PERSONNEL SECURITY POLICY

2022

31. PERSONNEL SECURITY POLICY

POLICY STATEMENT

Citadel Servicing Corporation will ensure that rules are established to govern and control who can have access to company locations and facilities. These rules and controls are to ensure the protection of the company's information assets from unauthorized access and adverse actions of personnel.

31.1. OVERVIEW

Citadel Servicing Corporation is critically dependent on information and information systems as the company's operations would be negatively impacted if sensitive/confidential information was disclosed inappropriately. It is important for the company to establish rules and requirements and ensure that employees meet them in order to have the appropriate access to corporate IT systems, assets, data and/or facilities. These policy standards implement security best practices with regards to personnel screening, requirements and training.

31.2. PURPOSE

The purpose of this policy is for Citadel Servicing Corporation to take reasonable and appropriate steps to ensure individuals and/or entity identities are validated and true and to prevent those individuals and/or entities who should not have access from obtaining access to the company's IT systems and data.

31.3. SCOPE

This policy applies to all corporate 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.

31.4. 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.

31.5. POLICY

31.5.1. Roles and Responsibilities

A. **Information Security Responsibility** — Responsibility for information security on a day-to-day basis is every employee's duty. Specific responsibility for information security is NOT solely vested in the Information Technology and Security Office/Leadership.

B. **Job Descriptions** — Specific information security responsibilities must be incorporated into all employee job descriptions if such employees have access to sensitive, valuable, or critical information.

C. **Health and Safety Information** — Management must fully disclose to the involved workers the results of toxic substance tests and other information relating to the health and safety of employees.

D. **Employee Status Changes** — Every change in the employment status of Citadel Servicing Corporation employees including, but not limited to, permanent employees, consultants, contractors, and temporaries, must be immediately reported by the individual's immediate manager to the Human Resources Department. The Human Resources Department must then immediately notify the involved Information Systems Administrators.

31.5.2. Pre-Employment Screening

A. **Background Checks** — All staff must pass a background check as a requirement to access the company's facilities, IT assets, information assets or other sensitive information and assets. Background checks will be conducted either by the company or an approved third-party that includes:

- Character reference verification
- Experience, academic record, and professional qualifications confirmation
- Government issued identification verification
- Criminal background check (*Note: criminal background checks will examine the last seven (7) years for any criminal history.)

All background check information will be retained for at least seven (7) years in a central and secure location for ease of maintenance.

B. **Non-Employee Background Checks** — Temporaries, consultants, contractors, and outsourcing organization staff must not be given access to sensitive information, or be allowed to access critical information systems, unless they have gone through a background check commensurate with the background checks given to regular employees. All background check information will be retained for at least seven (7) years in a central and secure location for ease of maintenance.

C. **Revealing Information to Prospective Employees** — Information systems technical details, such as network addresses, network diagrams, and security software employed, must not be revealed to job applicants until they have signed a confidentiality agreement and also have been hired or retained.

31.5.3. Terms and Conditions of Employment

A. **Required User ID Forms** — Users must sign both a confidentiality agreement and an information system security agreement prior to being issued a user ID permitting access to Citadel Servicing Corporation systems.

B. **Property Rights** — Without specific written exceptions, all programs and documentation generated by, or provided by any employee for the benefit of Citadel Servicing Corporation are the property of Citadel Servicing Corporation . Management must ensure that all workers providing such programs or documentation sign a statement to this effect prior to the delivery of these materials to Citadel Servicing Corporation .

C. **Non-Disclosure Agreements – Organization** — All Citadel Servicing Corporation employees will be required to acknowledge a non-disclosure, including but not limited to the protection and appropriate use of the company's IT assets, information assets, intellectual property, and any information in the custody of the company. Documentation of agreements will be retained in a secured, central location.

D. **Intellectual Property Rights** — While employees of Citadel Servicing Corporation , all staff members grant to Citadel Servicing Corporation exclusive rights to patents, copyrights, inventions, and all other intellectual property they originate or develop.

E. **Compliance Agreement** — As a condition of continued employment, employees, consultants, and contractors must annually sign an information security compliance agreement.

F. **Code of Conduct Acknowledgement** — All employees must indicate their understanding of the code of conduct by annually signing a form acknowledging that they agree to subscribe to the code.

G. **Conflicts of Interest** — All employees must avoid the actual or apparent conflict of interest in their business-related dealings with Citadel Servicing Corporation . Should there be any doubt as to the existence of a potential conflict of interest, the employee must consult their manager.

H. **Acceptable Use Policy** — Citadel Servicing Corporation will provide all employees a copy of the corporate Acceptable Use Policy for review. Employees are required to provide signed verification of a statement of understanding prior to consideration for authorized access.

31.5.4. Segregation of Duties

Maintaining and protecting the confidentiality, integrity, and availability of IT assets, information assets, and company reputation is of vital importance to Citadel Servicing Corporation . To help with this goal, the company requires procedures designed to assign responsibility of an activity to separate users when the actions of a single user could result in a high risk of disruption to business operations, financial loss or loss of sensitive/confidential information.

All users who access the company's facilities, IT assets or information assets, will be assigned a job/role/function, complete with job description to grant and verify the appropriate physical and logical security access.

