Acceptable Use Policy, version 1.0.0

Status: ☐ Working Draft ☒ Approved ☐ Adopted

Document Owner: Clean Claims

Last Review Date: March 2025

Acceptable Use Policy

Purpose

The purpose of the Clean Claims Acceptable Use Policy is to establish acceptable practices regarding the use of Clean Claims **Information Resources** in order to protect the confidentiality, integrity and availability of information created, collected, and maintained.

Audience

The Clean Claims Acceptable Use Policy applies to any individual, entity, or process that interacts with any Clean Claims **Information Resource**.

Contents

Policy

Acceptable Use

- Personnel are responsible for complying with Clean Claims policies when using Clean Claims information resources and/or on Clean Claims time. If requirements or responsibilities are unclear, please seek assistance from the Information Security Committee.
- Personnel must promptly report harmful events or policy violations involving Clean Claims assets or information to their manager. Events include, but are not limited to, the following:
    - Technology incident: any potentially harmful event that may cause a failure, interruption, or loss in availability to Clean Claims **Information Resources**.
    - Data incident: any potential loss, theft, or compromise of Clean Claims information.
    - Unauthorized access incident: any potential unauthorized access to a Clean Claims **Information Resource**.
    - Policy violation: any potential violation to this or other Clean Claims policies, standards, or procedures.
- Personnel should not purposely engage in activity that may
    - harass, threaten, impersonate, or abuse others;
    - degrade the performance of Clean Claims **Information Resources**;
    - deprive authorized Clean Claims personnel access to a Clean Claims **Information Resource;**
    - obtain additional resources beyond those allocated;
    - or circumvent Clean Claims computer security measures.
- Personnel should not download, install, or run security programs or utilities that reveal or exploit weakness in the security of a system. For example, Clean Claims personnel should not run password cracking programs, packet sniffers, port scanners, or any other non-approved programs on any Clean Claims **Information Resource**.
- All inventions, intellectual property, and proprietary information, including reports, drawings, blueprints, software codes, computer programs, data, writings, and technical information, developed on Clean Claims time and/or using Clean Claims **Information Resources** are the property of Clean Claims.
- Use of encryption should be managed in a manner that allows designated Clean Claims personnel to promptly access all data.
- Clean Claims **Information Resources** are provided to facilitate company business and should not be used for personal financial gain.
- Personnel are expected to cooperate with incident investigations, including any federal or state investigations.
- Personnel are expected to respect and comply with all legal protections provided by patents, copyrights, trademarks, and intellectual property rights for any software and/or materials viewed, used, or obtained using Clean Claims **Information Resources**.
- Personnel should not intentionally access, create, store or transmit material which Clean Claims may deem to be offensive, indecent, or obscene.

Access Management

- Access to information is based on a "**need to know**".

- Personnel are permitted to use only those network and host addresses issued to them by Clean Claims IT and should not attempt to access any data or programs contained on Clean Claims systems for which they do not have authorization or explicit consent.
- All remote access connections made to internal Clean Claims networks and/or clients environments must be made through approved, and Clean Claims-provided, virtual private networks (VPNs).
- Personnel should not divulge any access information to anyone not specifically authorized to receive such information, including IT support personnel.
- Personnel must not share their (personal authentication information, including:
    - Account passwords,
    - Personal Identification Numbers (PINs),
    - Security Tokens (i.e. Smartcard),
    - Multi-factor authentication information
    - Access cards and/or keys,
    - Digital certificates,
    - Similar information or devices used for identification and authentication purposes.
- Lost or stolen security tokens must be reported to physical security personnel as soon as possible.
- A service charge may be assessed for security tokens that are lost, stolen, or are not returned.

