DATA BACKUP AND STORAGE POLICY

2022

15. DATA BACKUP AND STORAGE POLICY

POLICY STATEMENT

Citadel Servicing Corporation recognizes that confidentiality, integrity, and availability of data is critical to continuity of business operations and adherence to mandated compliance requirements.

It is company policy to backup and retain copies of company records and software to ensure that computer operating systems, applications, and company data are available to restore business operations in the event of a disruption. This policy is designed to comply with state and federal laws and regulations governing the creation, maintenance, retention, and recovery of data backups.

15.1. OVERVIEW

Data may become negatively impacted due to a variety of risks ranging from malicious intent, human error, system compromise, physical damage, disaster, or any business disruption. It is essential that standardized practices are developed, validated, and adhered to ensure data is effectively backed-up, secured, and recoverable. Citadel Servicing Corporation recognizes that this is critical for maintaining critical operations and compliance with mandated requirements regarding protecting and restoring business systems and data. Citadel Servicing Corporation has established a formalized policy for backup and storage of data which includes:

- A comprehensive backup strategy.
- A process for data backup creation, cataloging, storage, and recovery.
- Secure on and off-site storage for critical data assets.
- Data loss prevention in case of accidental deletion, corruption of data, system failure, or disaster.
- Timely restoration of archived data in the event of a disruption or incident.

15.2. PURPOSE

This policy defines and establishes the requirements for backing up, maintaining, and recovering Citadel Servicing Corporation data to ensure that all data is retained, secured, and recoverable. This policy adheres to industry standards and takes into account all state and federal laws and regulations in maintaining and retaining a backup of all business and client data.

15.3. SCOPE

This policy applies to all Citadel Servicing Corporation computer systems and facilities, including those managed for Citadel Servicing Corporation and its customers. This policy applies to all employees, partners, contractors, consultants, other workers, and third-parties with access to company information assets. All systems and data within Citadel Servicing Corporation will adhere to these data backup and storage standards unless approved by management.

A stand-alone “Record Retention Policy” exists to address Federal and GSE recordkeeping and record retention requirements. Therefore, this policy primarily addresses Information Technology (IT) related record back up, maintenance, recovery requirements and methodology.

15.4. 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.

15.5. TRAINING

All policies regarding data backup and storage will be communicated to all employees, contractors, and business associates who have been granted access to the corporate network, media, and data.

15.6. POLICY

This policy extends to all company data backup and storage operations. Citadel Servicing Corporation employs a comprehensive strategy to ensure there are copies of data readily available at all times which cover the following:

- Original production data
- Local disk backups
- Remote backups (e.g., Data Center & Cloud Storage)

Backups occur on scheduled timelines and before any devices are moved or transferred.

15.6.1. General Guidelines

Citadel Servicing Corporation 's data backup and storage policy will follow, but are not limited to the following guidelines:

A. Only authorized personnel may execute or administrate backup and restore operations.
B. Backups of all records and software must be retained so that computer operating systems and applications are fully recoverable.
C. All critical data is replicated to be available for recovery in the advent of an incident and/or disaster that impacts normal operations.
D. All backup systems and media are logically and physically secured.
E. A limited number of authorized personnel have access to the backup applications and media.
F. All backups will be retained indefinitely via yearly backups (stored off-site).
G. Backup logs will be retained for at least 1 year.

15.6.2. Information Classification

All Citadel Servicing Corporation data backed up will adhere to standards as outlined under state and federal laws (e.g., Gramm-Leach-Bliley Act) and industry regulatory requirements (e.g., PCI DSS). The backup and recovery process for each system and/or set of data must align with the mandated requirements. These processes must be documented and approved for appropriateness.

Information determined to be of a sensitive or confidential nature must be protected from unauthorized access, disclosure, use, modification, recovery, and destruction. Any backup data stored on any medium will be protected from unauthorized access and disclosure using encryption and security methods approved by the Information Security Office.

Data that is determined to be non-critical (e.g., public data that can be seen without any harm to Citadel Servicing Corporation or its customers) may be stored on the local hard drive and backed up locally to CD, DVD, Flash Drive,

external hard drives, or other portable electronic media. All other data outside of these criteria must be stored utilizing the company's backup procedures either on a network server or cloud-based service, aligning with the standards and regulations as set out by state and federal statutes.

