CITADEL

SERVICING CORPORATION

ACCEPTABLE USE POLICY

2022

33. ACCEPTABLE USE POLICY

POLICY STATEMENT

Citadel Servicing Corporation provides computer devices, networks, and other electronic information systems to meet the goals of the corporation. They manage them effectively and responsibly in compliance with industry, state, and federal laws and regulations to protect from loss; to avoid reputation damage; and to avoid adverse customer impact.

33.1. OVERVIEW

This Acceptable Use Policy (AUP) is designed to protect Citadel Servicing Corporation , our employees, customers and other partners from harm caused by the misuse of our IT systems and our data. Misuse includes both deliberate and inadvertent actions.

The repercussions of misuse of our systems can be severe. Potential damage includes, but is not limited to, malware infection (e.g., computer viruses), legal and financial penalties for data leakage, and lost productivity and business resulting from disruptions.

Everyone who works at Citadel Servicing Corporationis responsible for the security of our IT systems and the data on them. As such, all employees must ensure they adhere to the guidelines in this policy at all times.

33.2. PURPOSE

The purpose of this policy is to establish the acceptable and unacceptable use of Citadel Servicing Corporation ’s corporate IT systems and data in conjunction with its established culture of ethical and lawful behavior, openness, trust, and integrity.

This policy requires the users of information assets to comply with company policies and protect Citadel Servicing Corporation against damage to its ability to operate and conduct business.

33.3. SCOPE

This policy applies to all corporate 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 corporate information assets and facilities.

This policy also applies to company-provided workstations accessing Citadel Servicing Corporation ’s network from a non-Citadel Servicing Corporation network through VPN.

33.4. 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.

33.5. POLICY REQUIREMENTS

33.5.1. Implied Consent

Each person with authorized access to Citadel Servicing Corporation 's IT assets, information assets, and/or facilities, is responsible for their appropriate use and by their use agrees to comply with all applicable policies and regulations as well as with the acceptable use policies of affiliated networks and systems.

In the absence of a specific policy or policy statement, employees are expected to utilize good judgment. If there is any uncertainty in the intentions, requirements, or expectations of this or other corporate policies or procedures, employees must consult their manager for clarification.

33.5.2. IT Requests

For all IT requirements, contact the Service Desk for assistance. Requests for access including, but not limited to adds, changes, and removal of access whether to facilities, IT assets, or information assets, must be made in adherence to corporate access administration policies and procedures. Only specifically authorized individuals may monitor equipment, systems, and network or voice traffic.

33.5.3. Clean Desk Practices

It is important to understand your responsibility as an Citadel Servicing Corporation employee to maintain the security of confidential information at your desk. Refer to the Corporate Security Policy for additional detail.

- Lock/secure your workstation while you are away from your desk.
- Do not write passwords down and store them in an unsecured location.
- Secure all confidential data at the end of the workday.

For more information, please contact your manager or the Human Resources Department.

33.5.4. Security Violations

Citadel Servicing Corporation employees (employee and non-employee authorized access users) are responsible for following the policies, procedures, and guidelines, including, but not limited to the corporate Acceptable Use Policy.

Policy violations (real, suspected or attempted), must be reported immediately. Any information relating to a flaw in or bypass of security must be reported immediately**.**

Any security violations or security weaknesses identified because of corporate Security Awareness training, or user knowledge, must also be reported immediately. For all security violations, contact the corporate Security Office.

33.5.5. IT Assets

Citadel Servicing Corporation employees are responsible to ensure the safeguarding of corporate IT assets (e.g., equipment and data).

In adherence to the corporate Mobile Device Policy, employees are responsible for the physical security of company issued portable IT assets. This includes securing laptops, smart phones, tablets and other mobile devices both during and after business hours. Passwords must be utilized on all mobile devices, where technologically possible.

All passwords are required to meet corporate password policy requirements and must not be shared with anyone. Revealing your account password to others or allowing use of your account by others is strictly prohibited.

Immediately report the loss of any laptops, smart phones, etc. to the Acra IT Technical Support. In the case of loss after business hours, call Acra IT Technical support as well as any other affected service providers to have the service immediately suspended.