Authentication/Passwords

- All personnel are required to maintain the confidentiality of personal authentication information.
- Any group/shared authentication information must be maintained solely among the authorized members of the group.
- All passwords, including initial and/or temporary passwords, must be constructed, and implemented according to the following Clean Claims rules:
    - Must meet all requirements including minimum length, complexity, and reuse history.
    - Must not be easily tied back to the account owner by using things like username, social security number, nickname, relative's names, birth date, etc.
    - Must not be the same passwords used for non-business purposes.
- Unique passwords should be used for each system, whenever possible.
- User account passwords must not be divulged to anyone. Clean Claims support personnel and/or contractors should never ask for user account passwords.
- If the security of a password is in doubt, the password should be changed immediately.
- Personnel should not circumvent password entry with application remembering, embedded scripts or hard coded passwords in client software.

Clear Desk/Clear Screen

- Personnel should log off from applications or network services when they are no longer needed.
- Personnel should log off or lock their workstations and laptops when their workspace is unattended.
- Electronic keys used to access **confidential information** should not be left in an unattended workspace if the workspace itself is not physically secured.

- Passwords must not be posted on or under a computer or in any other physically accessible location.

TOP

Data Security

- Personnel should use approved encrypted communication methods whenever sending **confidential information** over public computer networks (Internet).
- Only authorized **cloud computing applications** may be used for sharing, storing, and transferring **confidential** or **internal information**.
- Information must be appropriately shared, handled, transferred, saved, and destroyed, based on the information sensitivity.
- Personnel should not have confidential conversations in public places or over insecure communication channels, open offices, and meeting places.
- **Confidential information** must be transported either by an Clean Claims employee or a courier approved by Management.
- All electronic media containing confidential information must be securely disposed. Please contact Management for guidance or assistance.

TOP

Email and Electronic Communication

- Electronic communications should not misrepresent the originator or Clean Claims.
- Personnel are responsible for the accounts assigned to them and for the actions taken with their accounts.
- Accounts must not be shared without prior authorization from Clean Claims, with the exception of calendars and related calendaring functions.
- Employees should not use personal email accounts to send or receive Clean Claims **confidential information**.
- Any personal use of Clean Claims provided email should not:
    - Involve solicitation.
    - Be associated with any political entity.
    - Have the potential to harm the reputation of Clean Claims.
    - Forward chain emails.
    - Contain or promote anti-social or unethical behavior.
    - Violate local, state, federal, or international laws or regulations.
    - Result in unauthorized disclosure of Clean Claims **confidential information**.
    - Or otherwise violate any other Clean Claims policies.
- Personnel should only send **confidential information** using approved secure electronic messaging solutions.
- Personnel should use caution when responding to, clicking on links within, or opening attachments included in electronic communications.
- Personnel should use discretion in disclosing **confidential** or **internal information** in Out of Office or other automated responses, such as employment data, internal telephone numbers, location information or other sensitive data.

TOP

Hardware and Software

- All hardware must be formally approved by Management before being connected to Clean Claims or client's networks.
- Personnel traveling to a High-Risk location, as defined by FBI and Office of Foreign Asset control, must contact IT for approval to travel with corporate assets.
- Employees should not allow family members or other non-employees to access Clean Claims **Information Resources**.

Mobile Devices and Bring Your Own Device (BYOD)

- The use of a **personally owned mobile device** to connect to the Clean Claims network is a privilege granted to employees and contractors only upon formal Management approval.
- All **personally owned** laptops and/or workstations must have approved virus and spyware detection/protection software along with personal firewall protection active.
- Mobile devices that access Clean Claims email must have a PIN or other authentication mechanism enabled.
- **Confidential information** should only be stored on devices that are encrypted in compliance with the Clean Claims.
- Clean Claims **confidential information** should not be stored on any personally owned **mobile device**.
- Theft or loss of any **mobile device** that has been used to create, store, or access **confidential** or **internal information** must be reported to the Clean Claims Management immediately.
- All **mobile devices** must maintain up-to-date versions of all software and applications.
- All personnel are expected to use **mobile devices** in an ethical manner.
- **Jail-broken** or rooted devices should not be used to connect to Clean Claims **Information Resources**.
- Clean Claims Management may choose to execute "**remote wipe**" capabilities for **mobile devices** without warning
- In the event that there is a suspected **incident** or breach associated with a **mobile device**, it may be necessary to remove the device from the personnel's possession as part of a formal investigation.
- All mobile device usage in relation to Clean Claims **Information Resources** may be monitored, at the discretion of Clean Claims Management.
- Clean Claims IT support for **personally owned mobile devices** is limited to assistance in complying with this policy. Clean Claims IT support may not assist in troubleshooting device usability issues.
- Use of **personally owned** devices must be in compliance with all other Clean Claims policies.
- Clean Claims reserves the right to revoke **personally owned mobile device** use privileges in the event that personnel do not abide by the requirements set forth in this policy.
- Texting or emailing while driving is not permitted while on company time or using Clean Claims resources. Only hands-free talking while driving is permitted, while on company time or when using Clean Claims resources.

