CIVICPLUS RESPONSIBLE DISCLOSURE POLICY

1. PURPOSE

CivicPlus is committed to the security of its products and the communities they serve. We value the work of independent security researchers who help identify vulnerabilities in our systems. This Responsible Disclosure Policy provides a structured channel for reporting security vulnerabilities to CivicPlus and describes how we will work with researchers who report in good faith.
Please note this is not a bug bounty program. CivicPlus **does not** offer or pay monetary rewards for vulnerability reports.

2. HOW TO SUBMIT A REPORT

To report a security vulnerability, complete the Information Security reporting form. Please include the following information:

a) A description of the vulnerability, including the affected product, application, or URL.
b) Detailed steps to reproduce the issue.
c) The potential impact of the vulnerability, as you understand it.
d) Any supporting evidence (screenshots, logs, or proof-of-concept code), limited to what is necessary to demonstrate the issue.

Please do not include sensitive data (such as personal information of third parties) in your report.

Please provide a valid email address in the form so that CivicPlus can contact you. CivicPlus will respond to your submission by email, and you may reply to that email to provide additional information or continue communication about your report.

3. AUTHORIZED SCOPE

In Scope:

- CivicPlus-owned and operated web applications and domains
- CivicPlus APIs
- CivicPlus mobile applications

Out of Scope:

- Third-party services, applications, or websites, even if integrated with or linked from CivicPlus products
- Physical security
- Customer-owned or customer-managed environments (see Section 4 for additional guidance)

Corporate systems, employee accounts, and internal tools are not authorized for security testing. However, suspected vulnerabilities affecting those systems may still be reported to CivicPlus through the Information Security reporting form described in Section 2. The safe harbor described in Section 7 does not apply to active testing of corporate systems unless CivicPlus provides prior written authorization.

4. PROHIBITED CONDUCT AND TESTING RULES

To qualify for the protections described in this policy, researchers must comply with the following rules:

a) Act in good faith and conduct research in a manner designed to avoid harm to CivicPlus, its customers, and their end users.

b) Test only against in-scope assets identified in Section 3.
c) Do not exploit a vulnerability beyond what is minimally necessary to confirm its existence.
d) Do not access, copy, modify, or delete data belonging to CivicPlus customers or their end users.
e) Immediately stop testing and notify CivicPlus if you encounter personal data, government records, or other sensitive information during research.
f) Do not conduct testing that could degrade or disrupt CivicPlus services, including denial-of-service attacks, brute-force attacks, or resource exhaustion.
g) Do not engage in phishing, social engineering, or physical intrusion.
h) Use researcher-owned accounts and data for testing. Do not test against customer or third-party accounts.
i) Do not test a specific customer's site, tenant, account, data, configuration, or environment without that customer's express authorization. Researchers may report suspected platform-level vulnerabilities to CivicPlus using a researcher-controlled test environment where available.
j) Do not send unsolicited communications to other users as part of testing.
k) Do not upload malware or establish persistence.
l) Do not conduct automated scanning at a volume that may affect service availability.
m) Promptly delete any CivicPlus information inadvertently obtained during testing.
n) Comply with all applicable laws.

5. COORDINATED DISCLOSURE

Researchers must keep vulnerability information confidential and must not publicly disclose it without CivicPlus' prior written authorization.
CivicPlus will evaluate disclosure requests based on the nature of the vulnerability, the status of remediation, potential risk to customers and end users, and any applicable legal or contractual obligations. CivicPlus may authorize disclosure after the vulnerability has been remediated or otherwise sufficiently mitigated.
Researchers must provide CivicPlus reasonable advance notice of any proposed public disclosure and cooperate with CivicPlus regarding the timing and content of the disclosure.
Nothing in this section restricts disclosures required by applicable law, provided the researcher gives CivicPlus prior notice to the extent legally permitted.

