Acceptable Use Policy (AUP)

Purpose

Appropriate use of Acutis Workspaces in Acutis Cloud Enclave (ACE™) and effective security of those resources. Inappropriate use exposes the Acutis Cloud Enclave (ACE™) to potential risks including virus attacks, compromise of network systems and services, and legal issues.

Scope

This policy applies to users of any system's information or physical infrastructure regardless of its form or format, created or used to support the Acutis Cloud Enclave (ACE™) and Workspaces. It is the user's responsibility to read and understand this policy and to conduct their activities in accordance with its terms.

Authority

Business owner or CEO.

Access controls: Access to the secure cloud enclave is restricted to authorized personnel only. Users are granted access based on their job responsibilities and must use strong authentication methods such as multi factor authentication. The cloud enclave may be accessed only from authorized devices.

Confidentiality: All data stored within the secure cloud enclave is considered confidential and must be protected from unauthorized disclosure. Users must not share any confidential information with unauthorized individuals or use the data for any purpose other than authorized business activities. Data stored within the enclave is encrypted according to **FIPS 140-2 cryptography**. Any data that is transmitted outside of the secure cloud enclave must be encrypted and transmitted via secure encrypted email.

Integrity: Users must ensure that the data stored in the secure cloud enclave is accurate, complete, and up-to-date. They must take measures to prevent unauthorized modification or destruction of data, such as using strong passwords and limiting access to critical systems. Data classifications apply for CUI and kindly refer to https://www.archives.gov/cui/registry/category-list website on information related to data classifications and categorization.

Availability: The secure cloud enclave must be available to authorized users at all times. Users must not engage in any activities that may cause the system to become unavailable, such as running unauthorized applications or launching denial-of-service attacks.

Acceptable use: Users must not use the secure cloud enclave for any illegal or unethical purposes. They must not engage in any activity that may compromise the security of the system or other users' data, such as attempting to bypass security controls or probing for vulnerabilities.

User Compliance:
Users must also comply with all applicable laws, regulations, and organizational policies. All users of the Acutis Cloud Enclave (ACE™) and Workspaces

- Cannot use social media sites such as facebook, twitter, instagram, snapchat, whatsapp, linkedin, etc.
- Cannot use company resources such as USB drives, network storage devices, computers and network to post to an employees personal social media accounts
- Cannot engage in illegal activities. This includes engaging in hate speech against others based on race, religion or gender, or anything related to social as well as engaging in political dialogues,
- Cannot divulge any confidential information, trade secrets or government information
- Cannot misrepresent their employer
- Cannot defame competitors

Incident reporting: Users must report any suspected or actual security incidents, including unauthorized access or data breaches, to the appropriate authorities. Users must also cooperate with any investigations or audits related to security incidents.

Penalties for violations: Violations of this AUP may result in disciplinary action, up to and including termination of employment or contract, and legal action as applicable.