INTERNET USAGE SECURITY POLICY

2022

7. INTERNET USAGE SECURITY POLICY

POLICY STATEMENT

Employees using Citadel Servicing Corporation company 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 the organization and is potentially subject to monitoring, including discovery proceedings in legal actions.

Use of the Internet by Citadel Servicing Corporation employees are permitted and encouraged where such use supports the goals and objectives of the business. However, access to the Internet through Citadel Servicing Corporation is a privilege and all employees must adhere to the policies concerning such usage.

7.1. OVERVIEW

Internet access is a required tool for conducting business and is granted for the sole purpose of supporting business activities on an as-needed basis for employees to perform their jobs and professional roles.

Citadel Servicing Corporation 's network resources are intended for legitimate business purposes. It is expected that users will comply with corporate policies regarding Internet use requirements.

Users are expected to be familiar with and comply with this policy, and are also required to use their common sense and exercise their good judgment to use the access granted in a safe, responsible, and productive manner.

Acceptable use of the Internet for performing job functions might include:

- Communication between employees and non-employees for business purposes.
- IT technical support downloading software upgrades and patches.
- Review of possible vendor web sites for product information.
- Reference regulatory or technical information.
- Research.

7.2. PURPOSE

The purpose of this policy is to define the appropriate uses of the Internet by Citadel Servicing Corporation employees and network users.

This policy establishes the minimum requirements and responsibilities for the secure connection and use of the Internet and other public networks by Citadel Servicing Corporation employees and contractors, who access the Internet through Citadel Servicing Corporation computing or networking resources.

7.3. 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 applies to all personnel affiliated with third parties who use the Internet with Citadel Servicing Corporation computing or networking resources.

7.4. 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.

7.5. TRAINING

In order to receive Internet access privileges, all employees must complete the Citadel Servicing Corporation computer-based training information security course then pass the accompanying test.

7.6. POLICY

This policy is to manage use of Internet resources to prevent unauthorized access or misuse that could potentially compromise Citadel Servicing Corporation 's network infrastructure, its information assets and cause damage to Citadel Servicing Corporation , its customers and partners.

Citadel Servicing Corporation users must not access the Internet without a proper understanding of the associated personal and business risks. Access to the Internet, aside from electronic mail, is considered a productivity tool to assist employees who have a legitimate business need for such access. Internet access is not considered a fringe benefit and will be managed to protect the corporate network and its data systems and information.

7.6.1. Information Integrity

A. **Information Reliability** — Information acquired from the Internet must be considered suspect until confirmed by separate information from another source. Before using free Internet-supplied information for business decision-making purposes, employees must corroborate the information by consulting other sources.
B. **Virus Checking** — All non-text files downloaded from non-Citadel Servicing Corporation Internet sources must be screened with current virus detection software prior to being used. Downloaded files must be decrypted and decompressed before being screened for viruses.
C. **Software Downloading** — Citadel Servicing Corporation has implemented an automatic software distribution system to install the latest release of licensed software on Citadel Servicing Corporation computers. Employees must not install software on their Citadel Servicing Corporation supplied computers, whether the software was downloaded from the Internet or procured elsewhere.
D. **Spoofing Users** — Before employees release any internal Citadel Servicing Corporation information, enter into any contracts, or order any products through public networks, the identity of the individuals and organizations contacted must be confirmed. Identity confirmation is ideally performed through digital signatures or digital certificates, but in cases where these are not available, other means such as letters of credit, third-party references, and telephone conversations may be used.
E. **User Anonymity** — Misrepresenting, obscuring, suppressing, or replacing a user's identity on the Internet or any Citadel Servicing Corporation electronic communications system is forbidden. The user-name, electronic mail address, organizational affiliation, and related information included with messages or postings must reflect the actual originator of the messages or postings.

F. **Email Attachments** — Employees must not open electronic mail attachments unless they were expected from a trusted sender. When they are expected from a known and trusted sender, attachments must be scanned with a virus package prior to being opened.

G. **Responding to Information Requests** — Employees must never respond to unsolicited requests for personal information, including passwords or credit card numbers, from an electronic mail message. Any such message should be immediately reported to the Information Security department.

H. **Web Page Changes** — Employees must not establish new Internet pages dealing with Citadel Servicing Corporation business, or make modifications to existing web pages dealing with Citadel Servicing Corporation business, unless they have obtained the approval.

I. **Push Technology** — Automatic updating of software or information on Citadel Servicing Corporation computers through background push Internet technology is prohibited unless the involved vendor's system has been tested and approved by Information Security Office.

7.6.2. Information Confidentiality

A. **Posting Materials** — Employees must not post unencrypted Citadel Servicing Corporation material on any publicly-accessible Internet computer that supports anonymous FTP or similar publicly-accessible services, unless the posting of these materials has been approved by the director of Public Relations.

B. **Message Interception** — Citadel Servicing Corporation secret proprietary, or private information must not be sent over the Internet unless it has been encrypted by approved methods.

