MOBILE DEVICE POLICY

2022

13. MOBILE DEVICE POLICY

POLICY STATEMENT

The use of mobile devices, such as smartphones and laptops, are important tools for Citadel Servicing Corporation in helping business operations to serve its clients and achieve its business goals.

Citadel Servicing Corporation recognizes that these mobile devices can represent a significant risk to information security and data security. They can be compromised to give unauthorized access to corporate and client data and Citadel Servicing Corporation 's IT environment.

It is the policy of Citadel Servicing Corporation to set guidelines and standards for the safe use of mobile devices to effectively secure corporate/client data and networks so that security incidents and breaches are prevented.

13.1. OVERVIEW

Mobile devices (e.g.: mobile phones, smartphones, laptops, tablets) and other portable devices (e.g., flash drives, external hard drives) are important tools used in day-to-day business operations to assist Citadel Servicing Corporation in conducting its business. Citadel Servicing Corporation must maintain policies and technical security for these devices and other electronic media that contain or access corporate and client data used by employees. Controls are established to prevent the loss of confidentiality, integrity, or availability of data and support both privacy and security of sensitive information and compliance with applicable agency and regulatory requirements including local, state, and federal laws.

13.2. PURPOSE

This policy covers mobile telecommunication and mobile computing devices. This policy defines the requirements that must be followed when connecting either corporate or personally-owned mobile devices to Citadel Servicing Corporation systems or networks. All mobile device equipment procured by Citadel Servicing Corporation is corporate property.

13.3. 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 with company-owned or personally-owned (BYOD) mobile and portable devices used with corporate data or networks.

13.4. 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.

13.5. TRAINING

Due to the unique risks to mobile computing devices, all Citadel Servicing Corporation employees who are issued mobile computing devices and/or who are authorized to use their own mobile device according to the BYOD policy (detailed below) must receive training on the information risks.

13.6. 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.

13.6.1. General Requirements

A. Citadel Servicing Corporation will, unless agreed to otherwise, provide its employees mobile computing equipment ("mobile devices") such as laptops, smartphones or tablets as applicable. The provisioning of the equipment is strictly on a need-to-have basis, and final determination of the need of the employee to have access to one or more devices will be at the sole discretion of Citadel Servicing Corporation Management.

B. The security of company-owned mobile devices is managed by Citadel Servicing Corporation IT personnel to ensure that security solutions adequate to the business risks are maintained and that corporate data is thoroughly removed from all devices prior to reassignment or disposal.

C. Upon executive management approval, an employee may choose to use their own mobile computing devices for Citadel Servicing Corporation business. This model is commonly referred to as "Bring Your Own Device" (BYOD). Employees and managers agreeing to use this model will be governed by the "Personally-Owned Devices" section of this policy.

13.6.2. Configuration and Issuing of Mobile Devices

A. **Company-Only Mobile Devices** — Employees must not use personal mobile devices to store or process Citadel Servicing Corporation information (see exception agreement for Personally-Owned Devices). All mobile devices used for Citadel Servicing Corporation business purposes must be issued by the Information Technology department or in the case of BYOD devices approved by the Information Security Office.

B. **Approved Configuration of** Mobile Computing Devices — Mobile computing devices including (but not limited to) laptops, tablets, smart phones, flash drives, etc. must not be used to store Citadel Servicing Corporation business information unless they have been configured with the necessary controls and approved for such use by the Information Security Office.

13.6.3. Mobile Computing Configuration and Data Management

A. **Mobile Devices Containing Sensitive Information** — All mobile computing devices, including laptops, tablets, flash drives and any peripherals containing sensitive Citadel Servicing Corporation information must consistently employ encryption for all such files, and wherever possible, start-up and screen-saver-based password\boot protection.

B. **Ownership of Information Stored in Mobile Devices** — Citadel Servicing Corporation provides selected members of its workforce with mobile computing equipment so that they can perform their jobs at remote locations including hotel rooms and personal residences. The information stored in Citadel Servicing Corporation portable computer equipment is company property. Such property can be inspected, or used in any manner at any time by Citadel Servicing Corporation and, such equipment; must be returned to Citadel Servicing Corporation as defined by the Human Resources or IT departments. In the case of workers no longer under employment of Citadel Servicing Corporation , such computer equipment must

not be wiped clean unless in accordance with applicable regulations, and only by executive management approval.

