DATA CLASS AND PROTECTION POLICY

2022

26. DATA CLASS AND PROTECTION POLICY

POLICY STATEMENT

It is the policy of Citadel Servicing Corporation to ensure its data is managed properly to protect and safeguard the information in its care, grant proper authorized access in compliance with industry, state, and federal laws and regulations to protect from loss, to avoid reputation damage, and to avoid adversely impacting our customers.

26.1. OVERVIEW

Sensitive information must be protected regardless of its form, whether electronic, hard copy or intellectual. Rules and requirements for ensuring effective management of data are important for Citadel Servicing Corporation to meet the industry and legal requirements of protecting the confidentiality, integrity, and availability of corporate IT assets, information assets, and reputation.

26.2. PURPOSE

The purpose of this policy is for Citadel Servicing Corporation to establish guidelines and controls to classify and protect corporate information assets and data, granting access only to authorized individuals/groups. This policy is intended to work in conjunction with corporate data retention, electronic data disposal, encryption, and acceptable use policies. This policy addresses information originated, modified, stored, transferred, and/or recovered electronically and non-electronically.

26.3. SCOPE

The scope of this policy includes all employees, contractors, consultants, temporary employees, and other entities at Citadel Servicing Corporation including all personnel affiliated with third parties. This policy covers all computer and communication devices owned or operated by the company and includes all electronic communication mediums as well as all storage media. This policy applies to any of the company's information in hardcopy or electronic format.

26.4. 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.

26.5. POLICY

Citadel Servicing Corporation bases its information access on the concepts of "Need-to-Know" and "Least Privilege". The concept of "Need-to-Know" stipulates that you must have a business need to know information in

order to be authorized to access that information. The "Least Privilege" concept stipulates that you will be given the least amount of access to information that you need to accomplish your job functions.

26.5.1. GLBA Covered Information

Citadel Servicing Corporation is required to protect covered customer data in accordance with the Gramm Leach Bliley Act (GLBA). GLBA defines covered customer information as any record containing non-public personal information (NPI) or personally identifiable financial information (PII) about a customer of Citadel Servicing Corporation – whether in paper, electronic, or other form – that is handled or maintained by or on behalf of Citadel Servicing Corporation or its affiliates. Some examples of such data include, but are not limited to:

- Personnel and/or payroll records
- Social Security Numbers
- Customer contact information
- Credit card numbers
- Account numbers
- Account balances
- Any financial transactions
- Tax return information
- Driver's license number
- Date or location of birth
- Authentication information
- Legal Contracts

26.5.2. Responsibility for Data Management

Data is a critical asset of the company and is often referred to as information assets. All Citadel Servicing Corporation Technology, Information Systems and Business Systems users have a responsibility to protect the confidentiality, integrity, and availability of data originated, generated, accessed, modified, transmitted, stored or used by the company, irrespective of the medium on which the data resides and regardless of format (such as electronic, paper, or other physical form).

26.5.3. Information Protection

Information must be consistently protected throughout its life cycle: Creation, transfer, transmission, processing, storage, recovery, and destruction. Information must be protected in a manner appropriate with its level of classification, no matter where it resides, what form it takes, what technology was used to handle it, or what purposes it serves.

26.5.4. Guidelines for Interpretation of Policy

Refer to the policy section regarding "Information Classification" for more detail.

Public Data — Information can be seen by anyone anywhere without harm to the organization, including information identified for the public domain. Information still requires approval by management before release/disclosure.

Internal Use — Information can be seen or used by anyone within the organization regardless of job or business function. Approved contractors and vendors can view this information.

Confidential — Information must be limited to only those with a business need-to-know. This information can be viewed by contractors and vendors who have a business need for the information and approved by management.

Restricted — Information that can have a major impact on business if compromised/disclosed. Access limited to only those authorized to view or have been granted access to view on a need-to-know basis.

