CITADEL
SERVICING CORPORATION

WIRELESS COMMUNICATION POLICY

2022

12. WIRELESS COMMUNICATION POLICY

POLICY STATEMENT

Citadel Servicing Corporation will ensure the establishment of standards and guidelines for the use of wireless devices within the corporate environment. These standards and guidelines are to protect the corporate network, company and client data from compromise and maintain compliance with federal and state laws and regulations.

12.1. OVERVIEW

Wireless devices and networks enable un-tethered communications. Improperly installed, configured or managed wireless technology can provide a point of entry for unauthorized users to access company systems and data presenting a significant risk to the confidentiality of corporate information and resources. This policy defines the use of wireless devices and wireless network connectivity within the corporate environment.

12.2. PURPOSE

The purpose of the wireless policy is to assure that Citadel Servicing Corporation 's employees, guests, and contractors have access to a reliable wireless network, and to secure and protect the information assets of the corporate wireless network to the highest extent possible.

This policy defines requirements for the secure establishment, maintenance and use of wireless networks by Citadel Servicing Corporation , including equipment devices (e.g., notebooks, tablets, smart phones, etc.) used to make wireless connections to corporate networks. Only wireless systems that meet the criteria of this policy or have been granted an exclusive waiver are approved for connectivity to Citadel Servicing Corporation 's networks.

12.3. SCOPE

The policy applies to 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 computer systems and facilities, including those managed for company customers.

This policy covers all wireless data communication devices (e.g., mobile devices such as personal computers, cellular and smart phones) connected to any corporate internal networks. This includes any form of wireless communication device capable of transmitting packet data.

12.4. 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.

12.5. TRAINING

All users requiring or requesting wireless access to Citadel Servicing Corporation ’s internal network must complete a brief IT Security Awareness training program developed by and delivered by the Information Security Office.

12.6. POLICY

Due to the public nature of wireless signals, access to Citadel Servicing Corporation ’s wireless network is permitted only to authorized personnel with a valid network account. Wireless access to corporate networks and systems is a privilege extended to users; it is not an implicit right. Only wireless devices with approved configuration are allowed to connect to the wireless network. Requests for wireless network access must be approved by Citadel Servicing Corporation and in accordance with corporate policies and procedures.

12.6.1. Secure Deployment

The IT Department and the Information Security Office will approve all wireless devices connected to the corporate network.

All wireless devices and supporting resources, such as wireless access points, and other network devices, are to be positioned in a manner for ensuring unauthorized physical access and modification. Additionally, they are to be secured with approved fixtures and other necessary apparatuses for mitigating any unnecessary movement.

12.6.2. Automatic Discovery of Wireless Networks

Citadel Servicing Corporation automatically detects the presence of all internal-network-connected devices. To further ensure that all internal wireless networks have been registered and approved, testing will be conducted periodically to check for unauthorized wireless access points.

12.6.3. Approval and Access

A. Devices — Only those devices (notebooks, handhelds, portables, personal digital assistants, smart phones, etc.) that have been approved by the IT Department and the Information Security Office will be permitted to gain access to Citadel Servicing Corporation ’s internal network via wireless technology. The devices connecting to the corporate wireless network must meet all technical and security requirements and standards as established by the Information Security Office.

B. Wireless — Only approved users will be granted wireless network access, employing properly configured devices to access the corporate wireless network. Users are prohibited from setting up their own wireless networks without this approval process, whether or not these networks connect with Citadel Servicing Corporation ’s internal network.

C. Authentication Required — Access to Citadel Servicing Corporation ’s internal networks via a wireless connection will furthermore only be permitted in which the end user employs approved user authentication technology (e.g., network credentials). Citadel Servicing Corporation requires employees to use multi-factor authentication when connecting to corporate wireless networks.

D. Guest Access — Guest access to the corporate wireless network will only be supported in those areas designated as deemed appropriate by the Information Security Office (e.g., reception area, conference and meeting rooms). Any guest/public wireless networks must be separate with no direct access to Citadel Servicing Corporation ’s internal network and computers, providing only public Internet access as required.

E. **Disabled by Default** — Wireless communications capabilities found in desktop machines and all other Citadel Servicing Corporation computers must remain disabled until they have been evaluated and approved by the Information Security Office.

12.6.4. Establishing Wireless Networks

A. **Requesting Approval for a Wireless Network** — If a wireless network appears to be a good solution to a business problem, a request for a feasibility study examining the use of a wireless network must first be submitted to the IT Services. If this study indicates that a wireless network is a prudent technology that will serve company business needs, a risk assessment must then be performed by the Information Security Office prior to the deployment of any wireless networks. When considering the use of wireless networks for production applications, employees should be aware that the cost of these systems exceeds that of the wireless network alone.

B. **Failover Networks** — All wireless networks used for production applications must also employ an alternative fail-over networking technology. This will allow business activities to continue when the wireless network is inoperable (for instance due to radio frequency interference). Such a fail-over network must be built, thoroughly tested, and then approved by the Information Security Office before a wireless network will be permitted to operate with a production application.

12.6.5. Design

A. The highest level of encryption standards will be employed to protect wireless network traffic. Encryption protocol will employ a minimum key length of 256 bits.

B. Deploy software patches and updates on a regular basis.

C. Configure wireless devices to not broadcast SSID numbers or other network related information, where applicable.

D. Deploy firewalls between the wireless network and corporate network when possible.

E. Physically secure all wireless routers, gateways, or access points and lock down the administration interfaces.

F. Wireless networks that access and communicate Third Party data must be segregated from other corporate wireless networks.

