Vulnerability Disclosure Policy

Overview

Agronomix is committed to ensuring the security of our customers by protecting their information from unwarranted disclosure. This policy is intended to give security researchers clear guidelines for conducting vulnerability discovery activities and convey our preferences as to how to submit vulnerabilities discovered.

This policy describes what systems and types of research are covered, how to send vulnerability reports, and how long security researchers should wait before publicly disclosing vulnerabilities.

We want security researchers to feel comfortable reporting vulnerabilities, so they can be fixed. This policy has been developed to reflect our values and uphold our sense of responsibility to security researchers who share their expertise with us in good faith.

Authorization

If you make a good faith effort to comply with this policy during your security research, we will consider your research to be authorized. We will work with you to understand and resolve the issue quickly, and Agronomix Software will not recommend or pursue legal action related to your research. However, we do not offer monetary rewards for vulnerability disclosures.

Guidelines

Under this policy, “research” means activities in which you:

- Notify us as soon as possible after you discover a real or potential security issue.
- Make every effort to avoid privacy violations, degradation of user experience, disruption to production systems, and destruction or manipulation of data.
- Only use exploits to the extent necessary to confirm a vulnerability’s presence. Do not use an exploit to compromise or exfiltrate data, establish command line access and/or persistence, or use the exploit to “pivot” to other systems.
- Provide us with a reasonable amount of time to resolve the issue before you disclose it publicly.
- Do not intentionally compromise the privacy or safety of Agronomix Software personnel, Agronomix Software customers, or any third parties.
- Do not intentionally compromise the intellectual property or other commercial or financial interests of any Agronomix Software personnel or entities, Agronomix Software customers, or any third parties.

Once you have established that a vulnerability exists or encounter any sensitive data (including personally identifiable information, financial information, or proprietary information or trade secrets of any party), you must stop your test, notify us immediately, and not disclose this data to anyone else.

Scope

All systems and services associated with the domains listed are in scope, including any subdomains and any website with a link to this policy.

Vulnerabilities found in non-Cultura systems are out of scope and should be reported directly to the vendor in accordance with its own Vulnerability Disclosure Program (VDP) Policy (if any).

Though we develop and maintain other internet-accessible systems or services, we ask that active research and testing only be conducted on the systems and services covered by the scope of this document. If there is a system, which is out of scope that you think merits testing, please contact us to discuss it first.

Product	**Domain**
Website	Agronomix.com
Website	Genovix.io

Rules of Engagement

Security Researchers Must Not:

- Test any system other than the systems set forth in the 'Scope' section above.
- Disclose vulnerability information except as set forth in the 'Reporting a Vulnerability' and 'Disclosure' sections below.
- Engage in physical testing of facilities or resources.
- Engage in social engineering.
- Send unsolicited electronic mail to Agronomix Software personnel or customers, including "phishing" messages.
- Execute or attempt to execute "Denial of Service" or "Resource Exhaustion" attacks.
- Introducing malicious software.
- Test in a way that could degrade the operation of Agronomix Software systems or intentionally impair, disrupt, or disable them.
- Test third-party applications, websites, or services that integrate with or link to or from Agronomix Software systems.
- Delete, alter, share, retain, or destroy Agronomix Software data, or render Agronomix Software data inaccessible.
- Or use an exploit to exfiltrate data, establish command line access, establish a persistent presence on Agronomix Software systems, or "pivot" to other Agronomix Software systems.

Security Researchers Must:

- Cease testing and notify us immediately upon discovery of a vulnerability.
- Cease testing and let us know at once upon discovery of exposure of non-public data.

- Purge any stored Agronomix Software non-public data upon reporting a vulnerability.

Security Researchers may:

- View or store Agronomix non-public data only to the extent necessary to document the presence of a potential vulnerability.

Reporting a Vulnerability

We accept vulnerability reports at systems@agronomix.com

Information submitted under this policy will be used for defensive purposes only i.e., to mitigate or remediate vulnerabilities. If your findings include newly discovered vulnerabilities that affect all users of a product or service and not solely Agronomix Software, we may share your report with the Cybersecurity and Infrastructure Security Agency (CISA), where it will be handled under their coordinated vulnerability disclosure process. We will not share your name or contact information without express permission.

By submitting a vulnerability, you are indicating that you have read, understood, and agree to the guidelines described in this policy for the conduct of security research and disclosure of vulnerabilities or indicators of vulnerabilities related to Agronomix Software information systems, and consent to having the contents of the communication and follow-up communications stored on an Agronomix Software system.

To help us triage and prioritize submissions, we recommend that your reports:

- Adhere to all legal terms and conditions
- Describe the vulnerability, where it was discovered, and the potential impact of exploitation
- Offer a detailed description of the steps needed to reproduce the vulnerability (proof of concept scripts or screenshots are helpful).

Disclosure

Agronomix Software is committed to timely correction of vulnerabilities. However, we recognize that public disclosure of a vulnerability in absence of a readily available corrective action increases versus decreases risk. Accordingly, we require that you refrain from sharing information about discovered vulnerabilities for 120 calendar days after you have received our acknowledgement of receipt of your report. If you believe others should be informed of the vulnerability prior to our implementation of corrective actions, we require that you coordinate in advance with us.

We may share vulnerability reports with the Cybersecurity and Infrastructure Security Agency (CISA), as well as any affected vendors. We will not share names or contact details of security researchers unless given explicit permission.

Verification and Remediation

The Agronomix Software General Manager (or delegate) will be responsible for keeping an audit trail of public reports, verifications, and remediations. Verification and remediation will be assigned to the appropriate team members according to the source of the vulnerability.

Verification and Remediation Procedures

1. Upon receipt of an email the Agronomix Software General Manager is responsible for calling a Management Team meeting and deciding who should respond and the level of response.
    a. Level of response includes verifying the threat and communicating with the source.
2. The Agronomix Software General Manager (or delegate) will also be responsible for determining the severity of the threat e.g., the vulnerability may constitute a security incident and require involvement from other staff within the wider Volaris organisation.

Review and Revision

This policy will be reviewed on a regular basis, but no less frequently than every 12 months. The policy review will be undertaken by the Agronomix Software Data Security Team.