DATA LOSS PREVENTION POLICY

2022

28. DATA LOSS PREVENTION POLICY

POLICY STATEMENT

Citadel Servicing Corporation 's Information Technology resources exist for the purpose of conducting legitimate business for the company. Citadel Servicing Corporation is bound by state and federal law to protect certain information that is transmitted using corporate IT systems, hardware, and networks. Pursuant to these objectives, the company has a duty to actively prevent the loss of protected information.

It is the policy of the Citadel Servicing Corporation to engage in sustained and substantial efforts to provide for the confidentiality and integrity of protected information; to promptly discover and remedy any security breach or misuse of Information Technology resources; and to expeditiously take those measures needed to reduce the probability of a security breach or a misuse of those resources.

28.1. OVERVIEW

Sensitive information must be protected regardless of its form, whether electronic, hard copy or intellectual. Rules and requirements regarding data loss prevention (DLP) and digital rights management 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.

28.2. PURPOSE

Citadel Servicing Corporation must protect restricted, confidential or sensitive data from loss to avoid reputation damage and to avoid adversely impacting clients, employees, and the company. The protection of in-scope data is a critical business requirement, yet flexibility to access data and work effectively is also critical. This policy establishes the principles, by which Citadel Servicing Corporation will identify, protect and respond to the unauthorized disclosure of protected information by electronic means. The specific purposes of this policy are to:

- **A.** Further enable and affirm the responsibilities of the Information Security Office for monitoring and reporting compliance with corporate policy.
- **B.** Authorize Citadel Servicing Corporation Information Security Office to take reasonable measures to secure protected information by using, among other techniques and methods, Data Loss Prevention (DLP) software and equipment to monitor, identify and block the unauthorized disclosure of Protected Information.
- **C.** Prescribe mechanisms that help to identify and address areas of high risk for the unauthorized release of protected information and the misuse of data, applications, the company's networks and computers; and
- **D.** Further reduce the risk of exposure and identity theft when personal identifying information (e.g., Social Security Number, Credit Card information) is used by Citadel Servicing Corporation as a primary identifier and to provide for the consistent, secure and proper management of such information.

28.3. SCOPE

The scope of this policy includes all Citadel Servicing Corporation 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 regardless of where such data may be located.

28.4. 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.

28.5. POLICY

28.5.1. Employee Requirements

A. Employees will not use systems or communication channels (e.g., SMS, e-mail) not controlled by Citadel Servicing Corporation to distribute sensitive or confidential data. Employees will not reference the subject or content of sensitive or confidential data publicly or via systems not controlled by the company. Exceptions are secure contract service environments such as Box.com, and integrated affiliates or service providers. These are documented processes and may be integrated directly with system automation (e.g., automated file transfers, document generation, etc.), or manually initiated.

B. Employees need to use a secure password on all systems as per the corporate Password Security Policy. These credentials must be unique and must not be used on other external systems or services.

C. Terminated employees will be required to return all records, in any format, containing personal information. This requirement will be part of the employee onboarding and departure processes with employees signing documentation to confirm as required.

D. Employees must immediately notify IT personnel and their manager in the event that a device containing data is lost (e.g., mobile phones, laptops etc.).

E. In the event that employees find a system or process which is suspected not compliant with this policy or the objective of information security, they must notify their manager or the IT Department, so appropriate action can be taken.

F. For employees working remotely, they must follow corporate remote access and wireless communication policies to ensure that data is appropriately handled and protected.

G. Any information being transferred to or from an approved portable device (e.g., USB stick, laptop, tablet, etc.) must be encrypted in line with industry best practices and applicable law and regulations.

H. If these requirements are unclear due to your job duties or you have questions regarding the requirements, seek guidance from your supervisor, or contact IT Technical Support.

28.5.2. Data-in-Motion

A. Where technically feasible, and supported, a professional Data Loss Prevention (DLP) solution will be implemented and configured to identify data in motion to Browsers, IM Clients, E-mail clients, Mass storage devices and writable CD/DVD media etc.

B. DLP technology will scan for data-in-motion. DLP will identify specific content such as, but not limited to;

- E-mail addresses, names, addresses and other combinations of personally identifiable information.
- Documents that have been explicitly marked or identified with a ‘Confidential’ string.

C. The DLP will be configured to alert the user in the event of a suspected transmission of sensitive data, and the user will be presented with a choice to authorize or reject the transfer. This allows the user to make a sensible decision to protect the data, without interrupting business functions.

D. The DLP will log incidents centrally for review. First level triage conducted on events will identify data that may be sensitive and situations where its transfer was authorized and there is a concern of inappropriate use.

E. Access to DLP events will be restricted to a named group of individuals to protect the privacy of employees.

28.5.3. Endpoints and Workstations

A. All laptop and desktop in scope will have full disk encryption enabled.

B. Citadel Servicing Corporation Acceptable Use Policy (AUP) and Information Security Awareness Training Program(s) require users to notify the company (e.g., your supervisor, or IT Technical Support) if they suspect that they are not in compliance with this policy as per the AUP.

C. Where automated technical management is not possible and a standalone encryption is configured (pre-approved by a risk assessment), the device owner/user must provide a copy of the active encryption key to the IT Department.

D. The encryption technology must be configured in accordance with industry best practices and legal requirements and regulations to be hardened against attacks.

28.5.4. Security Reviews

Scope

Based upon a determination made by Citadel Servicing Corporation IT Management, may:

a) Access and examine company-issued or approved BYOD computers and other devices, data resources and all data (whether Data-In-Motion, Data-At-Rest, or Data-In-Use) utilizing Information Technology resources in any manner whatsoever.

b) Monitor company network activities of individual computer users.

c) Conduct a forensic analysis of systems and resources, and the frequency and usage of such systems and resources.

28.5.5. Probable Violations

Confirmation

In the event that IT personnel identify or are made aware of a probable violation of a policy through the misuse of an IT resource, the Information Security Office will be notified to review and analyze the incident. If it is identified that a probable violation has occurred or is likely to occur, the Information Security Office will promptly notify senior company management.

Notifications

Upon receiving a notification, company senior management will then determine if additional notifications are needed and send to the appropriate party/parties.

In the event of a suspected criminal activity or possible data breach, the company's legal department will be promptly notified.

28.5.6. Confidentiality

Confidentiality Agreements

IT personnel having knowledge of or access to, the equipment, software, data or methods will be required to sign a Confidentiality Agreement as a condition of employment and continued employment by Citadel Servicing Corporation . Such an agreement will be in a form and substance as mutually agreed upon by company management and in accordance with all state and federal employment regulations. The agreement will be maintained by Human Resources and reviewed annually.

No Expectation of Privacy

Persons who use Citadel Servicing Corporation IT systems for data storage, data transmission or data dissemination or for the processing of data will not expect that;

a) Such data is private and only accessible by them; or
b) That such data is exempt from retrieval, monitoring or analysis under this policy. Citadel Servicing Corporation may take actions authorized under this policy with or without prior notice.

28.5.7. Distribution and Training

Citadel Servicing Corporation will ensure that this policy is distributed to all supervisors and managers under their direct or indirect supervision. The Information Security Office will be responsible for devising and implementing such employee training programs and information as the company believes necessary and appropriate to effectively implement this policy.

28.5.8. Operating Procedure

The Information Security Office will adopt such operating procedures to implement this policy as may be appropriate, provided that, such operating procedures are not in conflict with any provision of this policy or any other company policy, and are made readily available to all employees.

28.5.9. Amendments

This policy and supporting procedures may be amended at any time by Citadel Servicing Corporation in accordance with company policies and to meet any industry or legal requirements.

28.6. 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.