CITADEL
SERVICING CORPORATION

REMOTE ACCESS POLICY

2022

6. REMOTE ACCESS POLICY

POLICY STATEMENT

Citadel Servicing Corporation will establish standards guidelines outlining the use and management of remote access to the corporate network. Remote access tools and privileges will be managed and monitored to ensure that they are not exploited or compromised. Corporate network users will ensure that their remote access connection is given the same security considerations as an on-site connection to the corporate network would.

6.1. OVERVIEW

Remote desktop software, also known as remote access tools, provide a way for computer users and support staff alike to share screens, access work computer systems from home, and vice versa. Examples of such software include LogMeIn, GoToMyPC, VNC (Virtual Network Computing), and Windows Remote Desktop (RDP).

While these tools can save significant time and money by eliminating travel and enabling collaboration, they also provide a back door into the Citadel Servicing Corporation network that can be used for theft of sensitive or company confidential data, intellectual property, damage to public image, damage to critical Citadel Servicing Corporation internal systems, unauthorized access to, or destruction of assets.

Only approved, monitored, and properly controlled remote access tools may be used on the Citadel Servicing Corporation computer systems.

6.2. PURPOSE

This policy defines the requirements for establishing the framework and ongoing management of Citadel Servicing Corporation remote access infrastructure. The purpose of this policy is to define standards for connecting to Citadel Servicing Corporation ’s network from any host from any location and the results from unauthorized use of corporate resources.

6.3. SCOPE

The scope of this policy includes all employees, contractors, consultants, temporary employees, and other entities at Citadel Servicing Corporation including all personnel affiliated with third parties. This policy applies to all company-owned or personally-owned (BYOD) computers or workstations used to connect to the corporate network.

This policy applies to remote access connections used to do work on behalf of Citadel Servicing Corporation . Remote access implementations that are covered by this policy include, but are not limited to; dial-in modems, DSL, VPN, SSH, and cable modems.

6.4. 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.

6.4.1. Programs

A. **Remote Access Strategy Development** — Prior to permitting or implementing any remote access to Citadel Servicing Corporation computer and communications systems, a detailed analysis must be performed that includes an examination of the risks associated with each solution.

B. **Remote Access Strategy Testing** — Before implementing a remote access solution, a prototype of the design must be tested and evaluated for security and performance compatibility.

C. **Software and Hardware** — All software and hardware used for remote access to Citadel Servicing Corporation computer and data networks must be approved by the Information Security Office to meet the standards and requirements of this policy.

6.4.2. Server Configuration

A. **Remote Access Server Isolation** — Citadel Servicing Corporation remote access servers must not be run on the same host as other services and applications.

B. **Remote Access Server Placement** — Remote access servers must be placed on the network perimeter behind the firewall and only accessed through VPN, unless there are compelling reasons to do otherwise.

6.4.3. Authentication and Access

A. **Remote Access Passwords** — User IDs with blank or null passwords (passwords with no characters) must not be permitted to gain remote access to any Citadel Servicing Corporation computer or network.

B. **Privilege Restriction – Need To Know** — The computer and communications system privileges of all users, systems, and programs must be restricted based on the need to know.

C. **Two-Factor User Authentication** — All in-bound access through a public network to every Citadel Servicing Corporation computer must employ two-factor user authentication (including pre-shared tokens/certificates) with at least one of the factors not subject to replay.

6.4.4. Data Integrity

A. **Secret Data Transmission** — All Citadel Servicing Corporation data classified as confidential or secret transmitted over any communication network must be encrypted.

B. **Standard Encryption Algorithm and Implementation** — If encryption is used, government-approved standard algorithms and standard implementations must be consistently employed. VPN (Virtual Private Network) technology will be employed to provide a secure and encrypted tunnel between the user and corporate network. Remote Access to the organization's private network via wireless devices, are addressed in the corporate wireless communication policy. Multi-factor authentication will be used by employees when connecting using VPN.

6.4.5. Server and Device Management

A. **Remote Access Server and Device Security** — All Citadel Servicing Corporation remote access servers and devices must be kept fully patched, operated using an organization-defined security configuration baseline, and only managed from trusted hosts by authorized administrators.

B. **Remote Access Client Software Management** — Remote access client software must be configured to have all security features and settings remotely managed by an Citadel Servicing Corporation system administrator.

C. **Remote Access Client Device Support** — Help desk personnel must be properly trained to support remote access users and the devices that are used.

D. **Remote Administration** — Remote administration of Internet-connected computers must employ secure passwords as per corporate password security policy using encrypted or secure links to connect.

6.4.6. Client Software

A. **Remote Access Client Software Configuration** — Remote access client software must be configured to provide Citadel Servicing Corporation with nearly complete control over the remote access environment.

6.4.7. Device Management and Security

A. **Mobile Device Usage with Corporate Information** — All mobile computing devices used to conduct any Citadel Servicing Corporation business must be provided or approved by Citadel Servicing Corporation , and properly configured with necessary security software.

B. **Remote Access Server and Device Security** — All Citadel Servicing Corporation remote access servers and devices must be kept fully patched, operated using an organization-defined security configuration baseline, and only managed from trusted hosts by authorized administrators.

C. **Remote Client Machines Automatically Disabled If Lost/Stolen** — All portable computers containing Citadel Servicing Corporation information must include software approved by the Information Security Office that will automatically erase the data resident on the machine after the machine has been reported to be lost or stolen.

D. **Personal Computer and Workstation Security** — All personal computers and workstations that connect to the Internet through dial-up, digital subscriber line (DSL), integrated services digital network (ISDN), cable modem, or similar connections must have approved security software (e.g., anti-virus and firewall) installed and continuously enabled.

E. **Remote Access Device Management Training** — All Citadel Servicing Corporation employees who are responsible for the management of any remote access devices must be trained to properly secure these devices.

6.4.8. Data Security

A. **Transportable Computers with Sensitive** Information — All portables, laptops, notebooks, and other transportable computers containing sensitive Citadel Servicing Corporation information must consistently employ hard disk encryption for all files.

B. **Remote Server and Device Disposal** — All sensitive information must be removed from any remote server or device prior to its disposal.

C. **Remote Device Encryption Keys** — The creation and use of cryptographic keys for encrypting data stored on remote devices must follow the same Citadel Servicing Corporation policies for encrypting data stored on non-remote systems.

D. **Using Public Networks** — When transmitting data using public networks, data encryption is required in accordance to corporate encryption policies and standards.

6.4.9. Documentation and Process

A. **Remote Access Device and Access Levels** — A list of approved remote access devices and the permitted access level of each device must be documented, maintained and distributed in a controlled fashion.

B. **Annual Review of Information Security Policy Documents** — All Citadel Servicing Corporation written information security policy documents must be reviewed on an annual basis.

C. **Remote Access Assessments** — Audits or assessments must be performed at least annually to ensure that the Citadel Servicing Corporation remote access policies, processes, and procedures are being followed.

D. **Security Standard for Home User Computers** — The Citadel Servicing Corporation Information Security Office must issue a standard for the security configuration of home computers which employees use for remote access to Citadel Servicing Corporation networks. The standard must include a list of required and prohibited software packages.

6.5. 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.