6. WHAT RESEARCHERS MAY EXPECT

CivicPlus generally aims to acknowledge reports within five business days. Depending on the volume, complexity, and quality of submissions, acknowledgment or assessment may take longer. CivicPlus may not respond individually to reports that are incomplete, duplicative, out of scope, or do not present a material security risk.
If a vulnerability is confirmed and accepted, CivicPlus will work to remediate it in a timeframe appropriate to the severity and complexity of the issue. CivicPlus may provide updates when appropriate but does not commit to individualized or recurring status updates.
The following types of reports are generally considered nonqualifying unless they demonstrate meaningful, exploitable security impact:

- Missing security headers without an exploitable condition
- Clickjacking on pages without sensitive actions
- Open redirects without demonstrated security impact
- Username or email enumeration
- Rate-limiting observations without demonstrated abuse
- Self-XSS
- Reflected text or content injection that cannot execute active content
- Automated scanner output without manual validation

- Outdated software claims based solely on version detection
- Denial-of-service testing
- Reports based only on unsupported or obsolete browsers
- Duplicate or previously known issues

7. SAFE HARBOR

CivicPlus will not initiate or support legal action against a researcher for security research that CivicPlus determines was conducted in good faith and in material compliance with this policy. This protection applies only to legal claims under CivicPlus' control and does not bind third parties. If a researcher's activity conducted in compliance with this policy is the subject of a legal inquiry by a third party, CivicPlus will take reasonable steps to make known that the activity was conducted in accordance with this policy.

CivicPlus expressly reserves all rights where a researcher:

a) Accessed or retained data beyond what is minimally necessary to demonstrate the vulnerability.
b) Disrupted services or degraded system availability.
c) Violated the privacy rights of CivicPlus customers or their end users.
d) Demanded payment or threatened disclosure.
e) Misrepresented compliance with this policy.
f) Otherwise acted unlawfully or outside the authorized scope described in this policy.

8. NO PAYMENT OR REWARD

CivicPlus does not offer monetary compensation, bounties, or other financial rewards for vulnerability reports. CivicPlus will not negotiate compensation in response to a report, a threatened disclosure, or a demand for payment.

Submission of a report does not entitle the researcher to payment, reimbursement, compensation, or any other reward. Any public acknowledgment of a researcher's contribution is voluntary, discretionary, and subject to the researcher's consent. CivicPlus controls the content, timing, and placement of any such recognition.

Submission of a report does not create any employment, agency, partnership, or contractual relationship between the researcher and CivicPlus.

9. REPORT HANDLING AND LEGAL TERMS

a) CivicPlus may share reports internally and with affected customers, vendors, insurers, advisers, law enforcement, or other parties as necessary. CivicPlus will determine, in its sole discretion and subject to applicable law and contractual obligations, whether a reported vulnerability constitutes a security incident and whether notice to any customer, regulator, law-enforcement authority, insurer, or other person is required. Researchers must not contact CivicPlus customers or end users regarding a report without CivicPlus' prior written authorization.
b) CivicPlus may retain reports and related communications.
c) CivicPlus may use submitted information to investigate, reproduce, mitigate, and remediate vulnerabilities.
d) CivicPlus may independently develop similar fixes or solutions without obligation to the submitter.
e) CivicPlus will evaluate whether a researcher qualifies for the protections described in this policy based on the researcher's conduct and material compliance with these terms.
f) No confidential relationship, implied contract, or obligation of any kind is created by the submission of a report, CivicPlus' review of a report, or CivicPlus' remediation of a reported vulnerability.

g) Submitting a vulnerability report does not grant the researcher any rights to CivicPlus intellectual property.
h) CivicPlus may, in its sole discretion, decline to act on a report, including reports involving known issues, duplicate reports, or issues that CivicPlus determines do not present a material security risk.
i) CivicPlus reserves the right to modify this policy at any time.
j) This policy does not create any contractual obligation or legal duty on the part of CivicPlus.
k) This policy does not waive, modify, supersede, or expand any provision of CivicPlus' Terms of Use, Master Services Agreement, Security Annex, Data Processing Addendum, applicable product terms, or any other agreement. CivicPlus will handle reported vulnerabilities and any resulting security incidents in accordance with its applicable contractual and legal obligations.

To report a security vulnerability, please complete the Information Security reporting form;
https://www.civicplus.com/security/department-security-more-information/