DATA ENCRYPTION AND DEVICE CONTROL POLICY

2022

9. DATA ENCRYPTION AND DEVICE CONTROL POLICY

POLICY STATEMENT

It is Citadel Servicing Corporation 's policy to use data encryption and a series of controls in order to protect restricted, confidential, and sensitive data from loss; to avoid reputation damage; and to avoid adversely impacting our customers in compliance with state and federal laws and regulations.

9.1. OVERVIEW

Data encryption and device controls are established to prevent the loss of confidentiality, integrity, or availability of Citadel Servicing Corporation's corporate and client data/information. The design and implementation of data encryption and device controls depends on many factors, including types and classification of data, types of computing devices, the quantity of media, and the type and method used to communicate the data.

Citadel Servicing Corporation has established controls for data encryption, data transmission, data removal, and device assignment in order to prevent the loss and compromise of confidential company and client information.

9.2. PURPOSE

The purpose of this policy is for Citadel Servicing Corporation to take reasonable and appropriate steps to ensure that encryption and decryption be utilized, where appropriate, as the principal means of access control and security protection for corporate and client data.

Citadel Servicing Corporation will take reasonable and appropriate steps to apply encryption mechanisms when deemed necessary to ensure that data sent is protected against unauthorized alteration or destruction during transmission over electronic communications networks or via any form of removable media.

9.3. SCOPE

The policy applies to all employees, contractors, consultants, temporary employees, and other entities at Citadel Servicing Corporationincluding all personnel affiliated with third parties. This policy applies to all company computer systems and facilities, including those managed for company customers.

This policy covers all computer and communication devices owned or operated by Citadel Servicing Corporation and includes all electronic communication mediums as well as all storage media.

9.4. 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.

9.5. POLICY

9.5.1. Data Encryption

A. Whenever possible, Citadel Servicing Corporation will use encryption to protect corporate and client data when:

- Stored on company and company-controlled networks and systems.
- During transmission over electronic and digital communications networks. If encryption is not suitable, another secured transmission mechanism, such as a virtual private network or secured portal or tunnel, must be used.

B. Any unauthorized access to or disclosure of unencrypted data is by definition a security breach and must be investigated, reported, and documented in accordance with corporate security policies and computer incident response policies.

C. The Information Security Office will approve the encryption methods used to protect corporate/client data stored on devices and systems and when the data is transmitted over an electronic and digital communications network.

D. Citadel Servicing Corporation will provide employees with training and awareness regarding encryption methods implemented to protect data from theft, unauthorized alteration, or destruction.

E. Media and devices will utilize encryption and decryption as the primary mechanism to protect data from unauthorized disclosure. Encryption and Decryption may also be utilized in combination with other access controls where indicated by risk analysis.

F. Data at rest on computer systems owned by and located within company-controlled spaces and networks must be protected by encryption with strict access controls, in accordance with corporate data class protection policies, that authenticate the identity of those individuals accessing the specific system or data.

G. Citadel Servicing Corporation will employ, where technically feasible and viable, the encrypting of critical databases and file servers as well as corporate/client data on mobile devices such as laptops and tablets. It is strongly recommended that any mobile technologies that access, store or transmit corporate/client data employ full disk encryption to protect the integrity of the data stored on those devices.

H. Citadel Servicing Corporation will ensure encryption endpoints are physically and logically secured from inappropriate access, in adherence to corporate access administration, malicious software management, and security zone policies and procedures.

9.5.2. Device Control

A. Citadel Servicing Corporation maintains a record of the movements of hardware, devices, and electronic media and persons responsible for such items. Citadel Servicing Corporationensures that an individual is responsible for, and records the receipt and removal of, hardware, devices, and software with data.

B. All devices and media used by Citadel Servicing Corporation will be stored in a safe, secure environment in accordance with the manufacturer's specifications as well as all legal and regulatory requirements.

C. Citadel Servicing Corporation has the ability to create or maintain a retrievable, exact copy of corporate/client data, when needed, before movement or reassignment of equipment. Citadel Servicing Corporation ensures that an exact, retrievable copy of the data is retained or available and protected to safeguard the integrity.

D. Citadel Servicing Corporation has implemented policies and procedures to address the final disposition of corporate and client data, and/or the hardware, devices or electronic media on which it is stored. Citadel Servicing Corporation has determined, approved, and documented appropriate methods to dispose of hardware, devices, software, and the data itself. Citadel Servicing Corporationensures through this process that the data is properly destroyed and cannot be recreated prior to disposal.

9.5.3. Transmission Security

Citadel Servicing Corporation is responsible for corporate/client data being transmitted inside/outside of Citadel Servicing Corporation ’s controlled networks/removable media and must use appropriate mechanisms and procedures.
Citadel Servicing Corporation will use encryption wherever possible to protect against the risks and costs of a security breach of unsecured (unencrypted) corporate/client data. All encryption mechanisms implemented to comply with this standard must support a minimum of 128-bit encryption.

Methods used to protect corporate/client data during transmission must be approved by Management and the Information Security Office.

A. **Electronic Data in Transit** — Data utilized that is accessed or transmitted locally, on Citadel Servicing Corporation 's network, on an outside network, or over the internet, is considered data in transit. Data that is transmitted through email or FTP or through web applications are also considered data in transit. As such, identification of whether or not the network is trusted impacts encryption requirements.

B. **Trusted Network Encryption** — The internal network is considered trusted and as such, no encryption is required. Therefore, authorized users accessing data on the internal network do not require encryption. Communications with external entities over trusted networks (e.g., vendor or partner-provided leased line connection) are considered secured and as such no encryption is required. In accordance with corporate policies, utilization of VPN technologies to create a secure encrypted tunnel, do not require additional encryption.

C. **Un-trusted/Public Network Encryption** — Communications of confidential information over un-trusted/public networks must be encrypted. This includes networks where trust cannot be assured (i.e., site-to-site VPN connections). Communication interfaces between Citadel Servicing Corporation 's trusted networks and un-trusted networks will reside in an approved area such as Citadel Servicing Corporation's DMZ or Business Partner Network. All new network connections over un-trusted networks must be encrypted when critical or sensitive information such as customer non-public personal information is being transmitted.

D. **Email Communications** — Email communications sent that contains sensitive business and customer information must be encrypted.

E. **Data File Transfer** — File transfer of information within Citadel Servicing Corporation does not need to be encrypted. File transfer of sensitive business or customer information that is external to Citadel Servicing Corporation(whether at point of origin, point of delivery or communications channel) will use secure file transfer methods and 128-bit encryption at a minimum. Specific requirements for wireless devices are addressed in corporate wireless security policies.

9.6. ENFORCEMENT

All users (employees, contractor, part-time and temporary employees) 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.