CITADEL
SERVICING CORPORATION

SECURITY MONITORING POLICY

2022

37. SECURITY MONITORING POLICY

POLICY STATEMENT

It is the policy of Citadel Servicing Corporation to ensure the communications security of devices and data on Citadel Servicing Corporation ’s corporate network by monitoring and conducting regular and periodic security audits of the corporate network system.

The monitoring and audits are designed to ensure integrity, confidentiality, and availability of information and resources, investigate possible security incidents, ensure compliance to corporate security policies, and to monitor user or system activity where appropriate.

37.1. OVERVIEW

To implement and maintain policies and procedures that ensure the effective communication of security processes used to protect Citadel Servicing Corporation ’s valuable information assets.

Citadel Servicing Corporation works to ensure the confidentiality, integrity, and availability of corporate and client data on company devices and systems. Early identification of wrongdoing (attempted or successful), or new security vulnerabilities can prevent wrongdoing before harm can be done or minimize the potential impact.

Citadel Servicing Corporation will establish expectations and accountability to monitor security events to ensure that information asset security controls are in place, are effective, and are not being bypassed. Citadel Servicing Corporation will follow specific procedures for conducting, on a periodic basis, activity reviews that include a review of auditable events.

37.2. PURPOSE

The purpose of this policy is for Citadel Servicing Corporation to establish the rules and requirements for enabling, logging, alerting and monitoring real time security alerts, security logs (automated or manual), as well as various condition monitoring tests and reviews. This policy also addresses documentation requirements toward security incident identification.

Citadel Servicing Corporation will take reasonable and appropriate steps to ensure that hardware, software and/or procedural mechanisms will record and examine information systems activity that contains and uses corporate and/or client data.

The Information Security Office will utilize various software and hardware to perform electronic scans of networks, servers, and/or firewalls or on any system within Citadel Servicing Corporation .

37.3. SCOPE

This policy applies to all company computer systems and facilities, including those managed for Citadel Servicing Corporation This policy applies to all employees, partners, contractors, consultants, other workers, and third-parties with access to company information assets and facilities.

The policy will apply to any computer and communications devices present on Citadel Servicing Corporation ’s premises, but which may not be owned or operated by Citadel Servicing Corporation .

37.4. 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.

37.5. POLICY REQUIREMENTS

37.5.1. General Implementation

A. Citadel Servicing Corporation will use risk assessment to determine the level of monitoring required for its corporate systems and facilities and ensure that all monitoring and logs comply with all relevant legal and industry requirements.

B. Citadel Servicing Corporation will employ system tools to provide notification either via reports or real-time alerts of detected wrongdoing and vulnerability exploitation. Based on the type of event, baseline thresholds will be established and documented in accordance with corporate configuration management policies and risk assessment. The system tools employed will be utilized to monitor, but not limited to, the following events:

- Internet traffic
- Electronic mail traffic
- LAN traffic, protocols, and device inventory
- Authorized access, including detail such as:
  - the user ID
  - the date and time of key events
  - the types of events
  - the program/utilities used
- All privileged operations, such as:
  - use of privileged accounts, (e.g., supervisor, root, administrator);
  - system start-up and stop
  - I/O device attachment/detachment
- Unauthorized access attempts, such as:
  - failed or rejected user actions
  - failed or rejected actions involving data and other resources
  - access policy violations and notifications for network gateways and firewalls
  - alerts from proprietary intrusion detection systems
- System alerts or failures such as:
  - console alerts or messages
  - system log exceptions
  - network management alarms
  - alarms raised by the access control system
- Changes to, or attempts to change, system security settings and controls Operation system security parameters.

C. Citadel Servicing Corporation will employ and maintain audit logs recording user activities, exceptions, and information security events. Logging will be used and maintained for signs of wrongdoing and vulnerability exploitation to assist in future investigations and access control monitoring. All user activities affecting production information must be able to be fully reconstructed from logs. Audit logs will include, when relevant:

- User IDs
- Dates, times, and details of key events, (e.g., log-on and log-off);
- Terminal identity or location if possible
- Records of rejected system access attempts
- Records of rejected data and other resource access attempts
- Changes to system configuration
- Use of system utilities and applications
- Files accessed and the kind of access
- Network addresses and protocols
- Activation and de-activation of protection systems, such as anti-virus systems and intrusion detection systems.

