CITADEL

SERVICING CORPORATION

CORPORATE SECURITY POLICY

2022

1. CORPORATE SECURITY POLICY

POLICY STATEMENT

Citadel Servicing Corporation is to ensure that the company vigorously protects corporate assets and confidential client information from technological or physical intrusion or misuse, keeping customer information safe and secure in compliance with federal and state laws and regulations.

1.1. OVERVIEW

In the course of business operations, Citadel Servicing Corporation routinely transacts business over both private and public networks that involve private customer and corporate information. In compliance with the Gramm-Leach-Bliley Act, the company has implemented a corporate information security program. Citadel Servicing Corporation ’s corporate security policy provides a security framework by establishing a comprehensive series of safeguards to ensure the protection of organizational systems, networks, equipment, applications, devices, and data against identified risks and threats in compliance with federal and state laws and regulations.

1.2. PURPOSE

The purpose of this policy is for the company to establish requirements and set direction for the corporate information security program. An information security policy requires the company to have an overall security plan that is designed to appropriately protect company systems, networks, equipment, applications, devices, and data against identified risks and threats. The company must understand its risks, monitor for unauthorized activity, identify and investigate potential violations, and apply sanctions as appropriate when violations occur.

This policy establishes the minimum requirements and responsibilities for the protection of company information assets, preventing the misuse and loss of information assets, establishing the basis for audits and self-assessments, and preserving company management options and legal remedies in the event of asset loss or misuse.

1.3. SCOPE

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

1.4. TRAINING

Citadel Servicing Corporation will develop appropriate training and education programs for all those covered by the security program. IT Security Awareness and Training are available to the users for access through a third-party vendor. All new employees, including temporary and contract personnel are required to review and comply with the Information Security Policies and complete the required modules of the Information Security Training and Awareness programs within a specified timeframe. Human Resources and the IT department will monitor the completion of initial training and subsequent training updates.

1.5. 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.

1.6. POLICY REQUIREMENTS

1.6.1. Programs

Citadel Servicing Corporation must implement and maintain the following comprehensive information security programs.

- **Information Security Program** — designed to secure information assets in a manner commensurate with each asset's value as established by risk assessment and mitigation measures.

- **Information Privacy Training Program** — a comprehensive information privacy program that will secure the personally identifiable information (PII) of employees and customers against unauthorized use or disclosure.

1.6.2. Policies and Procedures

To assure the security, reliability, integrity, and availability of company information assets; the information security program must contain policies and supporting procedures that define:

- The risk assessment process.
- Enterprise-wide security controls.
- Security testing.
- Service provider oversight.
- Requirements for periodic review and updating of the information security program.
- Appropriate requirements for management reporting.
- The safeguarding of customer information.
- Procedures to enforce security policies and assure the security, reliability, integrity, and availability of information assets.
- Protection against accidental or unauthorized modification, disclosure, or destruction.

1.6.3. Risk Identification and Assessment

Citadel Servicing Corporation will identify and assess internal and external risks to the security, confidentiality, and integrity of company networks, systems, and data. At a minimum, this process considers the risks to those systems and data, and the safeguards currently in place to manage those risks.
Citadel Servicing Corporation will establish procedures for identifying and assessing risks in the company's operations. The risk assessments will be performed at a minimum annually, to determine gaps where additional security controls are needed. If gaps are identified, recommendations will be made to mitigate potential risk.

Risk assessments include system-wide risks, as well as third-party services or other risks unique to the company business operations.

1.6.4. Information Safeguards and Monitoring

Citadel Servicing Corporation will design, implement, and regularly monitor safeguards to control identified risks to the security, confidentiality, and integrity of company systems and data. The safeguards are to ensure that access to company systems and data is limited to those who have a legitimate business reason to access such information. Such safeguards and monitoring will include, but are not limited to:

Information Systems: Citadel Servicing Corporation ’s information systems include network and software design, as well as information processing, storage, transmission, and disposal. Safeguards are designed and implemented in accordance with the nature and scope of the company's operations and the sensitivity of the data.

