ETQ Acceptable Use Policy

This Acceptable Use Policy (this **"Policy"**) describes prohibited uses of the Services offered by Hexagon Manufacturing Intelligence, Inc. ("**Hexagon**"). The examples described in this Policy are not exhaustive. Hexagon may modify this Policy at any time by posting a revised version at https://www.etq.com/app/uploads/2020/08/etq-acceptable-use-policy.pdf. By using the Services, you agree to the most recent version of this Policy. If you violate the Policy or authorize or help others to do so, Hexagon may suspend or terminate your use of the Services. This Policy governs the use of the ETQ Reliance® Services and related products by Customer under the terms of the Master Subscription Agreement (the "Agreement") between Hexagon and the Customer that is a party to the Agreement and is incorporated into the Agreement by reference. This Policy applies separately to each account using the Services. Capitalized terms will have the meaning specified in the Agreement.

Effective Date: April 1, 2024

1. **No Illegal, Harmful, or Offensive Use or Content.** Customers may not use, or encourage, promote, facilitate or instruct third parties, including its users, to use, the Services for any illegal, harmful, fraudulent, infringing or offensive use, or to transmit, store, display, distribute or otherwise make available content that is illegal, harmful, fraudulent, infringing or offensive. Prohibited activities or content include:

    - Any activities or content that are illegal, that violate the rights of others, including publicity or privacy rights, encourages conduct that would violate any applicable laws, or that may be harmful to others, Hexagon's operations or reputation.
    - Content that infringes or misappropriates the intellectual property or proprietary rights of others.
    - Content that is defamatory, obscene, abusive, hate-related or violent, that advocates discrimination or is otherwise objectionable.
    - Malicious code, including viruses, worms, built-in or use-driven destruction mechanisms, injurious or damaging algorithms, time bombs, Trojan horses or other software or hardware that can disable or adversely affect the Services.

2. **No Security Violations.** Customers may not use the Services to violate the security or integrity of any network, computer or communications system, software application, or network or computing device (each, a "System"). Prohibited activities include:

    - **Unauthorized Access.** Accessing or using any System without permission, including attempting to probe, scan, or test the vulnerability of a System or to breach any security or authentication measures used by a System.
    - **Interception.** Monitoring of data or traffic on a System without permission.
    - **Falsification of Origin.** Forging TCP-IP packet headers, e-mail headers, or any part of a message describing its origin or route. The legitimate use of aliases and anonymous remailers is not prohibited by this provision.

3. **No Network Abuse.** Customers may not make network connections to any users, hosts, or networks unless you have permission to communicate with them. Prohibited activities include:

    - **Monitoring or Crawling.** Monitoring or crawling of a System that impairs or disrupts the System being monitored or crawled.
    - **Denial of Service (DoS).** Inundating a target with communications requests so the target either cannot respond to legitimate traffic or responds so slowly that it becomes ineffective.
    - **Intentional Interference.** Interfering with the proper functioning of any System, including any deliberate attempt to overload a system by mail bombing, news bombing, broadcast attacks, or flooding techniques.
    - **Operation of Certain Network Services.** Operating network services like open proxies, open mail relays, or open recursive domain name servers.
    - **Avoiding System Restrictions.** Using manual or electronic means to avoid any use limitations placed on a System, such as access and storage restrictions.

4. **No E-Mail or Other Message Abuse.** Customers may not distribute, publish, send, or facilitate the sending of unsolicited mass e-mail or other messages, promotions, advertising, or solicitations (like "spam"), including commercial advertising and informational announcements. Customers may not alter or obscure mail headers or assume a sender's identity without the sender's explicit permission. Customers may not collect replies to messages sent from another internet service provider if those messages violate this Policy or the acceptable use policy of that provider.

5. **Our Monitoring and Enforcement.** We reserve the right, but do not assume the obligation, to investigate any violation of this Policy or misuse of the Services, including:

    - Investigating violations of this Policy or misuse of the Services; or

- Removing, disabling access to, or modifying any content or resource that violates this Policy or any other agreement we have with you for use of the Services.

We may report any activity that we suspect violates any law or regulation to appropriate law enforcement officials, regulators, or other appropriate third parties. Our reporting may include disclosing appropriate customer information. We also may cooperate with appropriate law enforcement agencies, regulators, or other appropriate third parties to help with the investigation and prosecution of illegal conduct by providing network and systems information related to alleged violations of this Policy.

6. Reporting of Violations of this Policy

If you become aware of any violation of this Policy, you will immediately notify us and provide us with assistance, as requested, to stop or remedy the violation. To report any violation of this Policy, please contact legal.etq.mi@hexagon.com.