CITADEL
SERVICING CORPORATION

ANTI-VIRUS SECURITY POLICY

2022

14. ANTI-VIRUS SECURITY POLICY

POLICY STATEMENT

A leading threat to corporate information systems and data is malicious software (e.g., viruses, malware) which has the potential to impact the access and availability of network services and data. These types of threats can undermine the confidentiality, integrity and availability of corporate systems and corporate and client data.

Citadel Servicing Corporation will develop, implement, and periodically review requirements and standards for guarding against, detecting and reporting malicious software posing a risk to corporate/client data and systems.

14.1. OVERVIEW

Citadel Servicing Corporation will develop, implement, and periodically review a documented process for guarding against, detecting and reporting malicious software posing a risk to corporate/client data and systems. Citadel Servicing Corporation ’s malicious software prevention, detection, and reporting procedures will include, but is not limited to:

- Corporate-approved anti-virus software installed and updated on all data devices and systems.
- Procedures for company employees to report suspected or confirmed malicious software (e.g., viruses, malware, trojans).
- Plan for recovering from malicious software attacks.

14.2. PURPOSE

This policy defines the requirements for establishing the controls to prevent and detect the dissemination of any viruses and malicious software on Citadel Servicing Corporation computer and communications systems.

14.3. 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 covers all computer systems and facilities owned or operated by Citadel Servicing Corporation.

14.4. 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.

14.5. TRAINING

Citadel Servicing Corporation will provide periodic training and awareness to its employees about guarding against, detecting, and reporting malicious software. Citadel Servicing Corporation employees and partners will be trained to contact the Information Security Office immediately in the event that any malicious software is detected. This will allow the Information Security Office to investigate and take proper measures and remedial action to avoid the event in the future.

Training and awareness for staff on protection from malicious software will include, for example, the following topics:

- □ How to discover malicious software.
- □ How to report malicious software.
- □ Not to disable anti-virus software or any other protective measures put in place to ensure the safety of the computing environment, such as desktop firewall and laptop encryption.
- □ How to avoid downloading malicious software, including not opening or launching email attachments that may contain malicious software.
- □ Not to install or use unlicensed or pirated software on corporate devices and network.

14.6. POLICY

It is the policy of Citadel Servicing Corporation to effectively secure corporate/client data and networks so that security incidents and breaches are prevented at the source and independent of the type of access.

All 'end' points and network 'entry' points will be protected from, and provide protection to the resources they host or provide access to from malicious software and its effects. All applicable workstations and servers that connect to the internal networks or that process, store, or examine the organization's non-public information will run approved anti-virus security software. This equipment will run the current version with the most recent updates available.

14.6.1. Anti-Virus Configuration

A. **Anti-Virus Software Updates** — All anti-virus programs deployed on Citadel Servicing Corporation computer and communications systems must be configured to accept automatic updates of the software.

B. **Anti-Virus Software Scans** — All anti-virus programs deployed on Citadel Servicing Corporation computer and communications systems must be configured to periodically scan the system for malicious software.

C. **Anti-Virus Software Logs** — All anti-virus programs deployed on Citadel Servicing Corporation computer and communications systems must be configured to log all anti-virus activity.

D. **Anti-Virus Checking Programs** — Anti-Virus checking programs approved by the Information Security Office must be continuously enabled on all local area network servers and networked computers. Those working for Citadel Servicing Corporation or their partners will not bypass or disable anti-virus software and other security measures installed on corporate devices unless properly authorized to do so.

14.6.2. Procedures

A. **Systems Network Access** — Systems without the required software patches or systems that are infected by viruses/malware must be disconnected from the Citadel Servicing Corporation network.

B. **Test System** — Whenever software or files are received from any external entity, this material must be tested for viruses, worms, and other malicious software on a stand-alone non- production machine before it is used on Citadel Servicing Corporation information systems. Where feasible, testing should be automated upon loading software.

C. **Outbound Software and Executables** — All files containing Company authorized software or executable statements must be certified as free of malicious software prior to being sent to any third party.

D. **Decrypting Files for Virus/Malware Checking** — All externally-supplied computer-readable files must be decrypted prior to being subjected to an approved security checking process.

E. **Scanning Downloaded Information** — All software and files downloaded from non-Citadel Servicing Corporation sources through the Internet or any other public network must be screened with malicious software detection software prior to the software being executed or the files being examined through another program.

F. **E-Mail** – E-mails are scanned with malicious software detection software on entry.

G. **Portable Media Scanning** — Users will scan portable media prior to access. Where possible, the security software will be configured to perform scans of new media automatically. The following guidelines will be used:

    - All portable media used to physically transport data from one computer or local area network (LAN) to another will be checked to ensure that the media does not contain copies of executable code; it will contain data files only. Files should be write-protected when possible.

14.6.3. Response

Unexpected errors or actions that are suspected to be an effect of malicious software must be reported immediately to the Information Security Office. If a user observes any unusual activity leading them to suspect a malicious software attack, the user must:

□ Inform the Information Security Office or your manager immediately.

□ Gather any media, external hard drives, CD-ROM disc(s), USB memory stick(s) used for transporting information in or out of the machine and make available to the Information Security Office.

□ Not use the PC (or suspected media) until it has been cleared as being safe to use.

In the case of a malicious software attack the Information Security Office will:

- Document the incident for reporting and escalating as needed.
- Arrange for the following to take place (where appropriate):

    □ Check the infected PC.
    □ Quarantine (e.g., disconnect from network) the infected PC and any other potentially infected devices.
    □ Check any media that has been used with the infected PC.
    □ Check any other PC that the media has been used with.
    □ Delete or clean any infected files.
    □ Check any servers that may also have been accessed.
    □ Try to determine where the virus may have originated.
    □ Ensure the incident is completed within appropriate timescales.
    □ Depending on the severity and impact of the incident a full incident report may be required.
    □ Files that have been identified as infected will be quarantined and the event will be logged. If the file can be safely sanitized, it can be restored. If not, contact the Information Security Office for resolution.

14.6.4. PII Data

For any infected devices that may impact PII-related data, after quarantine and remediation, Citadel Servicing Corporation will require approval from internal and external PII data owners before reconnecting the previously infected device to the network.

14.7. 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.