CITADEL

SERVICING CORPORATION

NETWORK SECURITY MANAGEMENT POLICY

2022

30. NETWORK SECURITY MANAGEMENT POLICY

POLICY STATEMENT

Citadel Servicing Corporation strives to assure the integrity and **confidentiality** of all information disseminated, produced, managed or stored on its networks. Citadel Servicing Corporation 's goal is to protect their information assets from any internal, external, deliberate or accidental threats and prevent disruption to its business operations and its clients.

30.1. OVERVIEW

It is important to ensure the secure communication of devices and data on Citadel Servicing Corporation 's network. Network security policies are designed to protect Citadel Servicing Corporation , our employees, customers and other partners from harm.

The network security management policy covers access, management, operation and use of company data networks, working in conjunction and complementing other security policies. This policy includes statements and references to areas such as:

- Management of the network
- Network design and configuration
- Physical security and resilience
- Change Management
- Continuity Management
- Connecting devices to the network
- Management of network devices
- Network services and protocols
- Controlling network access
- Firewalls and Routers
- Demilitarized Zones (DMZ)
- Incidents and emergency procedures
- Personally Identifiable Information and Networks

30.2. PURPOSE

The purpose of this policy is to establish the acceptable use and management of Citadel Servicing Corporation 's networks and systems. This policy defines the requirements for establishing the network controls related to Citadel Servicing Corporation 's computer and communications systems infrastructure.

30.3. SCOPE

This policy applies to all Citadel Servicing Corporation computer systems, network equipment and 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.

Exception will be permitted only if approved in advance and in writing by the Information Security Office. All new equipment and systems which fall under the scope of this policy must be configured according to corporate configuration standards, unless a waiver is obtained from Citadel Servicing Corporation Management.

30.4. 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.

30.5. POLICY REQUIREMENTS

30.5.1. Management of Network

Citadel Servicing Corporation will designate authorized groups and personnel to oversee the day-to-day responsibility for administering all network devices such as routers, switches, gateways, firewalls, network wall sockets, wireless access points and wall sockets forming Citadel Servicing Corporation ’s network infrastructure. Note the following restrictions:

- No unauthorized changes or other interference with these network devices or cabling is permitted.
- Moves, changes and other reconfigurations of cabling and users’ network access points will only be carried out by authorized staff.
- The IT Department and authorized IT staff are responsible for providing the enterprise wireless network service. Individuals and business departments are prohibited from establishing their own wireless networks and adding wireless access points. Where there is a known or suspected risk to network security, quality of service for network users, or in order to enforce Company Policies, the IT Department is authorized to impose restrictions and refuse connection to Network or network applications.
- Remove devices or sub-sections of the network from service.
- Manage network resource allocation (such as bandwidth).

Control of network address allocation rests with the IT Department although this may be delegated to authorized staff or designated third parties for specific address schemes.
Users of the corporate network are to be explicitly advised that normal operational network management procedures will include: probing devices to test their security and the monitoring of network traffic to detect operational problems or possible policy violations.

Any connections between in-house Citadel Servicing Corporation production systems and any external computer systems, or any external computer networks or service providers, must be approved in advance by IT Management.

The responsibility for the security of equipment deployed by external service providers must be clarified in the contract with the service provider with security contacts, and escalation procedures documented. Contracting departments are responsible for third-party compliance with this policy including addition of the Right-To-Audit terms.

30.5.2. Network Design and Configuration

The network must be designed and configured to deliver levels of performance, security and reliability suitable for company business needs, while providing a high degree of control over access.

Controls must be used where practical to partition the network into domains on the basis of security requirements. Access controls and routing must be used to prevent unauthorized access to network resources and unnecessary traffic flows between domains. In particular, appropriately configured firewalls must be used to help protect Citadel Servicing Corporation ’s critical computer systems.
The internal system addresses, configurations, products deployed, and related system design information for networked computer systems are restricted to preclude both systems and users outside the Citadel Servicing Corporation internal network from accessing this information.

30.5.3. Change Management

Any changes or updates to paths, services, existing equipment and deployment of new equipment must go through the change management approval process. Emergency change requests must be approved by the Information Security Office, or their designee.

