PHYSICAL SECURITY POLICY

2022

24. PHYSICAL SECURITY POLICY

POLICY STATEMENT

Citadel Servicing Corporation will ensure that standards are established and in place to govern and control physical access to all company locations and facilities. This is to ensure a system of physical security to prevent unauthorized access to company facilities, information technology systems, and data.

24.1. OVERVIEW

Physical controls must exist to protect information assets and systems from unauthorized access and safeguard against threats. Appropriate physical access control methods are needed to protect the full lifecycle of company information, systems, and assets from insider and outsider threats.

It is important for Citadel Servicing Corporation to establish and enforce physical security rules and requirements. All employees must comply with established standards regarding appropriate access to company facilities, company IT systems, and data.

24.2. PURPOSE

The purpose of this policy is to prevent unauthorized access to sensitive areas, systems, resources, and physical/electronic information. Citadel Servicing Corporation will take reasonable and appropriate steps to ensure that individuals and/or entity identities are validated and restrict individuals and/or entities that are not authorized to access Citadel Servicing Corporation 's locations and facilities. This policy defines the requirements for establishing physical and logical access controls at Citadel Servicing Corporation locations.

24.3. SCOPE

This policy applies to physical access to Citadel Servicing Corporation computer systems and facilities, including those managed for company customers. This policy applies to all employees, partners, contractors, consultants, other workers, outsourced services providers and third-parties (and all personnel affiliated with third parties) with access to company locations and information assets.

24.4. 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.

24.5. POLICY

Citadel Servicing Corporation employs a number of controls and barriers to ensure the protection of Citadel Servicing Corporation 's facilities and its employees. This policy is to provide direction and guidance for management and staff in controlling access to company offices and facilities.

24.5.1. Access Control

A. **Physical Access Control to Sensitive Information** — Access to every office, computer room, and work area containing sensitive systems and information must be physically restricted to unauthorized persons.
B. **Access to Computers and Communications Systems** — Buildings that house Citadel Servicing Corporation computers or communications systems must be protected with physical security measures that prevent unauthorized persons from gaining access.
C. **Unauthorized Physical Access Attempts** — Employees must not attempt to enter restricted Citadel Servicing Corporation facilities for which they have not received access authorization.
D. **Terminated Worker Access to Restricted Areas** — Whenever an employee terminates their working relationship with Citadel Servicing Corporation , all access rights to Citadel Servicing Corporation facilities and locations must be revoked.

24.5.2. Access Control Monitoring

A. **Physical Access Monitoring – Method** — Key FOBs or other access control mechanisms that monitor the entry and exit points to secure areas must be in place.
B. **Physical Access Monitoring – Security** — Key FOBs or other access control mechanisms that monitor secure areas must be protected from tampering and disabling.
C. **Physical Access Badge Procedures** — Procedures must be developed and implemented that control the issuance, modification, and revocation of Citadel Servicing Corporation physical access badges.
D. **Physical Access Badge System Access** — Access to the system that controls Citadel Servicing Corporation physical access key FOBs must be limited to only those employees with the responsibility to issue, modify, or revoke physical access badges.
E. **Securing Propped-Open Computer Center Doors** — Whenever doors to the computer center are propped-open, the entrance must be continuously monitored by an employee or a contracted guard.

24.5.3. Access Badges

A. **Badge-Controlled Access** — Each person must present his or her badge to the badge reader before entering controlled areas/doors within Citadel Servicing Corporation premises.
B. **Badge Access Sharing** — Employees must not permit unknown or unauthorized persons to pass through doors, gates, and other entrances to restricted areas.
C. **Individuals without Access Badges** — Individuals without Citadel Servicing Corporation Key FOBs must be questioned and if they cannot produce acceptable ID, they must be escorted to the receptionist/security desk.
D. **Temporary Badges** — Employees who have forgotten their Key FOBs must obtain a one-day temporary Key FOB by providing a driver's license or another piece of picture identification.
E. **Revoking Controlled Access** —Key FOBs of terminated employees and contractors are immediately revoked.

24.5.4. Visitors

A. **Visitor Identification** — All visitors to Citadel Servicing Corporation must show picture identification prior (e.g., valid government issued ID) to the person at the front desk gaining access to restricted areas.
B. **Third-Party Physical Access** — Visitor or other third-party access to Citadel Servicing Corporation offices, computer facilities, and other work areas containing sensitive information must be controlled by guards, receptionists, or other staff.

C. **Escorting Visitors** — Visitors to Citadel Servicing Corporation offices including, but not limited to, customers, former employees, worker family members, equipment repair contractors, package delivery company staff, and police officers, must be escorted at all times by an authorized worker.
D. **Visitor Log – Contents** — A visitor log must be maintained at the front desk containing the visitor's name, the firm represented, and the employee authorizing access to any Citadel Servicing Corporation facility.
E. **Visitor Log – Retention** — Visitor logs must be retained for a period of at least one year.
F. **Third-Party Supervision** — Individuals who are not Citadel Servicing Corporation employees, authorized contractors, or authorized consultants must be supervised whenever they are in restricted areas containing sensitive information.
G. **Repair People Who Show Up Without Being Called** — Every third-party repair person or maintenance person who shows up at Citadel Servicing Corporation buildings and facilities without being called by an employee must be denied access to the facilities. All such incidents must be promptly reported to the Information Security Office.
H. **Unescorted Visitors** — Whenever an unescorted visitor is observed in restricted areas, he/she must be questioned about the purpose for being in the area and escorted to a reception desk, a guard station, or the person they came to see.
I. **Data Center and Information Systems Department Visitors** — Visitors who do not perform maintenance on Citadel Servicing Corporation equipment must not access the data center or the Information Systems Department areas.

24.5.5. Access Review

A. **Data Center Staff Access** — A complete list of all employees who are currently authorized to access the data center must be maintained, reviewed, and updated periodically.
B. **Physical Access Monitoring – Data Review** — The data that is produced by video cameras or other access control mechanisms that monitor secure area entry and exit points must be monitored and secured.

24.5.6. Testing

A. **Testing of Physical Security Perimeter** — Citadel Servicing Corporation or an authorized independent third party will perform a comprehensive testing of the physical security controls of each location at least annually. This testing includes physical access controls, physical access monitoring controls, and logging controls (at a minimum).
B. **Third-Party Physical Penetration Testing Required** — Citadel Servicing Corporation must hire a qualified, independent third party to conduct a physical security penetration test at least once a year.

24.6. 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.