12.6.6. Access Points (AP)

A. Maintain and update an inventory of all Access Points (AP) and wireless devices.

B. Locate APs on the interior of buildings instead of near exterior walls and windows to avoid signal leakage.

C. Place APs in secured areas to prevent unauthorized physical access and manipulation.

D. The default settings on APs, such as those for SSIDs (using a unique character string), must be changed before being deployed.

E. Ensure that all APs have strong administrative passwords.

F. Enable user authentication mechanisms/integration for the management interfaces of the AP.

G. Turn on the audit capabilities of the AP; review log files on a regular basis.

12.6.7. Mobile Systems

A. Where appropriate, install anti-virus software on wireless clients.

B. Where appropriate, install personal firewall software on all wireless clients.

C. Disable file sharing between wireless clients.

D. Any Bluetooth devices used within the corporate systems environment must use Secure Simple Pairing with encryption enabled.

12.6.8. Installation and Configuration

A. All Citadel Servicing Corporation wireless access points must be installed by and configured by an authorized member of Citadel Servicing Corporation 's systems administration staff or authorized contractors.

B. Authorized individuals must follow the Information Security Office's installation, configuration, and management guide for wireless networks. This guide covers a wide variety of topics such as changing default passwords so that unauthorized parties cannot gain system access, turning on encryption so transmissions are protected, and disabling identifier broadcasting, so unauthorized parties cannot readily detect the presence of a wireless network.

C. All wireless access points must be running the latest version of the vendor-supplied operating system, firmware, and security software. Likewise, all mobile devices authorized to access Citadel Servicing Corporation 's wireless networks must be running an up-to-date suite of operating system and security software as defined by the Information Security Office. Those wireless access points or mobile devices that are not running up-to-date software are subject to being blocked from accessing Citadel Servicing Corporation internal network.

D. **Automatic Downloads** — Automatic download facilities must be provided to enable these machines to quickly and securely update their software. In the event that the security of any wireless device has been compromised, these devices will be isolated from the internal network using the same blocking technology, so that further problems are prevented.

12.6.9. Logical and Physical Security

A. **Secure Network Access Points** — To prevent tampering, reconfiguration, theft, and other unauthorized activity, all wireless network access points must be physically secured in areas accessible only by authorized personnel. Wireless network access points must also be placed, and the wireless coverage area designed, so that the possibility of unauthorized signal interception is minimized.

B. **Encryption and Intrusion Controls** — Company wireless network access points must always be configured so that they consistently employ communications encryption, firewalls, hardware device address (MAC address) filtering, intrusion detection systems, and other security measures defined by IT Network Management and/or the Information Security Office.

C. **Logical and Physical Separation** — All wireless access points must be logically distinguished from, and walled off from, the main corporate internal network using configurations approved by the Information Security Office. Wireless networks that access and communicate Third Party data must be segregated/separate from other corporate wireless networks.

D. **Inventory of Wireless Equipment** — The IT Department will perform periodic inventory of all internal-network-connected equipment including authorized wireless access points and authorized mobile devices that have wireless computing interfaces.

E. **Physical Protection of Wireless Devices** — Users must diligently protect wireless-enabled computing devices from loss, theft, and tampering. This effort includes not leaving unattended devices in the open in public areas such as airports or trains, and not leaving these devices in hotel rooms when the rooms are unattended.

F. **Physical Identification** — All wireless access points and mobile devices **must** have physical identifiers that will allow them to be readily returned to Citadel Servicing Corporation if they are recovered by police or other third parties following an incident where the devices were lost or stolen.

G. **Using Public Networks** — When transmitting data using public networks, data encryption (128-bit encryption) and/or VPN technology is required in accordance with corporate encryption policies and standards.

12.6.10. Managing a Wireless Network

A. **Change Control** — Changes to the configuration or set-up of a wireless network must follow the standard change control process that is required for other production information systems.

B. **Logging Support** — All wireless access points must have sufficient disk space and internal resources to support the logging and systems monitoring software specified by the Information Security Office. Systems administrators responsible for wireless access points must follow the lead of the Information Security Office in response to all security relevant events such as a denial-of-service attack, a computer virus infestation, or an intrusion by an unauthorized party.

C. **Test of Wireless Networks** — Prior to cut-over to production usage of a wireless network, an extensive test must be performed to ensure that all security and availability control mechanisms are working as they are intended to work. Only after the Information Security Office approves the successful completion of these tests can a wireless network be used for production information processing activities.

D. **Authorized Personnel** — The management, repair and administration of Citadel Servicing Corporation wireless networks must be performed by authorized company systems administration staff or authorized contractors. These efforts must follow the procedures defined in the Information Security Office's installation, configuration, and management guide for wireless networks. To ensure that wireless networks have been properly configured and managed, periodic audits will be conducted by the Information Security Office or their designees.

12.6.11. Loss and Recovery of Wireless Technology

A. **Reporting Lost Technology** — The IT Department or the Information Security Office must be notified whenever an approved wireless-enabled computing device (notebook, tablet, smart phone, etc.) is lost or stolen.

B. **Access Denial** — Mobile devices with wireless communications interfaces that have been reported as lost or stolen must be blocked from accessing Citadel Servicing Corporation network.

12.7. ENFORCEMENT

All users (employees, contractor, part-time and temporary employees) 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.