Unauthorized personnel will not be admitted to secure areas without a business reason to do so and will never be without escort.

Disturbing Citadel Servicing Corporation 's IT systems or interfering with legitimate access to IT assets is strictly prohibited, including using any program/script/command or sending messages of any kind with the intent to interfere with, or disable a user's terminal session via any means including locally or via the Internet/Intranet/Extranet.

Attempting to discover or alter passwords, subvert security technology, or circumvent user authentication or security in Citadel Servicing Corporation 's IT system or any other computing and/or network asset is strictly prohibited, including, but not limited to disabling security monitoring, antivirus software, etc.

Executing any form of network monitoring that will intercept data not intended for the IT asset of the specific user, is strictly prohibited, without explicit authorization as part of an individual's job/role/function.

Users will not affect security breaches or disruptions of network communication. Security breaches include, but are not limited to:

- Accessing data of which the employee is not an intended recipient.
- Logging into a server or account that the employee is not expressly authorized to access.

Disruptions include, but are not limited to Network Sniffing; Pinged Floods; Denial of Service.

Appropriate user identification information is required to request or obtain access to Citadel Servicing Corporation 's IT systems, along with all other relevant valid and complete information, and to establish connections or to access Citadel Servicing Corporation 's IT systems. Requests for access including, but not limited to adds, changes, and removal of access whether to facilities, IT assets, or information assets must be made in adherence to corporate access administration policies and procedures.

33.5.6. Third-Party Assets

Citadel Servicing Corporation will not provide technical or maintenance support for individual personal computer systems.

Citadel Servicing Corporation will not provide technical or maintenance support for third party computer systems used by contractors and/or vendors that are not the property of Citadel Servicing Corporation .

Any exception as a pre-requisite to allowing access by third party systems to IT assets must have approval.

33.5.7. Personal Electronic Devices

Authorized access personnel (Employee and non-employee) may use their personal electronic or communication devices. Use device may not interrupt, distract, or disturb customers or co-workers. During working hours, (Working hours include hours while in a paid status or on Citadel Servicing Corporation 's property) will limit the use of all types of personal communication devices and electronics including, but not limited to:

- Cell phones; Smart phones
  - Uses include speaking on the device as the caller/call recipient; text messaging; retrieval of text or voice mail messages; listening to the device or any other interaction with a personal communications or electronic device.
- Laptops, Tablets, iPads or similar.
- External data drives, or any other portable devices.

33.5.8. Securing Workstations

Protecting your workstation area, specifically your desktop computer and other supporting devices, is an important duty of all staff (employee or non-employee) and this responsibility should be taken very seriously. While many of the workstation security best practices mentioned below are also discussed in other areas of the Information Security Awareness Training Program, you'll find these additional requirements, tips, and suggestions considered important. Personnel (employee and non-employee) in certain cases use company-provided equipment to securely access from non-Citadel Servicing Corporation premises with authorized access to Citadel Servicing Corporation ’s network through secure VPN. It is critical to implement the following best practices:

- **It's your workstation.** That means only you should be using it, and primarily for business purposes only. Allowing other employees to use your workstation is strictly prohibited, unless otherwise approved in advance by your Department Manager and HR. Allowing another employee, or non-employee, use of your workstation who may inadvertently or intentionally access the Internet and possibly result in the downloading of unsuspected malware or sending an unprofessional email or any other action prohibited by Citadel Servicing Corporation . Do not share your workstation rights.

- **Use strong passwords**. While most passwords will be enforced by group policy settings issued from the IT Department, it is still important to make them unique. For passwords never create a password that is easily detected from association with your personal data or preferences (e.g., your favorite sports team, home address, middle name, family names, etc.). With password complexity requirements in place requiring the use of symbols and numbers and other mandates, adopt the same policies to other authorized third-party systems and websites that you personally have administrative password access rights to (e.g., online banking, social media accounts, or any business accounts you have administration rights that are not group policy enforced by the IT Department).