No single individual will have complete control of a business process or transaction from inception to completion. Likewise, an individual must not be responsible for approving his or her own work.

Examples of segregation are:

- Responsibilities will be assigned so that no one individual has the opportunity to create and conceal errors or irregularities.
- The processing of data will be completely isolated from any development process such as design, programming, testing, and implementation of application programs.
- System and database administrators will not perform security maintenance work.
- Individuals responsible for maintaining logs will not be the same individuals responsible for log review.
- Appropriate segregation of duties is also an integral part of change implementation, and as such, will fall in line with corporate Change Management policies and procedures. Relevant changes range from patch, configuration, hardware, and software implementations.

A. **Separation of Request and Approval** — For any significant transaction, administrative procedure or change to Citadel Servicing Corporation information systems falling under the scope of this policy, the one(s) approving the change must be separate from the one(s) initiating the request.

B. **Separate Security Administration Functions** — Accordingly, the functions of information technology security administration and the functions of security infrastructure changes are to be kept separate. All security administration processes are to be designed and implemented so that no one person, alone, can compromise a security control, either inadvertently or deliberately.

C. **Separation Of Duties** — Whenever a Citadel Servicing Corporation computer-based process involves confidential valuable, or critical information, the system must include controls involving a separation of duties or other compensating control measures that ensure that no one individual has exclusive control over these types of information.

31.5.5. Security Awareness and Training

All users must be well informed of their responsibilities for information security. Effective information security requires participation by all users.

In addition to the provisioning of all information security policies and procedures, employees shall be expected to participate in additional security awareness training activities.

A. **Security Violations and Reporting** — Users must be clearly informed about the actions that constitute security violations as well as informed that all such violations will be logged and how to properly report possible security incidents.

B. **Information Security Policy Distribution** — On or before their first day of work, all new Citadel Servicing Corporation employees must be advised of the information security policy (policies) and be made aware that they must comply with the requirements described in these policies as a condition of continued employment.

C. **Policy Work Agreement** — Every employee must understand Citadel Servicing Corporation 's policies and procedures about information security and must agree in writing to perform their work according to these same policies and procedures.

D. **Information Security Policy Changes** — All Citadel Servicing Corporation employees must receive prompt notice of changes in the company's information security policy, including how these changes may affect them, and how to obtain additional information.

E. **Security Awareness Training** — All Citadel Servicing Corporation employees must complete the company's security awareness training program. This also includes any ongoing security awareness training programs and initiatives undertaken by the company. A record verifying the employee has completed the security awareness training will be maintained by the Information Security Office.

31.5.6. Personnel Transfers and Changes

A. **Reporting Status Changes** — Employees have a duty to promptly report to their immediate manager all changes in their personal status which might affect their eligibility to maintain their current position. Examples of such status changes include convictions for job-related crimes and outside business activities.

31.5.7. Personnel Terminations

A. Citadel Servicing Corporation **Immediate Terminations** — Unless the special permission of senior company management is obtained, all employees who have stolen Citadel Servicing Corporation property, acted with insubordination, or been convicted of a felony, must be terminated immediately. Such instant terminations must involve both escort of the individual off company premises, as well as assistance in collecting and removing the individual's personal effects.

B. **Worker Termination Responsibility** — In the event that an employee, consultant, or contractor is terminating his or her relationship with Citadel Servicing Corporation , the employee's immediate manager must ensure that all property in the custody of the employee is returned before the employee leaves

Citadel Servicing Corporation , notify all administrators handling the computer and communications accounts used by the employee as soon as the termination is known, and terminate all other work-related privileges of the individual at the time that the termination takes place.

C. **Notification of Worker Terminations** — All employees must be immediately notified as soon as an employee has been terminated. With each such notice, the Human Resources Department must regularly remind employees that departed employees are no longer permitted to:
   - Be on Citadel Servicing Corporation property (unless escorted by an employee)
   - Use Citadel Servicing Corporation resources
   - In any other way be affiliated with Citadel Servicing Corporation

D. **Notification to Third Parties of Worker Terminations** — If a terminated employee had authority to direct contractors, consultants, or temporaries, or if this same employee had the authority to bind Citadel Servicing Corporation in a purchase or another transaction, then the Human Resources Department must promptly notify all relevant third parties that the terminated employee is no longer employed by Citadel Servicing Corporation .

E. **Involuntary Terminations** — In all cases where information technology support workers are involuntarily terminated, they must be immediately relieved of all of their duties, required to return all Citadel Servicing Corporation equipment and information, and escorted while they pack their belongings and walk out of company facilities.

F. **Information Retention at Employment Termination** — Upon termination of employment, employees may not retain, give away or remove from company premises any Citadel Servicing Corporation information other than personal copies of information disseminated to the public and personal copies of correspondence directly related to the terms and conditions of their employment. All other Citadel Servicing Corporation information in the custody of the departing employee must be provided to the employee's immediate supervisor at the time of departure.

G. **Recovery of Organization Property** — Employees, temporaries, contractors, and consultants must return all hardware, software, working materials, confidential information, and other property belonging to Citadel Servicing Corporation upon termination of their contract or employment.

31.6. 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.