SECURITY AWARENESS POLICY

2022

2. SECURITY AWARENESS POLICY

POLICY STATEMENT

In order to fully protect the confidentiality, integrity and availability of corporate and client data that is created, stored and transmitted by Citadel Servicing Corporation , all workers must be informed about relevant and topical information security matters, and must be motivated to fulfill their information security obligations.

2.1. OVERVIEW

Employees who possess an adequate level of security awareness are more likely to recognize and react appropriately to information security threats, attacks and incidents. Equally, a lack of awareness means employees are more likely to place valuable information assets in danger through ignorance and carelessness. Citadel Servicing Corporation is committed to providing workers with ongoing awareness of a broad range of information security matters related matters, policies and Security Awareness Training efforts.

2.2. PURPOSE

To implement and maintain policies and procedures that ensure the effective communication of security processes used to protect the company's valuable information assets.

2.3. SCOPE

As part of Citadel Servicing Corporation 's corporate governance framework, this policy is relevant to all employees, and also applies to third parties acting in a similar capacity to our employees whether they are explicitly bound (e.g., by contractual terms and conditions) or implicitly bound (e.g., by generally held standards of ethics and acceptable behavior) to comply with corporate information security policies.

2.4. 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.

2.5. MANAGEMENT COMMITMENT

Citadel Servicing Corporation Senior Management will commit to the development of a security and privacy awareness program allocating staff and resources. The Information Security Office will have access to both the compliance and training departments for completion and update of training materials and tracking results.

2.6. COORDINATION AMONG ORGANIZATIONAL ENTITIES

Compliance with this policy is mandatory for all staff, including contractors and executives. Citadel Servicing Corporation will monitor compliance with this policy and remediate any non-compliance. As security tends to cross departmental and organizational boundaries, Citadel Servicing Corporation employees and contractors will work together to ensure that required security controls are in place, are maintained, and comply with the

policy described in this document. Security concerns, security incidents, or suspected/confirmed vulnerabilities will be shared with appropriate personnel in the organization so that the vulnerability can be remediated (or mitigated with compensating security controls), we can ensure that similar vulnerabilities in other systems or processes can be addressed and communicated, as appropriate, inside and possibly outside of the organization

2.7. TRAINING

The Information Security Office is responsible for implementing and maintaining information security awareness policies and procedures that ensure that Citadel Servicing Corporation employees, including those working remotely, receive security information and awareness reminders, periodic training and testing as needed, including but not limited to:

- Information security risks significant to data and computer systems and networks.
- How to use corporate computer systems and networks in a manner that reduces information security risks.
- Citadel Servicing Corporation 's legal and business responsibilities regarding protection of data and computer systems and networks.
- Substantial changes made to the company's legal or business responsibilities.
- Substantial threats or risks arising against corporate data, computers, and networks.
- Approved security practices for email, internet access, mobile devices, portable media, and social media.

2.8. POLICY

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.

Additional training is appropriate for all employees (e.g., IT personnel) with specific information security obligations that are not satisfied by basic security awareness, (e.g. Systems Administration and Network Management). The particular training requirements will reflect employees' relevant prior experience, training and/or professional qualifications, as well as job requirements.

Security awareness and training and testing 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 IT Department and third-party vendor. 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.

2.8.1. Training Delivery

Security information and awareness reminders and updates may include, but are not limited to:

- Online training programs delivered periodically
- Periodic testing campaigns which ensure the organization is improving
- E-mail reminders
- Letters
- Staff meetings
- Screen savers
- Information system sign-on messages

2.8.2. Training Content

Security awareness and training must cover, but is not limited to the following topics:

- Security reminders
- Protection from malicious software
- Log-in monitoring
- Password management
- Employee responsibilities for corporate and client data
- What constitutes a security breach and violation and how to report it
- Workforce sanctions for violations
- Phishing Simulations

2.8.3. Related Policies, Standards, Procedures and Guidelines

Item	Relevance
Information security policy	Defines the overarching set of information security controls.
Information security standards, procedures and guidelines	Amplify and explain the information security policies, providing greater detail on particular topics and/or pragmatic advice for particular audiences as well as mandatory obligations and responsibilities.
Other information security awareness and training materials	A broad range of information security awareness and training materials is available, covering both general security matters and more specific security topics. The materials are proactively maintained to maintain relevance to the ever-changing information security risk and control landscape.

2.9. 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.