Citadel Servicing Corporation will implement and maintain administrative, technical, and physical safeguards to control the risks to information systems, as identified through the risk assessment process. Citadel Servicing Corporation will design and implement safeguards that may include, but are not limited to:

- Creating and implementing access limitations.
- Using secure, password-protected systems and encrypted transmissions within and outside the company.
- Regularly installing patches to correct software vulnerabilities.
- Managing the storage of corporate on transportable media.
- Permanently removing company data from computers, hard drives, or other electronic media prior to disposal.
- Storing physical records in a secure area with limited access.
- Protecting company data and systems from physical hazards such as fire or water damage.
- Disposing of outdated data under the company data retention policy.
- Other reasonable measures to secure and protect company data during the course of its life cycle.

Security Management: Citadel Servicing Corporation will develop and implement effective procedures for preventing, detecting, and responding to actual and attempted attacks, intrusions, and other systems failures. These security management procedures may include, but are not limited to:

- Implementing and maintaining current anti-virus software.
- Maintaining appropriate filtering or firewall technologies.
- Regularly obtaining and installing patches to correct software vulnerabilities.
- Disposal of data.
- Regular backing up of data.
- Implementing incident response plans.
- Other reasonable measures.

Citadel Servicing Corporation will be responsible for monitoring and disseminating information related to the reporting of known security attacks and other threats to the integrity of company networks.

Monitoring and Testing: Citadel Servicing Corporation will develop and implement procedures to test and monitor the effectiveness of information security safeguards. Monitoring will be appropriate to the probability and potential impact of the risks identified, as well as the sensitivity of the information involved. The monitoring may include sampling, systems checks, systems access reports, and any other reasonable measures adequate to verify that Information Security Program safeguards, controls, and procedures are effective.

1.6.5. Service Providers and Contract Assurances

Citadel Servicing Corporation will identify service providers with access to company systems and data. Citadel Servicing Corporation will ensure that reasonable steps are taken:

- To select and retain service providers capable of maintaining appropriate safeguards for company data and systems.
- To require service providers, by contract, to implement and maintain such safeguards.
- To require service providers, by contract, to grant the company assurances that they are in compliance of corporate security policies and other binding laws, statutes and regulations.

1.6.6. Exceptions

Exceptions to information security policies are permissible only under the following conditions:

- The Exception request has been submitted in writing by an Citadel Servicing Corporation employee responsible for information security.
- A member of the Information Security Office has signed off on the request.
- A risk assessment identifying and examining non-compliance has been performed and approved by company management.
- Documented and approved exceptions to Citadel Servicing Corporation security policy must be reviewed at least annually.

1.6.7. Distribution

A. Citadel Servicing Corporation management must publish written information security policies and make them available to all employees and relevant external parties.

B. Citadel Servicing Corporation employees and contractors must review and acknowledge acceptance of the information security policies on an annual basis and more often as required by the introduction of a new policy or significant revision to existing policies.

C. Citadel Servicing Corporation security policy documents must be labeled as “CONFIDENTIAL – Internal Use Only” and must be revealed only to Citadel Servicing Corporation workers and selected outsiders (such as auditors) who have a legitimate business need for this information.

1.6.8. Policy Review

Information security policy documents must be reviewed by management at least on an annual basis. This management review must include information related to:

- Any feedback from interested parties.
- Results of independent reviews of the policy.
- The status of preventive and corrective actions.
- The results of previous management reviews.
- Information security management.
- Threat and vulnerability trends.
- Information security incidents.
- Recommendations of relevant authorities.

Management review output must include any decisions and actions related to:

- Ensure the effectiveness of the program and improve the organization’s approach to managing information security and its processes.

- The improvement of control objectives and controls.
- Improvement in the allocation of resources and/or responsibilities.
- Ensure compliance with any related federal and state laws and regulations as required by business operations.

1.6.9. Responsibility Assignment

Information Security Responsibilities — The **Information Security Office** is responsible for establishing and maintaining organization-wide information security policies, standards, guidelines, and procedures.

Information Security Management Committee — An information security management committee composed of senior managers/IT leaders or their designees must meet quarterly to review the current status of information security at Citadel Servicing Corporation , approve and later review information security projects, approve new or modified information security policies, and perform other necessary high-level information security management activities.

Information Security Resources — Management must allocate sufficient resources and staff attention to adequately address information systems security.

Management Responsibility — Information security is a management responsibility, and decision-making for information security must not be delegated. While specialists and advisors play an important role in helping to make sure that controls are designed properly, functioning properly, and adhered to consistently, it is the manager in charge of the business area involved who is primarily responsible for information security.

Information Ownership Assignment — IT Leadership must clearly specify in writing the assignment of Information Ownership responsibilities for those product systems, databases, master files, and other shared collections of information used to support production business activities.