Where supported and if applicable, all Citadel Servicing Corporation network devices and systems will subscribe to software maintenance and software update services. Unless approved in advance by the IT Management or in the case of an operating flaw discovered in the release, it is the standard operating procedure for Network Administrators to install and run these updates within a normal business cycle.

To verify compliance with this policy, Citadel Servicing Corporation will periodically audit the network and related systems as per corporate audit control policies.

30.5.4. Continuity Management

Citadel Servicing Corporation must prepare and maintain continuity plans which specify the actions to be taken in the event of disruptions such as system compromise, malfunction, crash, or overload, and Internet service provider unavailability. Such plans are prepared and maintained per Business Continuity Plan (BCP) requirements and IT Management specifications. These contingency plans must be kept current to reflect changes in Citadel Servicing Corporation ’s information systems environment and periodically tested to ensure effective restoration of a secure and reliable networking environment.

Citadel Servicing Corporation will maintain up-to-date back-up copies of network devices (e.g., firewall) configuration files, connectivity permission files, systems administration procedural documentation files, and related files. Encrypted online versions of these same files are permitted as an alternative to offline copies.

30.5.5. Connecting Devices to the Network

Vendor-supplied default passwords and other security parameters will not be employed with routers and firewalls. Passwords and security parameters will be changed to conform and align with corporate security standards (e.g., password complexity) to ensure compliance and security of the corporate network.

Ownership of Network Devices — Only devices owned by, or authorized BYOD by Citadel Servicing Corporation or those devices authorized from third-parties (e.g., contractors, vendors) may be connected to Citadel Servicing Corporation network and access its systems. These devices may connect to the Citadel Servicing Corporation network after following the approval process as outlined in policy guidelines.

All devices, whether personally-owned or belonging to authorized third-parties, must meet policy hardware and software requirements, and their usage must conform to company policies.

Regardless of ownership of a device, its connection to the Citadel Servicing Corporation network is conditional on the IT Department having the right to inspect its configuration, test its security and monitor its network traffic in accordance with normal operational network management procedures.

Administration of Network Devices — Every network device must be associated with an identifiable and contactable person responsible for its administration. Devices for which the administrator cannot be identified or contacted are liable to be removed from the network.

Network devices on Citadel Servicing Corporation network may be administered by the IT Department, designated third-parties or an organization contracted to undertake their administration.

Users of personally-owned (BYOD) devices that access the corporate network and systems are, and will be assumed to be, responsible for ensuring their devices are configured, actively maintained and used in accordance with Citadel Servicing Corporation guidelines and policies related to mobile devices.

Authorization to Connect a Device — Approval must be obtained from Citadel Servicing Corporation before connecting a device to its network. The unauthorized connection of laptops, PCs or other devices to Citadel Servicing Corporation network is forbidden for security reasons.

Citadel Servicing Corporation will approve connection of devices to its network when they are certain the device meets all relevant requirements and security criteria as set out in company policies and guidelines.

Systems designers and developers must restrict their usage of external network interfaces and protocols to those that have been expressly approved.

Authentication of Network Users — Users of Citadel Servicing Corporation IT facilities and systems must not masquerade as another user or tamper with audit or activity logs.

It is the responsibility of the IT Department to manage the computers in a way that ensures that local user accounts can be identified.

Where it is necessary for an account to be shared, the system administrator, or the individual designated as responsible for managing that account, must have full knowledge of the users that have been authorized to share the account.

Hardware and Software Requirements — Network devices must meet current hardware and software requirements, where any such requirements are specified and published by the IT Department. At the discretion of the IT Department any devices not meeting any such requirements may be denied network access.

All network devices must be maintained so as to be up to date with security patches for both the operating system and any software applications installed. Where applicable, networked devices must have correctly configured firewall software installed. As a default all ports must be closed unless specifically opened. Services exposed to the network and the scope of exposure for each service must be the minimum possible.

30.5.6. Management of Network Devices

Those responsible for network devices must work in cooperation with the IT Department such that it can discharge its responsibility for managing the overall network. Responsibility for devices must be clear.

Primary control over access to the corporate network is to be implemented the IT Department or those parties authorized by them who must:

- Decide whether to approve requests for connection of devices to Citadel Servicing Corporation network on the basis of the connection requirements set out in this policy document.