- **Security updates.** Make sure your workstation computer has all the required security updates for the operating system and all other applications running. This also means having anti-virus running at all times and conducting periodic scans. Additionally, the use of anti-spyware may also be required as it provides additional layers of protection, especially during Internet usage. While most of the security updates are "pushed" to devices and managed by the IT Department, at times you may be required to manually accept these updates when logging in. If you have any concerns or questions about the ‘acceptance’ request, please contact IT Technical Support.

- **Do Not alter security settings.** If you have been provided any local administration rights approved and set-up by the IT Department, your workstation has been configured for maximum security and performance. Do not attempt to disable or modify configuration settings to the operating system or any other applications. Doing so may increase security vulnerabilities that would ultimately allow malicious files and other harmful scripts to reside on the workstation. If you have any additional requirement, request through IT Technical Support.

- **Do Not install any unapproved software**. Your workstation has also been configured for providing you the necessary tools in performing daily roles and responsibilities and no additional software is needed. Do not attempt to download, install, or modify any software or other connections to your workstation drives or ports. All software, installed, or internet-based access, not issued by the IT Department needed for your job, must be submitted as a request to IT Technical Support. IT engineers will evaluate for risk, resource consumption, compatibility, etc. prior to use.

- **Do Not use Removable storage devices.** They are easy-to-use, inexpensive, and a great way for transferring information, yet present risk to Citadel Servicing Corporation and customers if secure, sensitive and confidential information is on them and in an unauthorized user's possession. USB ports, such as thumb drives, external hard drives, and other removal storage and memory devices must never contain highly sensitive and confidential information (e.g., Personally Identifiable Information (PII), loan details with customer sensitive data, company information), or any other data deemed privileged information. Such information should be transferred over the network using approved secure protocols and residing on company servers only.

- **Use of Texting and Instant Messaging.** Texting and Instant messaging is a fun, informal, quick and easy, and affordable communication method. Use of these communication methods are allowed but restrictive to the type of content of messages you are sending and receiving. Restrictions include, but are not limited, to transmitting any type of highly sensitive, confidential, or privileged information. This includes what is commonly known as Personally Identifiable Information (PII), unique identifiers for any individual, (e.g., social security numbers, dates of birth, financial and medical accounts, etc.). If you are not confident as to the sensitivity of the information, Do Not send via Text or Instant Messaging.

- **Handle all privileged information with care.** From emails containing sensitive information to hard copy documents for contracts, company information, documents, trade secrets, or any other type of confidential data, all use and transmission must be handled in accordance with Corporate Policies and handled professionally. Do not divulge such information to unintended parties and never leave items (both hard copy and electronic media) unattended in public at any time (coffee shops, training seminars, conferences, hotel rooms, etc.).

- **Report security issues immediately.** Remember, if you observe an intentional, or un-intentional violation or risk, please report this to your Manager immediately. If there is a circumstance that occurs off company premises, treat this in the same manner, report to your Manager immediately. Should you be in a situation where you accidently left sensitive or confidential information exposed (e.g., hotel, restaurant, transportation, etc.) report this immediately to your Manager. You have a responsibility for helping to protect the organization, which means being aware of your surroundings and reporting suspicious activity to authorized personnel – immediately. From seeing a door ajar that should not be to finding sensitive documents lying in a commons area, you need to take action.

33.5.9. Telecommuting / remote work via a Non-Citadel Servicing Corporation Network

Citadel Servicing Corporation Personnel (employee and non-employee) may work from alternate locations, (home or alternate location) when authorized using company-provided workstations, or have been pre-authorized to use non-Citadel Servicing Corporation workstations with secure log-in controls. Remote access may include temporary data access and storage, processing and transmitting sensitive and confidential company information over their non-Citadel Servicing Corporation personal networks, which may pose significant security risks.

Listed below are best practices for secure use of a non-Citadel Servicing Corporation private or personal network.

- **Use Anti-virus.** Citadel Servicing Corporation -provided computer you are using on your home network comes with the current, updated anti-virus installed. This provides security safeguards as it protects your computer from malware and other malicious exploits. If prior approval was granted for use of non-Citadel Servicing Corporation Computer(s), all security updates must be installed as available.