26.5.5. Information Ownership

Information Owner — All production information possessed by or used by a particular organizational unit must have a designated Information Owner who is responsible for determining appropriate sensitivity classifications and criticality ratings, making decisions about who can access the information, and ensuring that appropriate controls are utilized in the storage, handling, distribution, and regular usage of information.

Information Custodian — Each significant type of production information must have a designated Custodian who will properly protect company information in keeping with the designated Information Owner's access control, data sensitivity, and data criticality instructions.

Information Systems Department Ownership Responsibility — With the exception of operational computer and network information, the Information Systems Department must not be the Owner of any production business information.

26.5.6. Information Classification

Sensitive information assets will be protected from unauthorized disclosure, use, modification, recovery, and destruction based on classification.

Four-Category Data Classification — All Citadel Servicing Corporation data must be broken into the following four (4) sensitivity classifications:

- Restricted
- Confidential
- Internal Use Only
- Public

Distinct handling, labeling, and review procedures must be established for each classification. If there is any uncertainty in the intentions, requirements, or expectations of this or other policies or procedures, users must consult their manager or contact human resources for clarification or guidance.

Data classified as Restricted and Confidential Data, also referred to as Non-public information (NPI), is information protected by statutes, regulations, laws, company policies, and/or contractual obligations. Data classified as Restricted or Confidential may be disclosed to individuals only on a "Need-to-Know" basis.

Data Classification Descriptions — The following descriptions are used for identifying and labeling each sensitivity classification for all Citadel Servicing Corporation information.

RESTRICTED — This classification label applies to the most sensitive business information that is intended for use strictly within the company. Its unauthorized disclosure could seriously and adversely impact the company, its customers, its business partners, and its suppliers. Examples include merger and acquisition documents, corporate level strategic plans, litigation strategy memos, and Trade Secrets (e.g., corporate-owned computer applications and code).

CONFIDENTIAL — This classification label applies to less-sensitive business information that is intended for use within the company. Its unauthorized disclosure could adversely impact the company or its customers, suppliers, business partners, or employees. Information that some people would consider to be private is included in this classification. Examples include employee performance evaluations, customer transaction data, strategic alliance agreements, unpublished internally-generated market research, computer passwords, and internal audit reports.

INTERNAL USE ONLY — This classification label applies to all other information that does not clearly fit into the previous two classifications. While its unauthorized disclosure is against policy, it is not expected to seriously or adversely impact the company or its employees, suppliers, business partners, or its customers. Examples include staff lists, partner or client lists, new employee training materials, and internal policy manuals.

PUBLIC — This classification applies to information that has been approved by company management for release to the public. By definition, there is no such thing as unauthorized disclosure of this information and it may be disseminated without potential harm. It is defined as information with no existing local, national, or international legal restrictions on access or usage. Public data, while subject to disclosure rules, is available to all members of the organization and to all individuals and entities external to the organization. Examples include product and service brochures, advertisements, job opening announcements, and press releases.

Default Classification — Information without a label is by default classified as Internal Use Only.

26.5.7. Declassification and Downgrading

Dates for Reclassification — If known, the date that Restricted or Confidential information will no longer be sensitive or declassified must be indicated on all company sensitive information. This will assist those in possession of the information with its proper handling, even if these people have not been in recent communication with the information's Owner.

Expired Classification Labels — Those employees in possession of sensitive information that was slated to be declassified on a date that has come and gone, but is not known definitively to have been declassified, must check with the information Owner before they disclose the information to any third parties.

Notifications — The designated information Owner may, at any time, declassify or downgrade the classification of information entrusted to his or her care. To achieve this, the Owner must change the classification label appearing on the original document, notify all known recipients and Custodians, and notify the company archives Custodian.

Schedule for Review — To determine whether sensitive information may be declassified or downgraded, at least once annually, information Owners must review the sensitivity classifications assigned to information for which they are responsible. From the standpoint of sensitivity, information must be declassified or downgraded as soon as practical.