1.6.10. Worker Roles

Citadel Servicing Corporation has established three categories that define general responsibilities with respect to information security: Owner, Custodian, and User. At least one of these categories applies to each worker.

A. **Owner** — Information Owners are the department managers, members of the top management team, or their delegates within Citadel Servicing Corporation who bear responsibility for the acquisition, development, and maintenance of production applications that process Citadel Servicing Corporation information.

B. **Custodian** — Custodians are in physical or logical possession of either Citadel Servicing Corporation information or information that has been entrusted to Citadel Servicing Corporation Custodians are responsible for safeguarding the information, including implementing access control systems to prevent inappropriate disclosure, and making backups so that critical information will not be lost.
   - While Information Technology department staff members clearly are Custodians,
   - Whenever information is maintained only on a personal computer, the User is also a Custodian.
   - Each type of production application system information must have one or more designated Custodians.

C. **User** — Users access customer and information according to their role in the company. Users are responsible for familiarizing themselves with and complying with all Citadel Servicing Corporation policies, procedures, and standards dealing with information security. Questions about the appropriate handling of specific information types should be directed to either the Custodian or the Owner of the involved information.

1.6.11. Clean Desk Practices

It is important for all users to understand their responsibilities to Citadel Servicing Corporation to maintain the security of confidential information at their desks. A clean desk can be an important tool to protect and minimize the risk of security breaches of sensitive and confidential corporate and client information. Examples of such sensitive and critical information are:

- Reports that contain corporate or client personal information, account numbers, card numbers.
- Corporate and client documentation (e.g., applications, notices, or correspondence).
- Company mobile devices, or portable storage devices (e.g., USB flash drives, external hard drives, CDs, DVDs)

To ensure corporate and client information is protected, users are required to do the following:

- Ensure that all sensitive/confidential information in hardcopy or electronic form is secure in their work area at the end of the day and when they are expected to be gone for an extended period.
- Any Restricted or Sensitive information must be removed from the desk and locked in a drawer or file cabinet when the desk is unoccupied and at the end of the workday.
- Private offices should be locked when unoccupied if confidential documents are left visible during business hours.
- File cabinets and Records rooms containing Restricted or Sensitive information must be kept closed and locked when not in use or when not attended. Keys or combinations to the cabinets will be tracked controlled by the Facilities department.
- Keys used for access to Restricted or Sensitive information must not be left anywhere unattended.
- Passwords must not be left on sticky notes posted on or under a computer; any passwords written down must comply with password protection policy guidelines and be stored in a secure location.
- Printouts containing Restricted or Sensitive information must be immediately removed from the printer or fax. Printers that auto print reports need to be turned off on when non-authorized (e.g., cleaning staff) are accessing the printer area.
- Upon disposal, Restricted and/or Sensitive documents should be shredded in official shredder bins or placed in locked confidential disposal bins.
- Whiteboards containing Restricted and/or Sensitive information must be erased when a meeting adjourns.
- Treat mass storage devices such as CD-ROM, DVD or USB drives as sensitive and secure them in a locked drawer or cabinet.

If users have any questions or require more information, regarding clean desk practices, they should contact their manager or the Human Resources department.

1.6.12. Information Disposal

Hard drives, USB drives, CDs/DVDs and other storage media contain various kinds of company data, some of which is considered sensitive. In order to protect the company's and client's data, all storage mediums must be properly erased before being disposed of. Citadel Servicing Corporation employs processes and procedures to ensure that any data is securely erased prior to equipment disposal.

1.6.13. Information Disposal Standards

Data Sanitation Standards— The Information Security Office working is responsible for establishing standards for the proper data sanitization of all computer equipment and media storage scheduled for destruction. Third-party vendors contracted to dispose of equipment must provide certification of standards and use the same standards or approval to use another standard in the contract prior to any disposal.

Approved Disposal Vendor List — Citadel Servicing Corporation will maintain an approved and certified list of commercial data disposal vendors to properly dispose of electronic media. Use of any other vendor for disposal of equipment must have prior approval.
Approved Software Vendor List — Citadel Servicing Corporation will maintain a list of approved commercial software packages and vendors which perform data overwriting operations. Employees must only use approved software to overwrite electronic media. Use of other software to perform any overwriting must have prior approval.

