ELECTRONICS COMMUNICATION POLICY

2022

25. ELECTRONICS COMMUNICATION POLICY

POLICY STATEMENT

Citadel Servicing Corporation provides and maintains a number of electronic communication and messaging systems to communicate information and data inside and outside Citadel Servicing Corporation to staff and clients for business purposes.

Citadel Servicing Corporation will ensure that proper rules, guidelines, and processes are in place to oversee and ensure proper governance and use of company electronic communication systems to prevent misuse and unauthorized access.

25.1. OVERVIEW

Citadel Servicing Corporation provides and maintains a number of electronic communications and messaging systems (e.g., E-mail, telephony, voice mail, instant messaging, etc.) to communicate information and data inside and outside Citadel Servicing Corporation to staff and clients.

Citadel Servicing Corporation recognizes the importance of managing these resources to prevent the loss and/or misuse of corporate and client data that may impact or compromise corporate and client systems, data, business operations, and reputation.

As a condition of providing this technology, Citadel Servicing Corporation enforces standards regarding electronic communications systems use to ensure alignment with corporate policies governing appropriate workplace conduct and behavior.

25.2. PURPOSE

The purpose of this policy is to ensure the proper use of company electronic communication systems and facilitate awareness of acceptable and unacceptable use of these systems. This policy defines the requirements for all staff when working with company electronic communications systems and data.

25.3. SCOPE

This policy applies to all Citadel Servicing Corporation computer systems and facilities, including those managed for company customers. This policy applies to all employees, partners, contractors, consultants, other workers, outsourced services providers, and third-parties (and all personnel affiliated with third parties) with access to company information assets.

This policy covers appropriate use of any electronic message and/or data sent from a corporate electronic messaging system and/or agent. This policy applies whether the electronic communication is accessed from company networks or via any remote location.

25.4. 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.

25.5. POLICY

All use of electronic communication systems must be consistent with company policies and procedures of ethical conduct, safety, compliance with applicable laws, and proper business practices. For questions regarding use, refer to corporate acceptable use policies for guidance or contact your manager or the human resources department.

Internal communications systems, including equipment and data stored, are the property of Citadel Servicing Corporation . All communication and information transmitted by, received from, or stored in company systems are the property of Citadel Servicing Corporation and are to be used primarily for job-related purposes.

Citadel Servicing Corporation permits employees to send and/or receive personal messages (e.g., via E-mail), within reason. Personal use of these electronic communication systems must not interfere with or conflict with business use.

All corporate data contained within an electronic message or an attachment must be secured.

Electronic messages and data (e.g., E-mail, etc.) will be retained if it qualifies as a company business record. It is a company business record if there is a legitimate and ongoing business reason to preserve the information contained in the message.

Citadel Servicing Corporation reserves the right to retrieve and review any message or file composed, sent, or received. Although e-mail and voice mail may use passwords for security, confidentiality cannot be guaranteed. It is possible for messages to be retrieved and viewed by someone other than the intended recipient.

Citadel Servicing Corporation complies with all applicable federal, state, and local laws, including but not limited to those that concern the employer/employee relationship. Nothing contained herein will be construed to violate any of the rights or responsibilities contained in such laws.

25.5.1. Prohibited Use of Electronic Communication Systems

E-mail, voice mail, and other electronic communications transmitted on Citadel Servicing Corporation equipment, systems, or networks may not contain any content that would reasonably be considered offensive, harassing, or disruptive to another individual. Offensive content includes, but is not limited to, sexual comments or images, racial slurs, gender-specific comments, or any comments that might be construed as offensive by a reasonable person on the basis of race, age, sex, sexual orientation, religious, political beliefs, national origin, or disability.

Regarding Internet and e-mail access and use, employees will be advised that Citadel Servicing Corporation expressly prohibits use of the Citadel Servicing Corporation provided Internet and e-mail for the following activities:

- Dissemination or printing of copyrighted materials, including articles and software, in violation of copyright laws.
- Sending, receiving, printing, or otherwise disseminating proprietary data, trade secrets, or other confidential information of Citadel Servicing Corporation or its business counterparts in violation of company policy or proprietary agreements.
- Using offensive or harassing statements or language, including disparagement of others based on their race, national origin, sex, sexual orientation, age, disability, religious, or political beliefs.