Citadel Servicing Corporation will also employ and maintain other logging activity to support, secure and maintain corporate information systems and data. Other logging that may occur will include, but not limited to the following:

- Intrusion prevention system configuration and logs
- Firewall access and configuration change logs
- Administrative account activity and access logs
- Application account access and activity logs
- Wireless access and activity logs
- Data backup logs
- System error logs
- Network scanning logs
- Logs of all physical access to protected areas, including electronic physical access systems, video monitoring and visitor access recorded on paper.

D. Citadel Servicing Corporation will review, on a periodic basis, records of the activity of its information systems that create, receive, maintain, or transmit corporate and/or client data.

E. Citadel Servicing Corporation will perform security monitoring reviews and/or testing on a scheduled periodic basis to verify continued appropriateness in identified areas, and potentially other areas as well. Evidence of monitoring and review activity and any corresponding test results will be retained in a central location for ease of administration. Such reviews may include, but are not limited to:

- Penetration Testing
- Vulnerability Security Assessments
- Information Security Policies and Procedures

F. Citadel Servicing Corporation will ensure that devices and systems, including mobile devices issued by Citadel Servicing Corporation , have the appropriate hardware, software, or procedural mechanisms installed on them to enable reviews of information system activity on a periodic basis.

G. The following factors should be considered with respect to the frequency of both scheduled and periodic reviews of audit mechanisms:

- The merit or sensitivity of corporate/client data on devices and systems.
- The importance of the applications operating on the information systems.
- The information system activity audit mechanism review process will include:

  - Definition of what activity is significant.
  - Procedures for defining how significant activity will be identified and, if appropriate, reported.
  - Procedures for maintaining the integrity of records of significant activity.
  - Identification of which workforce members will review records of activity.
  - Definition of which activity records need to be archived and for what duration.
- When requested, and for the purpose of performing an audit, consent to access-needed resources will be provided by members of the affected department.

H. The Citadel Servicing Corporation IT department will provide protocols, addressing information, and network connections sufficient for the Information Security Office to utilize the software to perform security testing/scanning. This access may include:

- User level and/or system level access to any computing or communications device.
- Access to information that may be produced, transmitted or stored on company equipment or premises.
- Access to work areas such as labs, offices, cubicles, storage areas, etc.
- Access to interactively monitor and log traffic on corporate networks.

The Information Security Office is responsible for publishing an internal standard defining the nature of the information that must be recorded in computer and network device system logs (e.g., system logging standards). This information must be made securely network-accessible in order to support a variety of network security systems (such as intrusion detection systems).

37.5.2. Security Monitoring

Alerting for defined events requiring a response will be enabled to provide centralized notification. Application logs will be monitored with the appropriate support groups/staff being notified in the event of an anomaly or incident being discovered to address the event. Security monitoring frequency, and either baseline thresholds or specific criteria for incident identification, will be documented and maintained in a central location.

37.5.3. Security Incidents

All identified security incidents, whether the source identification is via User, real time security alerts, log review, tests, maintenance activities, audits, or other activities, will be addressed by company incident response policies and procedures. When a potential security incident is identified, the appropriate company incident reporting forms will be utilized to identify and document the incident.

37.5.4. Permission

Citadel Servicing Corporation hereby provides its consent to allow the Information Security Office to access its networks and/or firewalls to the extent necessary to allow the team to perform the scans authorized in this policy.

37.5.5. Network Control

If audit scanning and system monitoring is to occur outside of the Citadel Servicing Corporation ’s corporate LAN, and if an office, client or vendor does not control their network, and/or Internet service is provided via a second or third party, these parties are required to approve scanning in writing.

37.5.6. Service Degradation and/or Interruption

Network performance and/or availability may be affected by the network scanning. Any outage will be announced prior to scanning of the systems.

37.5.7. Point of Contact during the Scanning Period

Where appropriate, the Information Security Office will communicate with the department that is being scanned to ensure business continuity and address any questions they may have.

37.5.8. Scanning Period

Citadel Servicing Corporation will identify in writing the allowable dates for a third-party security scan/assessment to take place.

37.5.9. Monitoring and Auditing Guidelines

Citadel Servicing Corporation will use the following guidelines to perform required monitoring, review and auditing of devices and systems used.