- Be a point of contact with the Information Security Office in relation to the security of the network device within their area of responsibility.
- Take responsibility for handling security problems that arise in relation to network devices in a timely manner. Technical support is to be provided to Citadel Servicing Corporation by the IT Department or authorized third parties. For devices not fully managed, ultimate responsibility for ensuring configuration and usage complies with policy rests with the IT Department.
- Where necessary, remove a device from the network to help protect operations or security of the wider network.

All Citadel Servicing Corporation network devices and systems are to be configured with unique passwords or other access control mechanisms for both the underlying OS (if applicable and accessible) and the device/system. Network administrators are required to use, where supported, extended user authentication mechanisms to access any of Citadel Servicing Corporation ’s network devices and systems.

30.5.7. Network Services and Protocols

Deploying web servers or other types of network servers which are not approved, and do not support recognized company activities and functions is prohibited.
Only the IT Department, or authorized parties with delegated responsibility can manage the network protocols and services (e.g., DHCP) that enable communication over Citadel Servicing Corporation network.

The use of network management tools (e.g., SNMP) is restricted to the IT Department or authorized parties by prior agreement.

Where access credentials, or other confidential information, may otherwise be transmitted on the network in clear text (e.g., unencrypted), use of encrypted network protocols is required using a minimum of 256-bit encryption protocol. The design, installation and managing of wireless networks within Citadel Servicing Corporation will be guided by Citadel Servicing Corporation ’s Wireless Communication Policy.

30.5.8. Controlling Network Access

Citadel Servicing Corporation ’s IT Department or authorized parties are responsible for controlling the network gateway between its network and the Internet. At this gateway, Citadel Servicing Corporation may exert control over which incoming or outgoing network connections are permitted. This access control may be used for:

- Limiting the scope of exposure of corporate network services to the Internet in order to reduce the risk of hacking, denial of service attacks, unauthorized disclosure of information, etc.
- Preventing propagation of malware or network traffic associated with malware.
- Applying control consistent with implementing current corporate IT strategy.

The internal system addresses, configurations, products deployed, and related system design information for networked computer systems are restricted to preclude both systems and users outside Citadel Servicing Corporation network from accessing this information.

Exposure of network services to incoming connections from the Internet is not permitted without prior agreement from IT Management. Note the following:

- “Incoming connections” are those initiated from devices on the Internet.
- All established provision of network services to the Internet may subject to review.
- The agreement to permit connections into company systems will be consistent with current corporate IT strategy and requirements.
- These network services include, however, are not limited to:
  - Websites
  - Login access for offsite users or automated processes; remote desktop access.

Access to the Citadel Servicing Corporation network from the Internet via Virtual Private Network (VPN) connections is not permitted without prior agreement and approval by Citadel Servicing Corporation . Dial-up access to a device on the corporate network using a modem is not permitted without prior agreement and approval from Citadel Servicing Corporation .

30.5.9. Firewalls and Routers

Only routers and firewalls approved by IT Management can be installed on Citadel Servicing Corporation networks. All firewalls and routers used on the Citadel Servicing Corporation network will follow best practices as outlined in Citadel Servicing Corporation ’s router and firewall procedures. These procedures are in place to ensure the security of the corporate network and the data transmitted on the network.

All computers needing greater protection than what can be provided by firewall(s) closer to the edge of the network (e.g., portable computers that are used outside a trusted Citadel Servicing Corporation network) require a client (“personal”) firewall approved by IT Management.

All in-bound real-time external connections to Citadel Servicing Corporation internal networks or multi-user computer systems must pass through a firewall before users can reach a logon banner. All Citadel Servicing Corporation computer systems may be attached to the Internet only when protected by a firewall.

Wherever a firewall supports it, logon screens display a notice indicating that the system may be accessed only by authorized users; users who log on represent that they are authorized to do so, unauthorized system usage or abuse is subject to disciplinary action including criminal prosecution, and system usage will be monitored and logged.

All inbound traffic, with the exception of Internet mail, approved news services, and push broadcasts, services, and push broadcasts, that accesses Citadel Servicing Corporation networks must be encrypted with an approved Virtual Private Network (VPN) solution.