15.6.3. Personally Identifiable Information (PII)

As per the requirements of state and federal laws (e.g., Gramm-Leach-Bliley Act) and industry requirements (e.g., PCI DSS), use and storage of Personally Identifiable Information (PII) data within Citadel Servicing Corporation 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 corporate systems and data.

Any PII data stored on backup media will be limited to access by designated, authorized personnel only. All backup media containing any PII data will be encrypted to ensure protection of that data.

15.6.4. Cloud Services

Where cloud services (e.g., AWS) are employed to store and backup company data, Citadel Servicing Corporation will ensure that backup and recovery process and requirements using these services will be properly documented for each system and/or set of data resting on these services. The backup to cloud services will be done following Citadel Servicing Corporation 's approved procedures. Citadel Servicing Corporation will work with the service provider to ensure the integrity and recoverability of the data stored on the cloud service. Data stored on cloud services will follow the same guidelines in accordance with the following corporate policies:

- Data Class and Protection
- Data Retention
- Information Disposal

15.6.5. Scheduling

The frequency (multiple times per day, daily, weekly, and monthly) and extent/type of backups (full or incremental) must be determined and documented based on the criticality or importance of the information and the associated risk to Citadel Servicing Corporation , should data be either temporarily or permanently unavailable. The maximum amount of time Citadel Servicing Corporation can realistically be without the data must also be a consideration.

The following scheduling guidelines will by employed:

A. All Citadel Servicing Corporation data will be backed up at least daily.
B. Data replication for use in disaster recovery scenarios will occur at least daily.
C. Full backups will occur at least weekly.
D. Incremental backups will be performed as necessary.
E. Backup jobs will be formally scheduled and ad-hoc backups may occur if appropriately approved (failure or request) by management.

15.6.6. Backup Labeling for Data Security

Data will be protected in alignment with Citadel Servicing Corporation 's data class and protection policies. To facilitate appropriate protection, backups must have at a minimum the following identifying criteria that can be readily identified by labels / e-labels:

- System Name
- Creation Date
- Point of Contact Information

15.6.7. Monitoring

Citadel Servicing Corporation will take the following steps to ensure that corporate backup procedures and tasks are being completed:

- **A.** Documentation of backup monitoring requirements for success or failure to ensure that backups conducted are complete with actions clearly documented to be taken in the event of unsuccessful backup or backup error.
- **B.** The IT department will monitor backup operations, checking, on a daily basis during the work week, to ensure backups are running properly.
- **C.** Re-run manually, the next working day, any continuing failed backups.
- **D.** Contacting, as necessary, vendor service/support to troubleshoot any problems or issues.
- **E.** Review regularly backup and recovery documentation, updating, as required, to account for new technology, business changes, and migration of applications to alternative platforms.
- **F.** Test recovery procedures on a periodic basis to ensure backups are recoverable.

15.6.8. Off-site Location Security

Critical backup data must be stored off-site. Physical access controls implemented at off-site backup storage locations must meet or exceed the physical access controls of the source systems. Additionally backup media must be protected in accordance with the highest sensitivity level of information stored. Procedures between Citadel Servicing Corporation and the off-site backup storage vendor(s) if implemented must be reviewed at least annually, and in accordance with Citadel Servicing Corporation 's vendor management and third-party security policies.

15.6.9. Testing and Review

Restoration of backups will be periodically tested within a reasonable time frame to ensure the backups are recoverable. These tests can be done in conjunction with testing of Citadel Servicing Corporation 's Disaster Recovery and Business Continuity Plans.

- **A.** **Backup Review** — Department managers or their delegates must ensure that proper backups of sensitive, critical, and valuable data are being made if such data is resident on personal computers, workstations, or other small systems in their area.
- **B.** **Backup Information Review** — Ensure all files and messages stored on company systems are routinely copied to tape, disk, and other storage media and are recoverable.
- **C.** **Backup Media Storage Review** — Each location that is used to store company media backups must be reviewed to determine that the backup media storage is secure. For media stored with off-site backup vendor(s), the procedures between the organization and the vendor(s) must be reviewed at least annually, and in accordance with corporate vendor management service provider policies.

15.6.10. Disposal of Backup Data

Disposal of backup data must be in accordance with the following corporate policies:

- Data Class and Protection
- Data Retention
- Information Disposal

15.7. 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.