PROVATION ACCEPTABLE USE POLICY

This Acceptable Use Policy (this "Policy") describes prohibited uses of the Provation Software-as-a-Service (the "Service") offerings provided by ProVation Software, Inc. ("Provation"). This Policy is in addition to any other terms and conditions under which Provation provides the Service to you. Notwithstanding the foregoing, in the event of a conflict between the terms of this Policy and the terms of the Agreement pursuant to which you purchased the Service (the "Agreement"), the terms of the Agreement will prevail.

You are solely responsible and liable for the completeness, integrity, quality, accuracy and content input into or stored using the Service or transmitted through the Service, and Provation has no responsibility for any offensive material contained therein, any infringement of third-party intellectual property rights arising therefrom, or any crime facilitated thereby. Notwithstanding the foregoing, Provation is not under any obligation to verify, authenticate, monitor, or edit the Customer Content or any other content input into or stored using the Service by Customer.

The examples listed in this Policy are not exhaustive. We may modify this Policy at any time by posting a revised version of this document at **https://provationmedical.com/apex-documents**. Revisions are effective immediately upon posting. By using the Service, you agree to the latest version of this Policy. Accordingly, we recommend that you visit the website regularly to ensure that your activities conform to the most recent version. You are solely responsible for your actions and the actions of your end users using the Service under your account. During the term of the Agreement, you acknowledge and agree to the following responsibilities:

No Illegal, Harmful, or Offensive Use or Content

You may not use, encourage, promote, facilitate, or instruct others to use the Service for any illegal, harmful, or offensive use, or to access, send, receive, disclose, transmit, store, display, distribute or otherwise make available content that is illegal, harmful, or offensive. Prohibited activities or content include but are not limited to:

- **Violating any Law**. Violating any local, state, national, and international laws, and regulations applicable to Customer's use of the Service, including without limitation, the provision and storage of content of, or committing conduct that is tortuous or unlawful in, any applicable jurisdiction.
- **Harmful or Fraudulent Activities**. Activities that may be harmful to others, our operations or reputation, including offering or disseminating fraudulent goods, Service, schemes, or promotions (e.g., make money fast schemes, ponzi and pyramid schemes, phishing, or pharming), or engaging in other deceptive practices.
- **Infringing Content**. Sending or storing content that violates, infringes, or misappropriates the intellectual property or proprietary rights of any individual or entity in any jurisdiction.
- **Offensive Content**. Content that is obscene, pornographic, lewd, lascivious, or excessively violent, regardless of whether the material or its dissemination is unlawful.
- **Harmful Content**. Content or other computer technology that may damage, interfere with, surreptitiously intercept, or expropriate any system, program, or data, including viruses, malware, Trojan horses, worms, time bombs, or cancelbots.
- **Harmful Conduct.** Content advocating or encouraging violence against any government, organization, group, individual or property, or providing instruction, information, or assistance in causing or carrying out such violence, regardless of whether such activity is unlawful. Transmitting or posting any material that encourages conduct that could constitute a criminal offense or give rise to civil liability.

No Security Violations

You may not use the Service 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 but are not limited to:

- **Unauthorized Access**. Accessing or using any System without permission, including attempting to (i) probe, scan, or test the vulnerability of a System, (ii) breach any security or authentication measures used by a System, (iii) gain unauthorized access to the Service or a System, or (iv) access or use the Service in a way intended to avoid incurring fees or exceeding usage limits.

- **Interfering**. Interfering with or disrupting any System or others' ability to access or use the Service by use of any program, script, command, or otherwise.

- **Viruses**. Introducing, activating, or uploading in anyway any information or content that contain viruses, worms, time bombs, Trojan horses and other harmful or malicious code, files, scripts, agents or programs, or data that may damage the operation of the Service or any System.

- **Falsification of Origin**. Forging TCPIP packet headers, email headers, or any part of a message describing its origin or route. This prohibition does not include the use of aliases or anonymous remailers.

- **Privacy.** Invading anyone's privacy by attempting to harvest, collect, store, or publish private or personally identifiable information, such as passwords, account information, credit card numbers, addresses, or other contact information without their knowledge and consent.

No Network Abuse
You may not make network connections to any users, hosts, or networks unless you have permission to communicate with them. Prohibited activities include but are not limited to:

- **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 Service**. Operating network Service 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.

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 Service. If you are in violation of this policy or any other Provation policy, at any time, as determined by Provation in its sole discretion:

- remove, disable access to, or modify content that violates this Policy or the Agreement we have with you for use of the Service; and/or
- suspend or terminate your Provation account without limiting any other rights or remedies that Provation may have under the Agreement.

We may report any activity that we suspect violates any law or regulation to appropriate law enforcement officials, regulators, or other appropriate third parties which 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.

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.