DATA RETENTION POLICY

2022

27. DATA RETENTION POLICY

POLICY STATEMENT

It is the policy of Citadel Servicing Corporation to ensure its data is managed in compliance with industry, state, and federal laws and regulations to provide secure retention of company data to protect from loss; to avoid reputation damage; and to avoid adversely impacting our customers.

27.1. 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 the company to meet the industry and legal requirements of protecting the confidentiality, integrity, and availability of corporate IT assets, information assets, and reputation.

27.2. PURPOSE

The purpose of this policy is for the company to take reasonable and appropriate steps to ensure that proper controls are in place to ensure secure record retention, storage, transmission and transportation of the company's data (both corporate and client) to protect against unauthorized or accidental access, alteration or destruction.

27.3. SCOPE

The scope of this policy includes all employees, contractors, consultants, temporary employees, and other entities at the company 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 company information in hardcopy or electronic format.

A stand-alone "Record Retention Policy" exists to address statutory loan origination and loan servicing related record keeping requirements and methodology.

27.4. 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.

27.5. POLICY

Citadel Servicing Corporation 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.

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

All Citadel Servicing Corporation data is broken into the following four (4) sensitivity classifications:

- Restricted
- Confidential
- Internal Use Only
- Public

Information is by default classified as Internal Use Only. Each data classification level has established its own distinct handling, labeling, and review procedures. 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.

For more information and guidance on Citadel Servicing Corporation data classification system, refer to the company's Data Class and Protection policy.

27.5.1. Retention and Maintenance of Records

Sensitive information must be protected regardless of its form, whether electronic, hard copy or intellectual. No distinctions between the words, data, information, knowledge, or wisdom are made for the purposes of this policy. It includes information known as intellectual property and or intellectual capital. This policy addresses information originated, modified, stored, transferred, and/or recovered electronically and non-electronically.

Federal and State regulations require organizations to adhere to numerous record retention mandates. The appropriate time periods for record retention are fact specific and are subject to ongoing statutory and regulatory changes. Therefore, data owners will develop a data management plan, in accordance with policy.

Citadel Servicing Corporation requires that its records be maintained in a consistent and logical manner and be managed so that the company:

- Meets legal standards for protection, storage and retrieval,
- Protects the privacy of the company's employees, customers, and vendors,
- Optimizes the use of space,
- Minimizes the cost of record retention; and
- Destroys outdated records in an appropriate manner.

Data owners that maintain organizational records are responsible for establishing appropriate record management procedures and practices. Each data owner or a designee must:

- Be familiar with the corporate data retention policy,
- Educate staff within the department in understanding sound record management practices,
- Restrict access to confidential records and information; and
- Coordinate the destruction of records as provided in the applicable procedures.

Electronic Media Storage of Cardholder Data

Type of Cardholder Data	Business Justifications/Requirements for Retention of Cardholder Data
▪ Primary Account Number ▪ Expiration Date ▪ Service Code	Can only be stored while waiting for an authorization.
▪ Cardholder Name	Can only be stored while waiting for an authorization. If not stored along with the PAN, the cardholder's name can be kept for 1 year.
▪ Full Magnetic Strip/Track Data (Track 1 and Track 2) ▪ Card Verification Code or Value CID, CAV2, CVC2, CVV2 Codes ▪ Pin and Pin Block	Cannot be stored.

Hard Copy Format Storage of Cardholder Data

Type of Cardholder Data	Business Justifications/Requirements for Retention of Cardholder Data
▪ Primary Account Number ▪ Expiration Date ▪ Service Code	Paper copies of forms that contain the PAN, cardholder name, expiration date or service code may be kept for a period of one week to allow time to enter the transaction. The information must be secured at all times and destroyed after processed.
▪ Cardholder Name	Printed receipts should only contain the truncated PAN and cardholder name. The receipts must be securely stored and destroyed one year after the close of the fiscal year.
▪ Card Verification Code or Value CID, CAV2, CVC2, CVV2 Codes ▪ Pin and Pin Block	Cannot be stored.

27.5.2. Confidentiality Requirement

Many records subject to record retention requirements contain confidential information (non-public information including, but not limited to, name, address, social security number, bank account numbers, financial information, etc.). Such records are protected by federal, state, and local statutes. In addition to the statutory requirements, any record that contains confidential information will be treated in accordance with corporate data class protection policies.

27.5.3. Electronically Stored Information

Recent years have witnessed a tremendous growth in the use of electronically stored information ("ESI"). The ease with which ESI may be created, the number places where ESI may be stored, and new rules regarding the use of ESI in litigation, all require that the organization manage its ESI effectively, efficiently, and consistent with Citadel Servicing Corporation legal obligations.

27.5.4. Disposal and Destruction of Records

If it is determined that, consistent with this policy, and with the records management practices and procedures applicable to the department, it is appropriate to dispose of any record, they can be destroyed in one of the following ways:

- Recycle non-confidential paper records.
- Shred or otherwise render unreadable confidential paper records.
- For electronic media stored on information systems that are no longer in use, data is to be disposed of through any one of the following procedures:
    - Disintegration by certified vendor under contract.
    - Shredding (disk grinding device) or pulverization, by certified vendor under contract.
    - Incineration by a licensed incinerator.

27.5.5. Data Transport and Transmission

Transmission of electronic data will be in accordance with Citadel Servicing Corporation policies and align with, but not limited to, the following company policies:

- Information Security Program Policy
- Workstation Security Policy
- Mobile Device Policy
- Data Class and Protection Policy
- Data Encryption and Device Control Policy
- Remote Access Policy
- Wireless Communication Policy
- Account Management Policy

The physical transportation of electronic media will be in adherence to, but not limited to, the following corporate policies:

- Data Class and Protection Policy
- Mobile Device Policy
- Remote Access Policy
- Data Encryption and Device Policy

The physical transportation of physical documents will be treated in accordance with Citadel Servicing Corporation Data Class and Protection policy. Based on data classification, appropriate shipment tracking and packaging will be utilized.

27.5.6. Personally Identifiable Information (PII) Data

Use of PII data within Citadel Servicing Corporation is classified as Confidential and this data will be managed (including destruction) as per the handling procedures for this classification level.

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 PII's data owner/partner.

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.

The storage of PII-related data must be limited to designated Citadel Servicing Corporation 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 Citadel Servicing Corporation systems and data.

If any incident occurs that involves PII data, Citadel Servicing Corporation is required to notify the PII data owner/partner within twenty-four (24) hours of the incident involving their data.

27.6. 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.