- A minimum of one external penetration tests will be performed each year by an independent specialist. Any penetration remediation will be tracked with each successive test, checking the remediation performed since the prior test.
- Appropriate software, database, network, and hardware audit logs will be activated to record additions, changes or deletions to corporate/client data. This includes audit logs associated with remote access.
- Audit logs will be activated to monitor network activity such as firewall activity, activity across routers, and activity of users with administrator level privileges.
- Logs to be activated will be determined by function (e.g., client information manipulation), to review general network activity including remote access.
- Logs will record any access to, additions, changes or deletions to corporate/client data, the date of the activity and the unique user ID of the employee or affiliated third party manipulating the data.
- Audit and error logs will not contain any clear text data classified as Secret or Confidential (e.g., user passwords, client account information).
- Software, database and application audit logs related to corporate and/or client data will be reviewed weekly by the Information Security Office or their designee.
- The logs will be maintained for a minimum of two months following review.
- If directed by Management or the Information Security Office pursuant to legal action, audit log deletion will cease until the legal action is resolved.
- Any noted inappropriate activity will be reported to Management, the Information Security Office or designee and, if appropriate, the security incident response team for investigation.
- An audit report that summarizes findings will be generated by the Information Security Office or their designee whether or not any inappropriate activity is discovered.
- The Citadel Servicing Corporation IT department will periodically monitor transmission of corporate/client data via Internet, e-mail and secure transmission.
- If data is transmitted inappropriately or unprotected over an open network, the Citadel Servicing Corporation IT department will report the incident to the Information Security Office or designee for follow-up and imposition of appropriate remedial actions/sanctions.

Audit Preparation

- Citadel Servicing Corporation or their designee will periodically inventory all applications, devices, and data repositories to determine what audit logs can be generated when corporate/client data is accessed.
- Citadel Servicing Corporation or their designee will periodically activate all appropriate audit logs to track data access.

- Citadel Servicing Corporation or their designee will also develop an audit log review schedule for each audit log generated. The schedule will reflect the criticality of the data (e.g., audit log reviews will be more frequent for more sensitive data).
- Citadel Servicing Corporation or their designee will review audit logs generated and evaluation criteria for periodic audits at least annually or whenever any major system or business changes occur.

Audit Process

- Anomalies will be documented in a periodic audit report that includes the audit logs reviewed, the date of the audit and a description of the anomaly.

Following a review of the set of audit logs, Citadel Servicing Corporation or their designee will investigate any anomalies found and document findings.

- Any anomalies along with scanning and testing results requiring remediation will be logged and tracked on Citadel Servicing Corporation ’s IT ticketing system.
- If an anomaly was caused by the application or data repository, Citadel Servicing Corporation or their designee will report such a finding to the designated information technology member.
- If the anomaly was caused by inappropriate action on the part of an Citadel Servicing Corporation employee, affiliated third party or business associate, the anomaly and the individual or entity responsible for inappropriate access or action will be reported to the Information Security Office.
- The IT member is responsible for mitigating any damages and/or applying the appropriate patches to prevent such anomalies in the future and is responsible for reporting back to Citadel Servicing Corporation or their designee who will document the mitigating action taken in the periodic audit report.

The Information Security Office is responsible for reporting back to Management or their designee who will document the mitigating action taken in the periodic audit report.

The Information Security Office is responsible for working with appropriate management and human resources to apply sanctions matching the severity of the incident. This may include disciplinary action, additional staff training and, if actions are criminal in nature, reporting the incident to the appropriate law enforcement authorities.

37.5.10. Report and Audit Log Retention

- On a regularly, scheduled monthly basis, the Information Security Office or designee will review logs of information system activity audit mechanisms implemented on corporate devices and systems.
- Periodic audit log review reports will be retained for a minimum of six years.
- The audit logs for the period covered by the review will be retained for ninety (90) days or the conclusion of any anomaly investigation or required remediation, whichever is later.
- Periodic audit reports will be reviewed at the time of the quarterly evaluation to determine if any patterns exist between audit periods.
- If such patterns exist, they will be noted in the annual compliance audit report.
- Citadel Servicing Corporation will maintain a log of all facilities (including electronic, video and manual logs) access control outages for a minimum of one calendar year. These logs will be classified as CONFIDENTIAL information and will be reviewed by the Information Security Office or their designee before destruction.

37.6. 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.