C. **Accepting SMS Messages** — Citadel Servicing Corporation workers must not accept text messages on mobile devices from unknown senders due to the risk of malicious software. Any messages or contacts received on a mobile phone from an unknown number or device should be treated with suspicion. Messages should be destroyed without opening and connections denied.

D. **Removable Storage Devices** — USB enabled devices, such as memory sticks, external hard drives, network attached storage devices are strictly prohibited. Though there may be circumstances that require storing of sensitive and confidential information onto these utilities, it must be approved in writing by the Information System Owner, and such data is never to reside on these devices for long-term storage measures.

13.6.4. Physical Security Protection

Due to their high-value and high storage capacity, mobile and portable devices are highly susceptible of theft. Users that utilize laptop computers or other mobile/portable devices that contain sensitive organizational information are expected to use reasonable care to secure these devices whenever they are left unattended.

A. **Personnel Responsibility** — All mobile devices in the possession of company personnel must be protected from physical threats such as loss due to theft or vandalism.

B. **Locking Personal Offices or Conference Rooms** — All workers with separate personal offices should lock the doors when these offices are not in use or otherwise unattended.

C. **Leaving Mobile Devices Unattended** — Workers must keep Citadel Servicing Corporation portable computers containing corporate information in their possession at all times unless they have been deposited in a secure location such as a locked closet or a hotel safe.

D. **Storing Mobile Devices** — All mobile/portable devices in the possession of company personnel must be stored in a secure location, such as a locked file cabinet or drawer, when not in use. Under no circumstances should mobile/portable devices be left in open view in public areas. Where feasible and practical, it is recommended to employ physical cable locks to secure laptops and other mobile devices.

E. All company-owned mobile devices must be configured for a session timeout to lockout and secure the workstation, obscuring the screen contents, after fifteen (15) minutes of no activity detected on the workstation.

13.6.5. Authentication and Network Access

A. **Automatic Wireless Network Connections** — Citadel Servicing Corporation mobile devices capable of making wireless network connections must be configured so that automatic network connections are disabled.

B. **Strong Passwords Required** — All portable devices used for Citadel Servicing Corporation business purposes must have passwords enabled. These passwords must be at least eight (8) characters in length.

C. **Using Public Networks** — When transmitting data using public networks, data encryption (256-bit encryption) is required in accordance corporate encryption policies and standards.

13.6.6. Travel Considerations

A. **Removal of Sensitive Information** — Sensitive (Confidential or Secret) information may not be removed from Citadel Servicing Corporation premises unless the information's Owner has approved in advance. This policy includes sensitive information stored on portable computer hard disks, USB flash drives, CD-ROMs, magnetic tape cartridges, and paper memos. An exception is made for authorized off-site backups that are in encrypted form.

B. Foreign Transport of Sensitive Information — Whenever Confidential information is carried by an Citadel Servicing Corporation worker into a foreign country, the information must either be stored in some inaccessible form, such as an encrypted external storage media, or must remain in the worker's possession at all times. Company workers must not take Secret company information into another country unless the permission has been obtained from Information Security Office and/or management.

13.6.7. Lost or Stolen Mobile Devices

All Citadel Servicing Corporation personnel must immediately report lost or stolen devices to both their immediate supervisor and the Information Security Office.

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 automatically barred from accessing Citadel Servicing Corporation 's internal network.

13.6.8. Return and Decommission of Mobile Devices

A. Mobile devices must be returned for decommission — All Citadel Servicing Corporation issued mobile devices, (including but not limited to laptops, flash drives, tablets or smart phones) must be returned to Citadel Servicing Corporation when no longer in use by employees or contractors. Under no circumstances should employees dispose of mobile devices that contained sensitive corporate information.

B. Information Removal before Disposal — Before disposal, donation, or recycling, all data stored on the mobile device must be removed or wiped as per corporate Information Disposal policies, making the data unreadable and unrecoverable. The Information Security Office must validate that sensitive information has been removed from any information systems equipment that has been used for company business. This validation process must take place before releasing such equipment to a third party.

C. Return of Property at Employment Termination — Once an employee, consultant, or contractor terminates his or her relationship with Citadel Servicing Corporation , all company property including, but not limited to, portable computers, documentation, building keys, magnetic access cards, and credit cards must be returned.

