Galvanize, Inc. — Vulnerability Disclosure Program Guidelines

Updated October 17, 2025

1. Purpose

Galvanize, Inc. ("Galvanize") encourages responsible security research and coordinated vulnerability disclosure. These guidelines describe the rules of authorized testing, submission expectations, coordination procedures, and protections for researchers acting in good faith.

2. General Requirements

- Reporters ("you") must comply with all applicable laws and this policy when conducting security research.
- All testing must be performed in good faith and for the sole purpose of improving security.
- You must coordinate directly with Galvanize before public disclosure of any vulnerability.
- Nothing in this policy authorizes access to data or systems beyond what is expressly permitted.

3. Safe Harbor for Good-Faith Research

Galvanize will **not pursue legal action** or refer for prosecution any researcher who acts in **good faith** and **within these guidelines**.

- Activities outside these terms, or that cause harm, may be considered unauthorized access under applicable law.
- Good-faith means your actions are intended to improve security, avoid harm, respect privacy, and comply with this policy.

4. Scope of Authorized Testing

Authorized testing is limited to **publicly available Galvanize services** and **any systems explicitly designated by Galvanize as in scope**.

In Scope

- Public-facing websites and applications owned by Galvanize.
- APIs or endpoints documented for public or partner use.
- Systems or environments explicitly listed as authorized for testing.

Out of Scope

Out of scope testing examples include but are not limited to:

- Internal corporate networks or employee systems.
- Production customer environments or data.
- Third-party services not owned by Galvanize.
- Physical access (e.g., offices, data centers).
- Social engineering (phishing, vishing, impersonation).
- Denial-of-service or stress testing.

5. Testing Rules

- Use only **accounts you own** or those for which you have **explicit written consent** from the owner.
- Avoid any actions that could harm Galvanize systems, users, customers, or data.
- **Do not intentionally access, copy, download, exfiltrate, store, retain, or share any data**, including personal, customer, or proprietary information. If you inadvertently access such data, stop immediately, do not save or transfer it, and notify **support@galvanize.com**.
- **Do not exploit vulnerabilities beyond the minimum necessary** to confirm their existence.
- **Do not** escalate privileges.
- **Do not** modify, destroy, or corrupt data.
- **Do not** access communications or files unrelated to proving the vulnerability.
- **Do not use or disclose** discovered information to harm individuals, organizations, or systems, or to obtain personal, competitive, or financial gain.
- **Do not attempt** physical intrusion, social engineering, or denial-of-service attacks.
- If uncertain whether an action is allowed, stop and contact **support@galvanize.com** before proceeding.

6. Handling of Evidence and Data

- Collect only the minimal information required to demonstrate the vulnerability.
- Securely delete all testing data, logs, screenshots, and proof-of-concept materials after the vulnerability has been reported and acknowledged.
- Do not publish or share any sensitive information discovered during testing.

7. Reporting Procedures

- Submit reports to **support@galvanize.com** or through an approved secure channel.
- Each report must include:
    - A clear description of the vulnerability and its impact.
    - Steps to reproduce or validate the issue.
    - Any relevant environment details (URLs, payloads, parameters).
    - Optional safe proof-of-concept code or screenshots.
- Do not submit unanalyzed fuzzer output or crash dumps without explanation.
- If multiple systems or vendors are affected, coordinate responsibly with all parties, or through a recognized disclosure coordinator (e.g., CERT/CC).
- Galvanize will acknowledge receipt of valid reports within **5 business days** and will provide updates when remediation progress is available.

8. Coordination and Confidentiality

- Keep all vulnerability information confidential until Galvanize confirms remediation or grants written permission to disclose.
- Galvanize requests at least a **90-day coordination window** before any public disclosure, unless otherwise agreed.
- You may coordinate with other affected vendors or service providers but must protect confidentiality at all times.
- Reporters may request anonymity in any public acknowledgments.
- Galvanize will not enter NDAs, customer agreements, or compensation arrangements unless part of a formal bug-bounty program.

9. Public Disclosure

- After remediation, reporters may publicly disclose the existence and technical details of the vulnerability **only after consultation with Galvanize**.
- Disclosures must not reveal any proprietary, personal, or customer data, or other sensitive content.
- Public discussion must not endanger privacy, safety, or operational security.

10. Prohibited Conduct

Reporters must **not**:

- Attempt to extort, demand payment, or threaten disclosure.
- Use discovered vulnerabilities for competitive advantage or reputation attacks.
- Interfere with normal business operations or customer use of services.
- Submit fraudulent or automated mass reports.
- Submit reports intended to solicit security services.

11. Galvanize Commitments

- Acknowledge valid and compliant reports within **5 business days**.
- Engage in good-faith communication with the reporter.
- Strive to remediate verified vulnerabilities promptly.
- Credit reporters (if desired) after verification and resolution.

12. Contact

All questions, coordination requests, and submissions should be directed to:

support@galvanize.com