1.6.14. Roles and Responsibilities

Information Management— The **Information Security Office** is responsible for establishing standards for the proper identification and labeling of Citadel Servicing Corporation information according to sensitivity levels. IT Management is also responsible for establishing detailed standards for the proper destruction of electronic data to implement this policy.
Data Owners — Data owners are responsible for ensuring that all Citadel Servicing Corporation data under their ownership is properly destroyed according to this policy.
Users — All users of computer systems within Citadel Servicing Corporation , including contractors and vendors with access to company systems, are responsible for taking the appropriate steps, as outlined below to ensure that all computers and electronic media are properly sanitized before disposal.

1.6.15. Disposal of Electronic Media

Storage Media Destruction — Destruction of sensitive information captured on computer storage media must only be performed with approved destruction methods including shredders or other equipment approved by IT Management.
Disposal of Electronic Media Outside of the Company — All electronic media other than computer hard drives must be erased, degaussed, or rendered unusable before leaving Citadel Servicing Corporation . Employees must only use approved commercial vendors from the Disposal Approved Vendor List.
Disposal of Media Containing Sensitive or Secret Data — Citadel Servicing Corporation must not resell or recycle media that contained highly classified data such as client or confidential company information. Media containing such information must be sanitized and physically destroyed.

1.6.16. Disposal of Computer Equipment

Used Component Equipment Release — Before donation, or recycling, the IT Department or their designee must validate that sensitive information has been removed from any information systems equipment that has been used for **Used Component Equipment Release** — Before donation, or recycling, the IT Department or their designee must validate that sensitive information has been removed from any information systems equipment that has been used for Citadel Servicing Corporation business. This validation process must take place before releasing such equipment to a third-party. A certified vendor under contract may handle equipment disposal without IT validation with approval of the CIO and Legal Department.
Information and Equipment Disposal — Managers are responsible for the disposal of surplus property no longer needed for company activities in accordance with procedures established by Citadel Servicing Corporation **'s** IT Department and Legal Department, including the irreversible removal of sensitive information and licensed software.
Inventory of Decommissioned Computer and Network Equipment — Citadel Servicing Corporation must maintain an inventory of all company computer and network equipment that has been taken out of commission. This inventory must also reflect all actions taken to clear memory chips, hard drives, and other storage locations in this same equipment of all stored information.
Labeling Required — Equipment designated for surplus or other re-use should have a label affixed stating that the hard drive has been properly data sanitized.
This validation process must take place before releasing such equipment to a third-party. A certified vendor under contract may handle equipment disposal without IT validation with approval of the CIO and Legal Department.

Information and IT Equipment Disposal — IT Managers are responsible for the disposal of surplus Information Technology property no longer needed for company activities in accordance with procedures established by Citadel Servicing Corporation ’s, Legal Department and CIO, including the irreversible removal of sensitive information and licensed software.
Inventory of Decommissioned Computer and Network Equipment — Citadel Servicing Corporation must maintain an inventory of all company computer and network equipment that has been taken out of commission. This inventory must also reflect all actions taken to clear memory chips, hard drives, and other storage locations in this same equipment of all stored information.
Labeling Required — Equipment designated for surplus or other re-use should have a label affixed stating that the hard drive has been properly data sanitized.

1.6.17. Transfer of Hard Drives and Media

Transfer of Hard Drives — Before a hard drive is transferred from the custody of its current owner, appropriate care must be taken to ensure that no unauthorized person can access the data by ordinary means. All electronic media should be data sanitized according to Citadel Servicing Corporation procedures.
Transfer of Electronic Media — Before electronic media is transferred from the custody of the current owner, appropriate care must be taken to ensure that no unauthorized person can access data by ordinary means. Electronic media such as floppy disks, rewritable CDs/DVDs, flash drives, external hard drives, cell phones, videotapes, and audiotapes should be erased if the media type allows it or destroyed if erasure is not possible.
Attempted Recovery — Attempts to recover deleted or sanitized data must only be done by specially trained personnel approved by Citadel Servicing Corporation management. Insofar as special recovery tools would have to be used by an individual to access the data erased by this method, any attempt by an individual to access unauthorized data would be viewed as a conscious violation of state or federal regulations, and Citadel Servicing Corporation Data Privacy guidelines.