13.6.9. Employee Responsibilities

A. It is the responsibility of Citadel Servicing Corporation employees, contractors, vendors, and agents with mobile devices and remote access to Citadel Servicing Corporation networks and data to ensure appropriate use and protection of the devices, data, and networks.

B. Employees must not bypass or disable Citadel Servicing Corporation required security mechanisms under any circumstances.

C. Use of corporate-owned devices and networks by non-workforce members of Citadel Servicing Corporation is prohibited. Access to Citadel Servicing Corporation networks and data by non-workforce members on employee-owned devices are also prohibited. Citadel Servicing Corporation employees are responsible for the consequences should the equipment or access be lost, compromised, or misused.

D. Contractors, vendors, and agents may be granted the authority to access Citadel Servicing Corporation devices and networks if deemed necessary for work they are providing. Access will be provided after the appropriate request has been submitted and the necessary approval has been given by the appropriate Citadel Servicing Corporation manager and the IT Department. Contractors, vendors, and agents will be

bound by the same IT policies as employees when using Citadel Servicing Corporation devices and networks.

E. Citadel Servicing Corporation employees and contractors using company-owned mobile devices for business must not use non-Citadel Servicing Corporation email accounts (e.g., Yahoo, Gmail, Office365), or other external resources to conduct Citadel Servicing Corporation business, thereby ensuring that official business is never confused with personal business.

F. Unauthorized physical access, tampering, loss, or theft of a mobile device must immediately be reported (within 2 hours of determination) to the Citadel Servicing Corporation IT Department in order to initiate effective and timely response and remediation of any possible breach of Citadel Servicing Corporation data.

13.6.10. Personally-Owned Devices (Guidelines and Recommendations)

Citadel Servicing Corporation will endeavor to provide its employees mobile computing equipment ("mobile devices") such as laptops, smartphones or tablets, but recognizes that in some circumstances, employees may need to use personally-owned devices in the course of their normal business routines in support of Citadel Servicing Corporation 's corporate goals and objectives. The use of such "BYOD" devices is strictly on a need-to-have basis, and final determination of the employee's requirement/need will be at the sole discretion of company management.

Like corporate-owned mobile devices, personally-owned mobile devices used within the corporate IT environment will be bound by the same policies applicable to similar company-owned mobile devices. Owners of personally-owned mobile devices are highly encouraged to adhere to the policies governing mobile devices.

Each user with a personally-owned device with authorized access to corporate IT assets, information assets, and/or facilities, the IT Department highly encourages adherence with all applicable policies and regulations as well as with the acceptable use policies of affiliated networks and systems.

Users agree to secure their wireless devices using software and/or controls which will be defined by the Citadel Servicing Corporation IT Department. These controls may include the following:

If the device accesses Citadel Servicing Corporation data of any type:

A. The IT Department highly encourages and promotes the use of following recommendation:

- Use of a personal identification number (PIN) security pattern, password or other form of authentication as provided by the device manufacturer consisting of a minimum of four (4) characters or other form of authentication to gain access to the device.
- Setting an inactivity timeout of no more than 15 minutes requiring the password or PIN to be entered when the timeout is exceeded.
- If the device is used to access confidential or restricted Citadel Servicing Corporation data, the IT Department will ensure that the approved security controls, including encryption, are installed. External storage devices are included (e.g. USB drives).

B. The user understands that he/she may be held liable for any criminal and/or civil penalties that may result from loss, theft, or misuse of the confidential information accessed and/or stored on the personal device.

C. Upon termination of affiliation with Citadel Servicing Corporation , users agree:

- To immediately delete all institutional data stored on the mobile device.
- To remove any Citadel Servicing Corporation email account(s) and any Wi-Fi settings from the mobile device.

D. Users acknowledge that Citadel Servicing Corporation does not provide support for personally-owned devices and has no liability for such devices. Configuration of any personally owned device is the user's responsibility.

13.6.11. IT Department Responsibilities

To ensure that mobile devices, networks, and data are protected against identified security risks, the IT department is responsible to:

A. Conduct periodic risk assessments related to mobile device use.
B. Establish specific processes and procedures for encryption and security breach protocols for mobile device use.
C. Utilize remote tools where possible to remotely secure, remote wipe, monitor and lock devices and prevent data breaches.
D. Enable strong user authentication, implement account lockout, and use two-factor authentication if available.

13.7. 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.