Vulnerability Disclosure Policy
Union County Board of Elections
February 5, 2025

Introduction

Union County Board of Elections is committed to ensuring the security of the public by protecting their information. This Policy is intended to give security researchers clear guidelines for conducting vulnerability discovery activities and to convey our preferences in how to submit discovered vulnerabilities to us.

This Policy describes **what systems and types of research** are covered under this Policy, **how to send us** vulnerability reports, and **how long** we ask security researchers to wait before publicly disclosing vulnerabilities.

We encourage you to contact us to report potential vulnerabilities in our systems.

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 *Union County Board of Elections* will not recommend or pursue legal action related to your research. Should legal action be initiated by a third party against you for activities that were 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 persistent command line access, or use the exploit to pivot to other systems.
- Provide us a reasonable amount of time to resolve the issue before you disclose it publicly.
- Do not submit a high volume of low-quality reports.

Once you've 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**.

Test methods

The following test methods are not authorized:

- Network denial of service (DoS or DDoS) tests or other tests that impair access to or damage a system or data
- Physical testing (e.g. office access, open doors, tailgating), social engineering (e.g. phishing, vishing), or any other non-technical vulnerability testing

Scope

This policy applies to the following systems and services:

- `https://www.unioncountyohio.gov/board-of-elections`
- `https://lookup.boe.ohio.gov/vtrapp/union/`

Any service not expressly listed above, such as any connected services, are excluded from scope and are not authorized for testing. Additionally, vulnerabilities found in systems from our vendors fall outside of this Policy's scope and should be reported directly to the vendor according to their disclosure Policy (if any). If you aren't sure whether a system is in scope or not, contact our reporting partner, the Election Infrastructure Information Sharing and Analysis Center (EI-ISAC) at Elections-VDP@cisecurity.org **before starting your research**.

Though we develop and maintain other internet-accessible systems or services, *active research and testing* must only be conducted on the systems and services covered by the scope of this document. If there is a particular system not in scope that you think merits testing, first contact us to discuss it. We aim to increase the scope of this Policy over time.

Reporting a vulnerability

Information submitted 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 **Union County Board of Election***, we may share your report with the EI-ISAC, which in turn may share it 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 from you.*

We accept vulnerability reports via email at Elections-VDP@cisecurity.org. Reports may be submitted pseudonymously, with the sender's email as the only required identifying information.

You **may not** submit sensitive information via email. If you need to send us sensitive information, indicate this in your report and the EI-ISAC will provide a secure fileshare link. To ease reviewing and responding to your submission, use the submission standard.

By submitting a vulnerability, you acknowledge that you have no expectation of payment and that you expressly waive any future pay claims against the Union County Board of Election related to your submission.

What we would like to see from you

In order to help us triage and prioritize submissions, we recommend that your reports:

- Describe the location the vulnerability was discovered and the potential impact of exploitation including URL/software/service(s) affected, and version.
- Offer a detailed description of the steps needed to reproduce the vulnerability (proof of concept scripts, illustrations, and screenshots are helpful).
- Describe potential attack scenarios and consequences.
- Provide any recommended mediation actions.
- Be in English.

What you can expect from us

When you choose to share your contact information with us, we commit to coordinating with you as openly and as quickly as possible.

- Within one business day, the EI-ISAC will acknowledge that your report has been received.
- The EI-ISAC will contact you if it requires additional information and, if necessary, provide you with a secure file share link for providing additional information.
- Within five business days of having all necessary information, the EI-ISAC will validate the existence of the vulnerability and share it with *[Organization name]*. If the EI-ISAC is unable to confirm the vulnerability, it will work with you to understand why.
- Within 120 days, the EI-ISAC will provide an update on the status of remediation. Additionally, the EI-ISAC or ***Union County Board of Elections*** may contact you regarding issues or challenges regarding remediation.
- We will maintain an open dialogue to discuss issues.

Questions

Questions regarding this policy may be sent to [**agency email**]. We also invite you to contact us with suggestions for improving this policy. **DO NOT send vulnerability reports to this email address.**

Document change history

Version	Date	Description
1.0	*February 5, 2025*	First issuance