and maintained by an Citadel Servicing Corporation Business Administrator adhering to this Policy.
B. Each person will be responsible for the login name assigned to him/her.
C. A password will not be displayed on the screen in clear text when logging in.
D. A login that is not successful will be logged and the logs will be reviewed at regular intervals.
E. In the case of a permanent or temporary employee or contractor leaving the organization, the Department Manager will be responsible for the notifications are made to the Human Resources Department and validating all the employee's system IDs are revoked prior to final settlement.
F. A login ID not used for thirty (30) days will be disabled following confirmation by the Human Resources Department.
G. Annual auditing conducted by Information Security Office to determine if this policy is being adhered to and to ensure terminated users no longer have access to Citadel Servicing Corporation systems.

4.5.1. Authorization

User ID and Privilege Approval — Should user IDs, business application system privileges, or system privileges involve capabilities that go beyond those routinely granted to general users, must be approved by the responsible Manager and IT.

Access Control Authorization — The majority of positions have roles-based permission access pre-defined. Requests for the addition, deletion, and modification of all User IDs, credentials, and other identifier objects on Citadel Servicing Corporation computer and communications systems must be authorized by the employee's immediate Supervisor or Manager and submitted to IT Operations utilizing the system access Request Form. If a request is outside the normal role-based accesses, the System Owner must approve access in addition (D below).

Information System Privilege Usage — Information system privileges must not be employed for any Citadel Servicing Corporation business purpose until they have been approved as defined in the procedures.

System Access Request Authorization — All requests for additional privileges on Citadel Servicing Corporation **'s** multi-user systems or networks must be authorized by the User's manager and the System Owner.

4.5.2. Authorizing Accounts

A. All employees must be formally designated as requiring access to corporate information systems.

B. All account administration and management operations require a ticket and approvals from the system owner (or designate) prior to implementation.

C. All requests for the addition, deletion, and modification of all User IDs, credentials, and other identifier objects on Citadel Servicing Corporation **'s** computer and communications systems must be submitted and authorized by the employee's immediate supervisor or manager.

D. All requests for additional privileges on company multi-user systems or networks must be submitted on a completed system access request form that is authorized by the user's immediate manager.

E. If an employee requires permissions outside of their access group, it must be justified, approved, and documented by system owners or designated system managers.

F. Whenever user IDs, business application system privileges, or system privileges involve capabilities that go beyond those routinely granted to general users, they must be approved by the user's manager.

G. The level of access must be appropriate to the business purpose and be consistent with corporate security policies.

H. A formal naming standard will be implemented for all accounts (User ID).

I. All authentication methods will be unique and, in the case of password use, known only to the employee or business associate.

J. All user IDs will be tracked and associated with a unique individual for the purpose of appropriate auditing of application and data access.

K. Information system privileges must not be employed for any Citadel Servicing Corporation business purpose until they have been approved by the Information Security Manager/Director.

L. Access to corporate information must always be authorized by a designated Owner of such information, and must be limited on a need-to-know basis to a reasonably restricted number of people.

M. Computer and communication system privileges must be granted only by a clear chain of authority delegation.

N. All users must be positively identified prior to being able to use any multi-user computer or communications system resources.

O. Access to sensitive or valuable company information must be provided only after express management authorization has been obtained.

4.5.3. Account Definition

A. **Non-Anonymous User IDs** — All User IDs on Citadel Servicing Corporation computers and networks must be constructed according to the Citadel Servicing Corporation User ID construction standard and must clearly indicate the responsible individual's name.
B. **Unique User ID and Password Required** — Every user must have a single unique User ID and a personal secret Password for access to Citadel Servicing Corporation computers, data stores, file shares, and computer networks.
C. **Unique User IDs** — Each computer and communication system User ID must uniquely identify only one user. Shared or group User IDs must not be created or used.
D. **Non-Employee User ID Expiration** — Every User ID established for a non-employee must have a specified expiration date, with a default expiration of sixty (60) days when the actual expiration date is unknown.