C. **Security Parameters** — Unless a connection is known to be encrypted, credit card numbers, telephone calling card numbers, fixed logon passwords, and other security parameters that can be used to gain access to goods or services, must not be sent over the Internet in readable form. Encryption processes are permissible if they are approved by the corporate Information Security manager.

D. **Information Exchange** — Citadel Servicing Corporation software, documentation, and all other types of internal information must not be sold or otherwise transferred to any non-corporate party for any purposes other than business purposes expressly authorized by management. Exchanges of software or data between Citadel Servicing Corporation and any third party must not proceed unless a written agreement has been signed. Such an agreement must specify the terms of the exchange, and the ways that the software or data is to be handled and protected. Regular business practices need not involve such a specific agreement since the terms and conditions are implied.

7.6.3. Public Representations

A. **Private Email Addresses** — Employees posting information on any publicly available web site must not include their personal Citadel Servicing Corporation electronic mail address.

B. **Removal of Postings** — Those messages sent to Internet discussion groups, electronic bulletin boards, or other public forums, that include an implied or explicit affiliation with Citadel Servicing Corporation , may be removed if management deems them to be inconsistent with Citadel Servicing Corporation business interests or existing company policy.

C. Citadel Servicing Corporation **Inadvertent Disclosure** — Care must be taken to properly structure comments and questions posted to mailing lists, public news groups, Employees should keep in mind that several separate pieces of information can be pieced together by a competitor to form a picture revealing confidential information that then could be used against Citadel Servicing Corporation . Employees must never post on the Internet the specific computer or network products employed by Citadel Servicing Corporation .

D. **Appropriate Behavior** — Whenever any affiliation with Citadel Servicing Corporation is included with an Internet message or posting, written attacks are strictly prohibited. Employees must not make threats

against another user or organization over the Internet. All Internet messages intended to harass, annoy, or alarm another person are similarly prohibited.

E. **External Representations** — Employees may indicate their affiliation with Citadel Servicing Corporation in mailing lists, chat sessions, and other offerings on the Internet. This may be done by explicitly adding certain words, or it may be implied, for example through an electronic mail address. In either case, whenever workers provide an affiliation, unless they have been expressly designated as a spokes-person of Citadel Servicing Corporation , they also must clearly indicate the opinions expressed are their own, and not necessarily those of Citadel Servicing Corporation . If an affiliation with Citadel Servicing Corporation is provided, political advocacy statements and product or service endorsements also are prohibited unless they have been previously cleared by company management. With the exception of ordinary marketing and customer service activities, all representations on behalf of Citadel Servicing Corporation must be cleared by company management.

F. **Disclosing Internal Information** — Employees must not publicly disclose internal company information through the Internet that may adversely affect Citadel Servicing Corporation , customer relations, or public image unless the approval company management has been obtained. Such information includes, but is not limited to; business prospects, performance analyses, and internal information systems issues and problems. Responses to specific customer electronic mail messages are exempted from this policy.

7.6.4. Intellectual Property Rights

A. **Copyrights** — When at work, or when Citadel Servicing Corporation computing or networking resources are employed, copying of software in a manner that is not consistent with the vendor's license is strictly forbidden. The reproduction, forwarding, or in any other way republishing or redistribution of words, graphics, or other copyrighted materials must be done only with the permission of the author or Owner.

B. **Publicly-Writable Directories** — All publicly-writable directories on Citadel Servicing Corporation Internet-connected computers must be reviewed and cleared each evening. Employees using Citadel Servicing Corporation computers must not be involved in any way with the exchange of pirated software, purloined passwords, stolen credit card numbers, and inappropriate written or graphic material.

7.6.5. Access Control

A. **Inbound User Authentication** — All users wishing to establish a real-time connection with Citadel Servicing Corporation internal computers through the Internet must employ a virtual private network (VPN) product approved by the Information Security department that can encrypt all traffic exchanged. These VPN products also must authenticate remote users at a firewall before permitting access to the Citadel Servicing Corporation internal network.

B. **Remote Machine Security** — Employees who have not installed required software patches or upgrades, or whose systems are virus-infested must be disconnected automatically from the Citadel Servicing Corporation network until they have re-established a secure computing environment. The computers used by all employees employing VPN technology must be remotely scanned automatically to determine that the software is current and that the system has been properly secured.

C. **Restriction of Third-Party Access** — Inbound Internet access privileges must not be granted to third-party vendors, contractors, consultants, temporaries, outsourcing organization personnel or other third parties unless the relevant system manager determines that these individuals have a legitimate business need for such access. These privileges must be enabled only for specific individuals and only for the time period required to accomplish approved tasks.

D. **Data Aggregators** — Employees must not provide their Internet user IDs and passwords to data aggregators, data summarization, and formatting services, or any other third parties.

E. **Internet Service Providers** — With the exception of telecommuters and mobile computer users, employees must not employ Internet service provider accounts and dial-up lines to access the Internet with Citadel Servicing Corporation computers. All Internet activity must pass through Citadel Servicing Corporation firewalls so that access controls and related security mechanisms can be applied. Users must employ their Citadel Servicing Corporation electronic mail address for Internet electronic mail. Use of a personal electronic mail address for this purpose is prohibited.

