Vulnerability Disclosure Policy

Agronomix Software Vulnerability Disclosure Policy
This Vulnerability Disclosure Policy applies to any vulnerabilities you are considering reporting to Agronomix Software. We recommend reading this policy fully before you report a vulnerability.

This policy describes the finding, testing, and reporting of vulnerabilities discovered on agronomix.com or Genovix.io websites owned by Agronomix software inc.
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 collaborate with you to understand and resolve the issue and Agronomix Software will not recommend or pursue legal action related to your research. However, we do not offer monetary rewards for vulnerability disclosures.

Scope

All systems and services associated with the domains listed below are in scope. Likewise, subdomains of each listing, unless explicitly excluded, are always in scope. Additionally, any website published with a link to this policy shall be considered in scope. Vulnerabilities found in non-agronomix.com or Genovix.io from our vendors fall outside the scope of this policy and should be reported directly to the vendor according to their disclosure policy (if any).

Though we develop and maintain other internet-accessible systems or services, we ask that active research only be conducted on the systems and services covered by the scope of this document. If there is a system not in scope that you think merits inclusion, please contact us to discuss it first. We will increase the scope of this policy over time as required.

DOMAIN:

Agronomix.com
Genovix.io

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. Should legal action be initiated by a third party against you for activities conducted in accordance with this policy, we will make this authorization known.

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.
- You do not intentionally compromise the privacy or safety of Agronomix Software personnel, Agronomix Software customers, or any third parties.
- You 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. However, we do not offer monetary rewards for vulnerability disclosures

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.
- View or store Agronomix Software non-public data.

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.

Reporting a Vulnerability

We accept vulnerability reports at systems@agronomix.com Information sent under this policy will be used for defensive purposes only – 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, 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, understand, 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 a 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 likely 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.

Verification and Remediation

The Data Security Manager will be responsible for keeping an on-going list of public reports, verifications, and remediations. Verification and remediation will be assigned to the appropriate IT Team members according to the source of the vulnerability (i.e., if from website will be assigned to sales and marketing).

Verification and Remediation Procedures

1. Upon receipt of an email the Agronomix Software Data Security 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 data security manager will also be responsible for determining the severity of the threat and may raise a security incident with Agronomix Software IT, involving legal and/ or the Volaris Data Security Team.