4.5.4. Account Maintenance

A. **User Status Changes** —The Human Resources Department or the Legal Department notifies the IT Operations/Systems Administration unit regarding required action associated with changes in a user's status with Citadel Servicing Corporation .
B. **Inactive Account Maintenance** — All inactive accounts over thirty (30) days old must be either removed or disabled following consultation with Human Resources.

4.5.5. Access and Privilege Assignment

A. **Read Access Sensitive Information** — Employees who have been authorized to view information classified at a certain sensitivity level must be permitted to access only the information at this level and at less sensitive levels.
B. **Role-Based Access Control Privileges** — The information systems access privileges of all users must be defined based on their officially assigned roles within Citadel Servicing Corporation .
C. **Third Party Software Developers Access to Source Code** — Citadel Servicing Corporation Only the modules as-needed for a specific programming task may be revealed to third-party application developers.
D. **Privilege Restriction: Need to Know** — The computer and communications system privileges of all users, systems, and programs must be restricted based on the need to know and follow the principle of least privilege needed to do one's job function.
E. **Application User ID Restriction** — Every Citadel Servicing Corporation application user ID must be restricted to use only by the application for which it was established.
F. **Number of Privileged User IDs** — The number of privileged user IDs must be strictly limited to those individuals who absolutely must have such privileges for authorized business purposes.
G. **Business Production Information Updates** — System privileges must be defined so that non-production staff are not permitted to update production business information. This includes, but is not limited to, internal auditors, systems administrators, programmers, and computer operators.
H. **Personal Information Access** — All identifying information about customers such as credit card numbers, credit references, and social security numbers, must be accessible only to those Citadel Servicing Corporation personnel who need such access in order to perform their jobs.
I. **Developer Access to Production Business Information** — Where access to production business information is required so that new or modified business application systems may be developed or tested, only "read" and "copy" access must be granted on production machines.
J. **Database Access: Direct** — All direct access to any Citadel Servicing Corporation database must be restricted to authorized administrators.

4.5.6. Managing Accounts

Maintenance and monitoring of user accounts is important to ensuring the continued security of Citadel Servicing Corporation systems and data. Citadel Servicing Corporation ensures that:

A. The system owners (or designated manager) will review end-user worker accounts and access privileges to systems on a semi-annual basis at a minimum.
B. Account reviews will be performed at least semi-annually for systems.
C. Active Directory Accounts that are inactive for greater than thirty (30) days will be disabled (temporarily or permanently) following review with Human Resources.
D. Authentication and system access will be disabled upon employee termination or the termination of a business contractor, consultant, temporary worker or vendor.
E. Accounts must be deactivated the same day upon receipt of termination notice.
F. Password policies are standardized in terms of complexity, aging, restrictions, re-use, change, auto log-off, account lockouts after bad logins, etc. Refer to the Password Security Policy.

4.6. AWARENESS TRAINING

The information security awareness program should ensure that all employees achieve and maintain a basic level of understanding on a broad range of information security matters, including their obligations under various information security policies, standards, procedures, guidelines, laws, regulations, contractual terms and plus generally held standards of ethics and acceptable behavior.

Security awareness and training activities should commence as soon as practicable after employees join the organization, ideally starting with an information security induction/orientation session. These awareness activities should occur on a continuous periodic basis thereafter in order to maintain a reasonably consistent level of awareness.

Citadel Servicing Corporation 's Information Security Awareness materials are in an online library and are securely accessed via a network login with instructions provided by the Human Resources Department. These materials are intended to provide information and guidance on a wide variety of information security matters. Employees with limited or no network access must also be kept informed by other means such as seminars, posters, newsletters, briefings and courses.

4.7. ENFORCEMENT

All users (employees, contractor, part-time and temporary workers, authorized third party service providers) 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.

The company reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity.

The company does not consider conduct in violation of this policy to be within the scope of employment for employees or partners, or the direct consequence of the discharge of employee or partner duties. Accordingly, to the extent permitted by law, the company reserves the right not to defend or pay any damages awarded against employees or partners that result from violation of this policy.

Any employee or partner, who is requested to undertake an activity which he or she believes is in violation of this policy, must provide a written or verbal complaint to his or her manager, any other manager, Legal, or the Human Resources Department as soon as possible.