F. **Browser User Authentication** — Employees must not save fixed passwords in their web browsers. These fixed passwords must be provided each time that a browser is invoked. Browser passwords may be saved if a boot password must be provided each time the computer is powered up, and if a screen saver password must be provided each time the system is inactive for a specified period of time. Citadel Servicing Corporation computer users must refuse all offers by software to place a cookie on their computer so that they can automatically log on the next time that they visit a particular Internet site. Cookies that serve other purposes are permissible.

G. **Establishing Network Connections** — Unless the prior approval of management has been given, employees must not establish Internet or other external network connections that could permit non-Citadel Servicing Corporation users to gain access to Citadel Servicing Corporation systems and information. These connections include the establishment of multi-computer file systems, Internet pages, Internet commerce systems, and FTP servers.

H. **Business Use and Conduct** — Employees of Citadel Servicing Corporation will only perform and conduct approved business activity using the corporate Internet. Any changes outside of normal business activity and practices (e.g., establishing new business channels, purchasing goods and services) over the corporate Internet must have approval of company management.

7.6.6. Personal Use

A. **Personal Use** — Employees who have been granted Internet access and who wish to explore the Internet for personal purposes must do so on personal rather than company time.

- Games, news groups, and other non-business activities must be performed on personal, not company time. Use of Citadel Servicing Corporation computing resources for these personal purposes is permissible as long as the incremental cost of the usage is negligible, no Citadel Servicing Corporation business activity is pre-empted by the personal use, and the usage is not likely to cause either a hostile working environment or a poor behavioral example.

- Employees must not employ the Internet or other internal information systems in such a way that the productivity of other employees is eroded. Examples of this include chain letters and broadcast charitable solicitations. Citadel Servicing Corporation computing resources must not be resold to other parties or used for any personal business purposes such as running a consulting business on off-hours.

B. **Offensive Web Sites** — Citadel Servicing Corporation is not responsible for the content that employees may encounter when they use the Internet. When and if users make a connection with web sites containing objectionable content, they must promptly move to another site or terminate their session. Employees using Citadel Servicing Corporation computers who discover they have connected with a web site that contains sexually explicit, racist, sexist, violent, or other potentially offensive material must immediately disconnect from that site.

C. **Blocking Sites and Content Types** — The ability to connect with a specific web site does not in itself imply that users of Citadel Servicing Corporation systems are permitted to visit that site. Citadel Servicing

Corporation may, at its discretion, restrict or block the downloading of certain file types that are likely to cause network service degradation. These file types include graphic and music files.

D. **Use of Social Networking sites** — 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 Office and must be for documented business purposes. Citadel Servicing Corporation reserves the right to block access to these or other web sites. Employees 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.

7.6.7. Privacy Expectations

A. **No Default Protection** — Employees using Citadel Servicing Corporation information systems or the Internet must realize that their communications are not automatically protected from viewing by third parties. Unless encryption is used, employees must not send information over the Internet if they consider it to be confidential or private.

B. **Management Review** — At any time and without prior notice, Citadel Servicing Corporation management reserves the right to examine electronic mail messages, files on personal computers, web browser cache files, web browser bookmarks, logs of web sites visited, computer system configurations, and other information stored on or passing through Citadel Servicing Corporation computers.

C. **Logging** — Citadel Servicing Corporation routinely logs the web sites visited, files downloaded, time spent on the Internet, and related information. Department managers receive reports of such information and use it to determine what types of Internet usage are appropriate for their department's business activities.

D. **Junk Electronic Mail** — Users must not use Citadel Servicing Corporation computer systems for the transmission of unsolicited bulk electronic mail advertisements or commercial messages that are likely to trigger complaints from the recipients reporting security problems.

E. **Sensitive Information** — Users are strictly prohibited from posting, uploading or discussing sensitive information. The term "sensitive information" may include, but is not limited, to the following:

   a. Internal policies and procedures and other Standard Operating Procedure (SOP) documents.
   b. Company-wide operational and information technology attributes.
   c. Financial data and accounting data, management meeting minutes, employee personnel files.
   d. Client provided data and information.
   e. Contractual documents (SOW, SLA, MSA, etc.).
   f. Any confidential Intellectual Property.

7.6.8. Security

A. **Notification Process** — If sensitive Citadel Servicing Corporation information is lost, disclosed to unauthorized parties, or suspected of either, the Information Security Office must be notified immediately. If any unauthorized use of Citadel Servicing Corporation information systems is suspected of taking place, the corporate Information Security Office must be notified immediately.

B. **False Security Reports** — Employees in receipt of information about system vulnerabilities must forward it to the corporate Information Security manager, who then will determine what if any action is appropriate. Employees must not personally redistribute system vulnerability information to other users.

C. **Testing Controls** — Employees must not test or probe security mechanisms at either Citadel Servicing Corporation or other Internet sites unless they have obtained written permission from the corporate Information Security Office. The possession or the usage of tools for detecting information system

vulnerabilities, or tools for compromising information security mechanisms, are prohibited without the advance permission of the corporate Information Security Office.

7.7. 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.