1.6.18. Disposal of Hardcopy Records

Hardcopy Disposal — When disposed of, all secret, confidential, or private information in hardcopy form must be either shredded or incinerated. To ensure that documents are properly destroyed, only shredders approved by Citadel Servicing Corporation will be used to shred hardcopy records containing sensitive information.
Secure Information Containers — Sensitive information that is no longer needed must be placed in a designated locked destruction container within Citadel Servicing Corporation offices and never placed in trash bins, recycle bins, or other publicly-accessible locations.
Physically Securing Trash Dumpsters — Citadel Servicing Corporation trash dumpsters located outside company offices must be kept in a secured area (e.g., locked metal cage), and must be opened only for authorized trash hauling company staff.

1.6.19. Litigation Hold

Destroying Documents and Electronic Media Relevant to Litigation — If there is credible reason to believe that certain Citadel Servicing Corporation internal documents and electronic media containing data may be needed as evidence in upcoming litigation, these documents/media must not be destroyed by the ongoing Citadel Servicing Corporation document/media destruction process. They must instead be brought to the attention of the Legal Department, and then properly secured.

1.6.20. Personally Identifiable Information (PII)

Personally Identifiable Information (PII) is information that can be used to identify an individual, whether on its own or in combination with other personal or identifying information that is linked or linkable to an individual. Protected health information (PHI) is considered a separate category of information and is governed under the Health Insurance Portability and Accountability Act (HIPAA).

Federal and state information privacy laws require Citadel Servicing Corporation to protect certain elements of PII, often because of the sensitivity of the data and/or its potential for misuse for fraudulent activities or other forms of identity theft. These laws may require Citadel Servicing Corporation to self-report to the state or federal government and/or provide notice to affected individuals if the security of certain PII is breached.

The following table provides examples of different types of PII:

Examples of PII that may require legal notification of breach	**Examples of other Legally Protected PII that is considered Sensitive/Confidential**	**Examples of other forms of PII with the potential of misuse**
Social Security Numbers	Student education records	Date of Birth
Credit card numbers	Employee records	User credentials
Financial account information	Records of corporate meetings	Partially redacted PII (e.g., last 4 digits of SSN)
Driver's license numbers	Banking and personal financial information that does not include account information	Employee ID numbers

The following table lists PII elements that are not necessarily considered private, however combining these elements with other PII may have privacy implications.

Examples of other PII that may be misused if combined with other PII or aggregated
Address
Phone number
Email address

A given element of PII may be protected under more than one federal or state law or Citadel Servicing Corporation policy. The company has adopted other information privacy policies governing specific categories of information, as set forth in the company's data class and protection policies and guidelines.
Citadel Servicing Corporation Employees and all non-employee authorized access to information users having any questions, or concerns, regarding the protection of PII, should be immediately directed to the Compliance department.

1.6.21. Protection and Handling of PII

General — In addition to complying with all applicable legal requirements, Citadel Servicing Corporation further limits the collection, use, disclosure, transmission, storage and/or disposal of PII to that which fulfills the requirements of Citadel Servicing Corporation **'s** business operations.