- **Use strong passwords.** Use strong passwords in accordance to Citadel Servicing Corporation ’s set guidelines, those that contain a mixture of letters, numbers, and symbols. This applies to your actual computer for which you're logging onto.

- **Use a personal firewall.** A personal firewall is an extra layer of added protection for helping protect your home network in the following manner:
  - Protects the user from unwanted incoming connection attempts, ultimately allowing the user to control which programs can and cannot access the Internet.
  - Blocks and/or alerts a user about outgoing connection attempts.
  - Monitors and regulates all incoming and outgoing Internet users.

  Personal firewalls have been enabled on the workstation by IT personnel. Personnel (Employees and Non-Employees) are prohibited to disable or change any settings. For assistance, contact IT Technical Support.

- **Be cautious online.** Remember that working from an alternate location, home means you are accessing Citadel Servicing Corporation ’s information requires you to adhere to the same guidelines and procedures under Corporate Policies as when in an Citadel Servicing Corporation office location. Practice caution on what websites you are visiting, information you are downloading, etc. Being cautious and having a "security first" mindset is your responsibility.

- **Change your WI-FI broadcast**. Known technically as an SSID, it is the wireless (if you are using wireless) network you connect to. Make sure to change the default SSID to something more unique. SSID's that are left with their default names often are an indicator to hackers that the passwords are also still the same default that was shipped with the devices. Thus, change both the default SSID and the default password. Your router is the bridge to the Internet, so protect it by removing any default settings. Do not conduct any company business with confidential or sensitive information on a public computer with public wi-fi.

- **Enable MAC filtering.** Additionally, you want to allow wireless access only to trusted devices, by allowing wireless connections only to known MAC address. MAC (Media Access Control) address is a unique identifier attached to most network adapters, which, in this case would be the unique identifier of your laptop wireless adapter.

- **Change default wireless access to your router.** The default password for wireless web access is essentially the same for all of a specified model of a wireless router assigned by the manufacturer.

33.5.10. Internet and Network

Citadel Servicing Corporation 's corporate network resources are intended for legitimate business purposes. All company employees and non-employee authorized users with access to the corporate network will comply with the corporate Internet Usage Security Policy and network use requirements. Personnel (employee and non-employee) are required to take prudent and appropriate actions to avoid the introduction of malicious programs (e.g., viruses and malware) on to the network or servers.

A small percentage of company internet resources may be used on occasion for personal reasons. Personal use does not exempt any employee from the other obligations of this policy, codes of conduct, or any policy, procedure or guideline. Personal use must not interfere with employee job responsibilities, company's IT network, or Email services, either directly or indirectly.

Persons using IT assets, including the Internet, must understand that they do not have any expectation of privacy. All information originated, viewed, sent, received or stored by Citadel Servicing Corporation ’s IT assets, is the property of Citadel Servicing Corporation and is potentially subject to monitoring, including discovery proceedings in legal actions. Therefore, it is recommended that employees consider alternative means of transmission, if a communication is ever intended to be "personal and confidential".

Under no circumstances is an employee authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing company-owned resources and network, including the Internet.

To protect the network and ensure secure communications, Citadel Servicing Corporation utilizes URL filters to limit access to specific web sites and certain types of traffic. Connections creating routing patterns that flood the network with unnecessary traffic are prohibited. If access to a particular internet location is required for business purposes, but is unavailable (likely due to filtering), please make an IT Request.

33.5.11. Email Use

Citadel Servicing Corporation 's email services are intended for legitimate business communication purposes. It is expected that, because email is a networked function, that email users will also comply with internet use requirements.

A small percentage of company resources may be used on occasion for personal reasons. Personal use does not exempt any employee from the other obligations of this policy, codes of conduct, or any policy, procedure or guideline. Personal files and emails must not be stored at or in Citadel Servicing Corporation 's email. Personal use must not interfere with employee job responsibilities, company's IT network, Internet, or Email services, either directly or indirectly.

