Hart InterCivic
Vulnerability Disclosure Policy

Introduction

Hart InterCivic welcomes feedback from security researchers working in good faith to help improve the security of our company. If you believe you have discovered a vulnerability in any of our digital assets covered by this policy, we want to hear from you. This policy outlines steps for disclosing vulnerabilities to us, what you can expect from us, and what we expect from you.

Scope

This policy applies to all corporate IT networks and public-facing web sites that are owned or operated by Hart InterCivic.

This policy does not apply to the networks or assets owned, leased, operated, or maintained by state and local government election officials. Researchers should follow guidance from those entities for security research opportunities and conditions. Special security research project requests involving developmental or preproduction devices on which a voter's ballot may be generated or tabulated will be addressed on an individual and as-needed basis. Contact Hart at security@hartic.com to inquire.

The following actions are not covered by this policy:

- Denial of Service (DoS) attacks, including distributed DoS (DDos) and degraded service
- Physical security attacks
- Social engineering attacks

Guidelines

In participating in our vulnerability disclosure program, we request that you:

- Act in good faith. This includes following this policy, as well as any other relevant agreements that may apply. If there is any inconsistency between this policy and any other relevant terms, the terms of this policy will prevail.
- Report any vulnerability you believe you have discovered promptly.
- Avoid violating the privacy of others, disrupting our systems, destroying data, and/or harming user experience.
- Perform testing only on in-scope systems listed above.
- If a vulnerability provides unintended access to data, do not access data beyond the minimum extent necessary to effectively demonstrate the presence of a vulnerability. If you encounter any Personally Identifiable Information (PII), financial or credit card data, or proprietary information while testing, we ask that you cease testing and submit a report immediately.
- Third-party vulnerabilities: If issues reported affect a third-party library, external project, or another vendor, Hart reserves the right to forward details of the issue to that party without further discussion with the researcher. We will do our best to coordinate and communicate with researchers throughout this process.

Reporting

In order to submit a vulnerability report, please email security@hartic.com with all relevant information. The more details you provide, the easier it will be for us to triage and fix the issue.

- Use only the security@hartic.com email address to discuss vulnerability information with us.
- We ask that you keep the details of any discovered vulnerabilities confidential until either they are fixed or at least 120 days have passed.
- If you are able and prefer to encrypt your report prior to submission, please contact us at security@hartic.com for further instructions.

Our Commitment

When working with us according to this policy, you can expect us to:

- Acknowledge receipt of reports promptly.
- Strive to keep you informed about the progress of a vulnerability as it is processed.
- Work to analyze and remediate discovered vulnerabilities in a timely manner.
- Extend Safe Harbor for your vulnerability research that is related to this policy.

Safe Harbor

When conducting vulnerability research according to this policy, we consider this research to be:

- Authorized in accordance with the Computer Fraud and Abuse Act (CFAA) (and/or similar state laws), and we will not initiate or support legal action against you for accidental, good faith violations of this policy;
- Exempt from the Digital Millennium Copyright Act (DMCA), and we will not bring a claim against you for circumvention of technology controls;
- Exempt from restrictions in our Terms & Conditions that would interfere with conducting security research, and we waive those restrictions on a limited basis for work done under this policy; and
- Lawful, helpful to the overall security of Hart InterCivic and the broader elections industry in the United States, and conducted in good faith.

All individuals who engage with any Hart asset(s) are expected to comply with all applicable state and federal laws.

If at any time you have concerns or are uncertain whether your security research is consistent with this policy, please contact us at security@hartic.com before going any further.