Safeguards — To protect PII against inappropriate access, use, disclosure, or transmission, Citadel Servicing Corporation requires appropriate administrative, technical and physical safeguards. The company is responsible for establishing Information Security Awareness programs and training, procedures, security controls, and risk management consistently within the company. Examples of physical safeguards include storing documents containing PII in secured cabinets or rooms and ensuring that documents containing PII are not left on desks or in other locations that may be visible to individuals not authorized to access the PII.
Collection — Collection of PII should be done in a way that is consistent with the other provisions of this section (e.g., Minimization). Collected data should be appropriate for the intended authorized use, and collection should be conducted according to best practice and legal requirements for the type and purpose of data collected. Since the collection process itself can potentially lead to unintended PII disclosure, considerations of confidentiality in collection and recording should be explicitly addressed.
Minimization — All staff of Citadel Servicing Corporation (e.g., management, employees and contractors) are responsible for minimizing the use of PII (including redaction of financial account information, use of less sensitive substitutes such as partial SSN and corporate unique identifiers) and minimizing aggregations of PII. The risk of unauthorized disclosure of or access to PII increases with the amount of data. All staff (employee and non-employee) of Citadel Servicing Corporation are responsible for ensuring that the number and scope of physical and electronic copies and repositories of PII are kept to the minimum necessary and only for the time period where a valid business need for the information exists.
Permitted Use within the Company — Only individuals authorized by Citadel Servicing Corporation who are permitted under law, regulation and company policies and have a legitimate "need to know" are authorized to access, use, transmit, handle or receive PII, and that authorization only extends to the specific PII for which the relevant individual has a legitimate “need to know” for the purposes of performing their job duties.
Permitted Disclosure to Third Parties — Citadel Servicing Corporation may release PII to third parties only as permitted by law/regulation and company policy. Third party contractors to whom Citadel Servicing Corporation is disclosing PII must be bound by agreements with appropriate PII safeguarding and use provisions.
Oral Communications — Only authorized individuals may engage in oral communications involving PII. Caution is required in all oral communications involving PII, and oral communications involving PII may not take place in any location where the communication may be overheard by an individual not authorized to access the PII.
Storage of PII — PII may be stored only as necessary for the requirements of Citadel Servicing Corporation **’s** business operations and permitted under company policy. Citadel Servicing Corporation is responsible for providing guidelines around where information can be scanned/stored (e.g., in hardcopy, on shared drives, on other media/devices) and how long information may be retained before requiring deletion or destruction). In addition, the company is responsible for maintaining an up-to-date inventory of stored or maintained documents, files, data bases and data sets containing PII, and their contents; and requiring encryption of PII stored on mobile devices, media or other at-risk devices such as public workstations.
Transmission of PII — PII may not be transmitted to external parties outside of the company (e.g., via mail, fax, e-mail, FTP, instant messaging) without appropriate security controls. Generally, such controls include encryption and authentication of recipients (e.g., password protection of files; verifying fax numbers; cover sheets; marking documents as confidential). Precautions are to be taken to ensure that e-mails are sent only to intended recipients.
Disposal — PII must be destroyed and rendered unreadable prior to disposal. For example, this may include shredding papers or wiping electronic files.
Training — Citadel Servicing Corporation is responsible for ensuring that its staff have appropriate training on the company’s information privacy policies and sign confidentiality agreements to the extent necessary and appropriate, before accessing, using, transmitting, handling or receiving PII.

1.6.22. Breaches of the Privacy

Known or suspected violations of policy should be reported promptly. Any incidents that have the potential to damage Citadel Servicing Corporation and/or the company’s network operations should be reported immediately to the Compliance and Legal Departments. Violators of this policy may be subject to criminal and/or civil penalties and to disciplinary action, up to and including termination.

1.6.23. Program Reporting

Annual Security Program Report — Annual reports must be submitted to company management that includes information on:

- The status of the program.
- The updated risk assessment and analysis.
- Management decisions for the level of risk mitigation and residual risk accepted.
- Service provider oversight activities and status.
- The results of testing of key controls.
- Management's response to any identified deficiencies and recommendations for program changes.
- The independent validation of the information contained in the report.

1.6.24. Program Review and Maintenance

A. **Annual Program Updates** — The information security program must be updated and re-approved by Citadel Servicing Corporation management annually or whenever there is a material change in the organization or infrastructure.

B. **Risk Assessments** — The information security program must be updated, as appropriate, based on the results of the internal risk assessments and any risk assessment completed by a third party.

C. **Information System Control Reviews** — An independent and externally-provided review of information systems security must be obtained periodically to determine both the adequacy of and compliance with controls.

D. **Change Considerations** — The appropriate level of expertise must be applied to evaluate whether changes in the organization or infrastructure should trigger a change to the information security program. Changes that must be considered that could require an update to the information security program are the effect of changes in:
   - Technology.
   - The sensitivity of information.
   - The nature and extent of threats.
   - Citadel Servicing Corporation ’s business arrangements (e.g., mergers. alliances. joint ventures).
   - Customer information systems (e.g., new configurations, new connectivity, new software).

1.6.25. Program Compliance

All relevant statutory, regulatory, and contractual requirements for every Citadel Servicing Corporation production information system must be thoroughly researched, explicitly defined, and included in current system documentation.

1.6.26. Policy Sanctions

Policy Sanctions — Citadel Servicing Corporation must implement sanctions against employees and third parties who violate the written policies.

Policy Sanction Disciplinary Process — Assuming the action is inadvertent or accidental, first violations of information security policies or procedures must result in a warning. Second violations involving the same matter must result in a letter being placed in the involved worker's personnel file. Third violations involving the same matter must result in a five-day suspension without pay. Fourth violations involving the same must result in dismissal. Willful or intentional violations, regardless of the number of violations, may result in disciplinary action up to and including immediate dismissal.

1.7. 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.

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 or the Human Resources Department as soon as possible.