Sending or forwarding unsolicited email messages, including the sending of "spam", "chain emails" or other advertising material to individuals who do not specifically request such material is prohibited. Sending or forwarding emails that support, promote, or proclaim subjects that include, but are not limited to, harassment, pornography, gambling or hate crime is strictly prohibited.

Appropriate user identification information is required in all email correspondence. Unauthorized use, or forging, of email header information is strictly prohibited.

Automatically forwarding company email to an external destination / account outside Citadel Servicing Corporation network, unless expressly approved as a policy exception, is strictly prohibited.

Be aware that Citadel Servicing Corporation may restrict the type or size of email file attachments (inbound and/or outbound messages) to increase security or system availability.

Personnel who fulfill IT requests are not required by this policy to retrieve back up emails, although they may do so on occasion as a courtesy. If a request is received, it will be handled in accordance with Policy.

33.5.12. Voice / Telephone Communications

Citadel Servicing Corporation 's voice (e.g., telephone systems, equipment and services plans) and network resources are intended for legitimate business purposes. It is expected that, because voice communication is a networked function, that voice users will comply with corporate Internet and network use policies.

A small percentage of company voice and voicemail resources may be used on occasion for personal reasons. Personal use does not exempt any employee from the other obligations of this policy, codes of conduct, or any policy, procedure or guideline. Personal use must not interfere with employee job responsibilities, company's IT network, or Email services, either directly or indirectly.

Persons using IT assets, including telephone and voicemail, must understand that they do not have any expectation of privacy. All information originated, viewed, sent, received or stored by the IT assets, is the property of Citadel Servicing Corporation and is potentially subject to monitoring, including discovery proceedings in legal actions. Therefore, it is recommended that employees consider alternative means of transmission, if a communication is ever intended to be "personal and confidential".

Under no circumstances is an employee authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing company-owned resources and network, including voice communications.

33.5.13. Social Media

Users are prohibited from accessing web sites designed for the sole purpose of posting and sharing personal information. Exceptions require the approval of the Information Security Governance Sub-Committee and must be for documented business purposes. Citadel Servicing Corporation reserves the right to block access to these or other web sites. Citadel Servicing Corporation reserves the right to review any posted information, approved, or otherwise, to ensure compliance. Employees and non-employee staff personnel, are also prohibited from discussing specific Citadel Servicing Corporation business within any personal home pages they may have established on these sites outside of Citadel Servicing Corporation business hours.

33.5.14. Information Assets

Employees are expected to protect the integrity and privacy of Citadel Servicing Corporation 's technology and information assets, including but not limited to, respecting the confidentiality and sensitivity of data and content of emails, files, data, and transmissions.

Confidential electronic files must be password protected, whether stored on a portable device, desktop, or network server. In addition to password protection, electronic confidential files must be encrypted in accordance with corporate Data Encryption and Data Class Protection policies.

Employees will not attempt to circumvent security technology on the IT assets, or any other computing and/or network asset. Accessing or viewing Citadel Servicing Corporation 's information assets without a business reason to do so is strictly prohibited. Legitimate access for business reasons can be requested in adherence to corporate access administration policies and procedures.

Printers used to create hard copy confidential documents will be secured to an area where access is appropriately limited to those with the authority to view the confidential data in the course of their legitimate job responsibilities.

Confidential hard copy files or documents must be secured in a locked cabinet, and will not be left unattended under any circumstance. This is including, but is not limited to pay stubs, personal information, customer identifiable information, and any other non-public information, as described in corporate Data Class Protection policies.

Employees will not destroy or alter data owned by or in the custody of Citadel Servicing Corporation , customers, vendors, or others, unless the activity is a requirement of the employee's legitimate job responsibilities, in which case the corporate Data Retention Policy and Data Class and Protection Policy will be strictly adhered to.

Copying or distributing copyrighted material when neither Citadel Servicing Corporation nor the employee has an active license is strictly prohibited.

33.5.15. Right to Audit

Citadel Servicing Corporation reserves the right to monitor, audit, and record network and system activity, and potentially content. This includes email traffic, internet traffic, network traffic, and voice communications.

33.6. 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.