26.5.8. Internal Use Data Protection

Protection of Citadel Servicing Corporation data classified as INTERNAL USE ONLY must be protected with safeguards to prevent loss, theft, unauthorized access, and/or unauthorized disclosure. Protection of this data will include, but not limited to, the following measures:

- Must be stored in a closed container (i.e., locked file cabinet, closed office, or department where physical controls are in place to prevent disclosure) when not in use.
- Must be destroyed when no longer needed subject to corporate data retention policies. Destruction must be destroyed in accordance with the corporate Information Disposal Policy. Destruction may be accomplished by:
    - "Hard Copy" materials must be destroyed by shredding or another process that destroys the data beyond either recognition or reconstruction. After destruction, materials may be disposed of with normal waste.
    - Electronic storage media will be sanitized in accordance with the Information Disposal Policy to make the data unreadable and irretrievable.

26.5.9. Restricted and Confidential Data Protection

Protection of Citadel Servicing Corporation data classified as RESTRICTED or CONFIDENTIAL must be protected with safeguards to prevent loss, theft, unauthorized access, and/or unauthorized disclosure. Protection of this data will include, but not limited to, the following measures:

- When stored on servers in an electronic format, must be protected with strong passwords and servers must have protection and encryption measures in place to protect the data.
- When stored locally on desktops, laptops, or portable devices, password protection and encryption are required.
- When transmitted electronically, encryption is required in accordance corporate encryption policies and standards. Restricted and Confidential data must be encrypted (256-bit encryption) when transiting over public networks.
- Ensure that any audit or error logs do not contain any clear text data classified as Restricted or Confidential (e.g., user passwords, client account information).
- Must not be disclosed to parties without explicit authorization.
- Must be stored only in a locked drawer or room or an area where access is controlled by a guard, cipher lock, and/or card reader, or that otherwise has sufficient physical access control measures to afford adequate protection and prevent unauthorized access by members of the public, visitors, or other persons without a need-to-know.
- When transmitted via e-fax/fax, must be sent only to a previously established and used address or one that has been verified as using a secured location.
- Must be destroyed when no longer needed subject to corporate data retention policies. Destruction must be destroyed in accordance with the corporate Information Disposal Policy. Destruction may be accomplished by:
    - "Hard Copy" materials must be destroyed by shredding or another process that destroys the data beyond either recognition or reconstruction. After destruction, materials may be disposed of with normal waste.
    - Electronic storage media will be sanitized in accordance with the Information Disposal Policy to make the data unreadable and irretrievable.

26.5.10. PCI DSS Compliance

As per the provisions of the Payment Card Industry Data Security Standards (PCI DSS) those data elements identified as requiring being stored/retained for business requirements will be classified in accordance with Citadel Servicing Corporation policies surrounding data classification and protection. Such data will be considered “Confidential Data” and the storage, handling and transmission of this data will be in accordance with corporate policies and align with the following company policies:

- Corporate Security Policy
- Mobile Device Policy
- Data Retention Policy
- Data Encryption and Device Control Policy
- Remote Access Policy
- Wireless Communication Policy
- Access Administration Policy
- Data Loss Prevention Policy
- Information Disposal Policy

Citadel Servicing Corporation does not currently store any PCI related information.

26.5.11. Storage of Personally Identifiable Information (PII)

Use of Personally Identifiable Information (PII) data within Citadel Servicing Corporation is classified as Confidential. As a requirement of access and use, storage of PII-related data is prohibited from end-user devices (e.g., laptops, workstations, tablets, smart phones).

If the storage of PII information on end-user devices is required, Citadel Servicing Corporation must obtain written permission from the appropriate data partners.

All devices storing PII-related data must have disk encryption enabled to protect the data. Encryption must meet the industry standard of 256-bit encryption.

Storage of PII-related data must be limited to designated systems, designed to store and protect that data. PII-related data must be stored on systems to isolate the data to prevent copying and intermingling with other company systems and data.

26.6. 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.