- Gambling or engaging in any other activity in violation of local, state, or federal law.
- Circulating jokes, comics, or non-job-related computer graphics.

25.5.2. Access to Employee Electronic Communications Data and Logs

Per Citadel Servicing Corporation HR & Legal guidance, the process below is required when requesting access to an employee's Internet, voice communication, and data access information. This process is to ensure that Citadel Servicing Corporation is adhering to employee privacy laws and not misusing the data it collects.

A. Active Employees/Contractors:

1. Written/e-mail approval from the employee's manager and Department Manager with approval from Human Resources.
2. Manager submits a General Service Request to IT with approvals attached.
3. The requested information will be provided to the employee's manager and must be handled confidentially.
4. If warranted, the Citadel Servicing Corporation HR / Legal Partner may be required to approve prior to release of information, as determined by the employee's manager.

B. Former Employees/Contractors:

1. Written/e-mail approval from the employee's manager.
2. Written/e-mail approval from the employee's HR Partner.
3. Manager submits a General Service Request to IT with approvals attached.
4. The requested information will be provided to the employee's manager and must be handled confidentially.
5. If warranted, the Citadel Servicing CorporationHR / Legal Partner may be required to approve prior to release of information, as determined by the employee's manager.

C. Voice or E-mail Communications Access — Special Provisions:

For access to an employee's voice or e-mail communication, please complete an Electronic Records Authorization request. The request must be approved by both an Citadel Servicing Corporation Department Legal & Human Resources Partner.

25.5.3. Recording of Telephone Calls

Citadel Servicing Corporation strictly adheres to California State privacy laws and the California wiretapping law. This applies to recording conversations and the requirement for "two-party consent". In the state of California, it is a violation to record or eavesdrop on any confidential communication, including a private conversation or telephone call, without the consent of all parties to the conversation. Citadel Servicing Corporation reminds employees to have both the authority and consent before recording conversations with any party (employees, contractors, partners & customers).

Reference: California Penal Code § 632

25.5.4. Internal Monitoring

Citadel Servicing Corporation reserves the right at any time to monitor, access, retrieve, read, or disclose internal communications when a legitimate business need exists that cannot be satisfied by other means, the involved individual is unavailable and timing is critical to a business activity, there is reasonable cause to suspect criminal activity or policy violation, or monitoring is required by law, regulation, or third-party agreement.

Citadel Servicing Corporation may log web sites visited, files downloaded, and related information exchanges over the Internet. Citadel Servicing Corporation may record the numbers dialed for telephone calls placed through

its telephone systems. Department managers may receive reports detailing the usage of these and other internal information systems and are responsible for determining that such usage is both reasonable and business-related.

All files and messages stored on corporate information systems are routinely backed up to tape, disk, and other storage media. This means that information stored on corporate information systems, even if a worker has specifically deleted it, is often recoverable and may be examined at a later date by system administrators and others designated by management.

Citadel Servicing Corporation management reserves the right to examine archived electronic mail, personal computer file directories, hard disk drive files, and other information stored on corporate information systems. This information may include personal data. Such examinations are typically performed to assure compliance with internal policies, support the performance of internal investigations, and assist with the management of corporate information systems.

25.5.5. Disclosure of Personal Data

Citadel Servicing Corporation may provide third parties with personal data processed on its systems for generally accepted business purposes such as court orders, subpoenas, employment verification, governmental licensing, underwriting, and other reasons. All recipients of such information must definitively identify themselves, certify in writing the legal and customary purposes for which the information is sought and certify that the personal data will be used for no other purposes. All disclosures will follow approved corporate procedures to ensure that Citadel Servicing Corporation is adhering to all relevant privacy laws and not misusing the data.

25.5.6. Confidentiality and Security

Citadel Servicing Corporation implements and maintains appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction, accidental loss, unauthorized alteration, and unauthorized disclosure or access in accordance with all applicable federal, state, and local laws.

25.6. 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.

Disciplinary action for violation of this policy may include termination, suspension or transfer of the offending employee. In cases involving less serious violations, disciplinary action may consist of a warning or reprimand. Remedial action may also include counseling, changes in work assignments or other measures designed to prevent future misconduct. The measure of discipline will correspond to the gravity of the offense as weighed by its potential effect on Citadel Servicing Corporation and fellow employees.

Nothing in this policy will be construed to prohibit conduct that is expressly permitted or protected under applicable federal, state or local laws.