Privileges to modify the functionality, connectivity, and services supported by firewalls is restricted to designated Firewall Administrators. Unless the Information Security Office has granted permission otherwise, designated Firewall Administrators are limited to individuals who are permanent company employees, and not temporaries, contractors, consultants, or outsourcing personnel.

All Citadel Servicing Corporation firewalls outside of a secured data center must be located in locked rooms, closets, or cabinets which meet Citadel Servicing Corporation Physical Security standards and which are accessible only to authorized Firewall Administrators and authorized Citadel Servicing Corporation IT personnel. Firewall Administrators are expected to subscribe to internet alert advisories available and other relevant sources providing current information about firewall vulnerabilities.

All changes to a firewall rule-set (aka “policy configuration”) require the following process over and above the standard Change Management process. All firewall rule change requests will be evaluated to ensure that they conform to current security best practices and current Citadel Servicing Corporation security policy.

All firewall rule change requests must include the following pieces of information:

- Source address(es), including IP's and domain names (where applicable)
- Destination address(es), including IP's and domain names (where applicable)
- Port(s) requested to be open
- Date when the change should be made; Date the change was implemented.

30.5.10. Demilitarized Zones (DMZ)

All Internet commerce servers including payment servers, database servers, and web servers must be protected by firewalls, and be located within a demilitarized zone (DMZ), a subnet that is protected from the Internet by one or more firewalls.

IT equipment and applications used for the DMZ system, application, and/or network management must be administered by support groups approved by Citadel Servicing Corporation . These support groups will be responsible for the following:

- Equipment must be documented and at a minimum, the following information is required:
  - Host contacts and location.
  - Hardware and operating system/version.
  - Main functions and applications.
- Changes to existing equipment and deployment of new equipment must follow and corporate governess or change management processes/procedures.

All equipment must comply with the following configuration policy:

- Operating system configuration must be done according to the secure host and router installation and configuration standards and be approved by Citadel Servicing Corporation .
- All patches/hot-fixes recommended by the equipment vendor and Citadel Servicing Corporation must be installed. Administrative owner groups must have processes in place to stay current on appropriate patches/hotfixes.
- Trust relationships between systems may only be introduced according to business requirements, must be documented, and must be approved by Citadel Servicing Corporation .
- Services and applications not for general access must be restricted by access control lists.
- Remote administration must be performed over secure channels (e.g., encrypted network connections using SSH or IPSEC) or console access independent from the DMZ networks.
- All host content updates must occur over secure channels.

Security-related events must be logged and audit trails saved to company-approved logs, including the following:

  - User login failures; failure to obtain privileged access; access policy violations.
  - Failure to obtain privileged access.
  - Access policy violations.
- Citadel Servicing Corporation will address non-compliance waiver requests on a case-by-case basis and approve waivers if justified.

30.5.11. Incidents and Emergency Procedures

Any incident or emergency relating to the Citadel Servicing Corporation network must be reported to Information Security Office, appropriate technical staff or management. The handling of any incident or emergency must follow the steps as provided in Citadel Servicing Corporation 's Computer Incident Response and Forensics Readiness policies.

30.5.12. Personally Identifiable Information and Networks

Personally Identifiable Information (PII) data within Citadel Servicing Corporation has requirements that the storage and use of PII-related data is prohibited from end-user devices (e.g., laptops, workstations, tablets, smart phones).

All devices storing PII-related data must have disk encryption enabled to protect the data. The encryption must meet the industry standard of 256-bit encryption. Storage of PII-related data must be limited to designated systems, designed to store and protect that data. PII-related data must be stored on systems to isolate the data to prevent copying and intermingling with other Citadel Servicing Corporation systems and data.

Networks that will be used to transmit PII data will employ a minimum 256-bit encryption protocol to protect network traffic. When transmitting data using public networks, data encryption (256-bit encryption) is required in accordance company encryption policies and guidelines.

Where wireless networks are used to access and communicate PII data, they must be segregated from other company wireless networks.

30.6. ENFORCEMENT

All users (employees, contractor, part-time and temporary workers) and those employed by others to perform work for Citadel Servicing Corporation , 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.