ALTINITY.CLOUD RESPONSIBLE DISCLOSURE POLICY

1. **Preamble.** Data security is a top priority for Altinity. We believe that working with independent security researchers is an effective way to ensure the highest possible level of security in our products. We also encourage users to report potential security vulnerabilities immediately. We will work with you to resolve the issue as quickly as possible.

   Thank you for helping to keep Altinity.Cloud and our users safe!

2. **Disclosure Policy:**

   2.1. You may perform such research as is necessary and sufficient to disclose vulnerabilities in Altinity products and services fully.
   2.2. If you believe you have discovered a potential vulnerability, please let us know by emailing us at security@altinity.com. We will acknowledge your email within five business days.
   2.3. Provide us with a reasonable amount of time to resolve the issue before disclosing it to the public or a third party. We aim to resolve critical issues within 24 hours of disclosure.
   2.4. Make a good faith effort to avoid violating privacy, destroying data, or interrupting or degrading the Altinity.Cloud service. Please only interact with accounts you own or for which you have explicit permission from the account holder.

3. **Prohibited Activities:** You may not perform the following without written permission from Altinity, Inc.:

   3.1. Distributed Denial of Service (DDoS)
   3.2. Spamming
   3.3. Social engineering or phishing of Altinity employees or contractors
   3.4. Any attacks against Altinity physical property, online services or data centers

4. **Changes:** We may revise this policy from time to time. The most current version of the policy is available at https://altinity.com/legal.

5. **Contact:** Altinity is always open to feedback, questions, and suggestions. For security-related topics please email us at security@altinity.com. For general topic, please email info@altinity.com.