Removable Media

- The use of **removable media** for storage of Clean Claims information must be supported by a reasonable business case.
- All **removable media** use must be approved by Clean Claims prior to use.
- **Personally, owned removable media** use is not permitted for storage of Clean Claims information.
- Personnel are not permitted to connect **removable media** from an unknown origin without prior approval from the Clean Claims.
- Confidential and internal Clean Claims information should not be stored on **removable media** without the use of encryption.
- All removable media must be stored in a safe and secure environment.
- The loss or theft of a **removable media** device that may have contained any Clean Claims information must be reported to the Clean Claims.

Security Training and Awareness

- All new personnel must complete an approved **security awareness** training class prior to, or at least within 30 days of, being granted access to any Clean Claims **Information Resources**.
- All personnel must be provided with and acknowledge they have received and agree to adhere to the Clean Claims Information Security Policies before they are granted to access to Clean Claims **Information Resources**.
- All personnel must complete the annual security awareness training.

Social Media

- Communications made with respect to social media should be made in compliance with all applicable Clean Claims policies.
- Personnel are personally responsible for the content they publish online.
- Creating any public social media account intended to represent Clean Claims, including accounts that could reasonably be assumed to be an official Clean Claims account, requires the permission of Clean Claims Management.
- When discussing Clean Claims or Clean Claims -related matters, you should:
    - Identify yourself by name,
    - Identify yourself as an Clean Claims representative, and
    - Make it clear that you are speaking for yourself and not on behalf of Clean Claims, unless you have been explicitly approved to do so.
- Personnel should not misrepresent their role at Clean Claims.
- When publishing Clean Claims-relevant content online in a personal capacity, a disclaimer should accompany the content. An example disclaimer could be; “The opinions and content are my own and do not necessarily represent Clean Claims Claims’ position or opinion.”
- Content posted online should not violate any applicable laws (i.e. copyright, fair use, financial disclosure, or privacy laws).
- The use of discrimination (including age, sex, race, color, creed, religion, ethnicity, sexual orientation, gender, gender expression, national origin, citizenship, disability, or marital status or

any other legally recognized protected basis under federal, state, or local laws, regulations, or ordinances) in published content that is affiliated with Clean Claims will not be tolerated.

- **Confidential information**, internal communications and non-public financial or operational information may not be published online in any form.
- Personal information belonging to customers may not be published online.

Third Party Risk Management

All third-party service providers and contractors with access to Clean Claims and its clients IT systems or data are to be identified and evaluated annually. The evaluation will include identifying parties who no longer require access, the process will result in the removal of access that is no longer required.

Cloud services that have been purchased without formal approval or documentation are to be identified and assessed for removal.

References

- ISO 27002: 6, 7, 8, 9, 11, 12, 13, 16, 18
- NIST CSF: PR.AC, PR.AT, PR.DS, DE.CM, DE.DP, RS.CO
- NYDFS 500.07,500.03
- SOC2 CC 6.4.1, 6.4.2, 6.4.3
- FRSecure a full-service information security consultancy. https://frsecure.com/

Waivers

Waivers from certain policy provisions may be sought following the Clean Claims Waiver Process.

Enforcement

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

Version History

Version	Modified Date	Approved Date	Approved By	Reason/Comments
1.0.0	March 2025	March 2025	Clean Claims	Document Origination