VULNERABILITY DISCLOSURE POLICY

As Tuscarawas Board of Elections is doing its part to deliver a thriving democracy and a prosperous economy for all residents of Tuscarawas County. The Tuscarawas Board of Elections is working to ensure that Tuscarawas County Elections are both secure and accessible.

As the hard work continues in support of these critical functions across Tuscarawas County, the threats to our nation's infrastructure, including our elections infrastructure, have never been greater. Because of this, the Tuscarawas Board of Elections has announced this new program. The Tuscarawas Board of Elections takes the security of our systems seriously. We value the security research community and believe by working together we can help ensure the security and privacy of our users, our systems, and our data.

This policy describes what systems and types of research are covered under this policy, how to report vulnerabilities to us, what we ask of researchers, and what researchers can expect from us. For those researchers willing to provide their expertise and committing public service hours to defending our democracy, we thank you and look forward to working with you!

GUIDELINES

We require that you:

- Make every effort to avoid privacy violations, degradation of user experience, disruption to production systems, and destruction or manipulation of data during security testing;
- Only test to the extent necessary to confirm a vulnerability in systems identified within the scope section below. Do not compromise or exfiltrate data, establish command line access and/or persistence, or "pivot" to other systems. Once you've established that a vulnerability exists, or encounter any of the sensitive data outlined below, you must stop your test and notify us immediately;
- Use the identified communication channels to report vulnerability information to us; and,
- Keep confidential any information about discovered vulnerabilities for at least 120 calendar days after you have notified Tuscarawas Board of Elections. For details, please review Coordinated Disclosure below.

SCOPE

This policy applies to the following systems:

- boe.ohio.gov/tuscarawas/
- tuscarawas.boe.ohio.gov
- tuscboe.net

The Tuscarawas County, co.tuscarawas.oh.us and state.oh.us are not within the scope of this policy.

Any services not expressly listed above, including 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. Systems not covered under this policy include but are not limited to: voting machines, electronic pollbooks, remote ballot markers, county voter registration systems. If you aren't sure whether a website, system, or endpoint is in scope or not, contact us at Tuscaraw@ohiosos.gov before starting your research.

The following test types are not allowed:

- Denial of service (DoS or DDoS) tests.
- Defacement
- Physical testing (e.g. office access, open doors, tailgating).
- Social engineering (e.g. phishing, vishing).
- Intentionally or potentially disruptive test types, including but not limited to DNS spoofing or DNS tunneling.
- Functionality bugs, clickjacking, email spoofing, etc. are considered out of scope. Our intent is to work with researchers to identify software and system vulnerabilities, not to identify low impact issues. Testers may report such issues, but they may not be handled as an issue subject to this vulnerability disclosure process.

SENSITIVE INFORMATION

If you encounter any of the below on our systems while testing within the scope of this policy, stop your test and notify us immediately:

- Personally identifiable information (Social Security numbers, driver’s license numbers)
- Financial information (e.g., credit card or bank account numbers)

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, will work with you to understand and resolve the issue quickly, and Tuscarawas Board of Elections will not initiate or recommend legal action related to your research.

When conducting vulnerability research according to the guidelines and scope of 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 any software 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

You are expected, as always, to comply with all applicable laws.

If at any time you have concerns or are uncertain whether your security research is consistent with this policy, please contact us through one of the channels in the "Reporting a vulnerability" section before going any further.

REPORTING A VULNERABILITY

Submit a vulnerability report by email at Tuscaraw@ohiosos.gov

Reports should include:

- Description of the location and potential impact of the vulnerability.
- A detailed description of the steps required to reproduce the vulnerability. Proof of concept (POC) scripts, screenshots, and screen captures are recommended. Please use extreme care to properly label and protect any exploit code.
- Any technical information and related materials needed to reproduce the issue.

Vulnerabilities in Tuscarawas Board of Elections system may be relevant to other state and local governments who use similar technology. We may share your vulnerability reports with U.S. federal, state, and local government agencies and the information sharing organizations that work closely with them. This sharing may include the U.S. Department of Homeland Security, the Cybersecurity & Infrastructure Security Agency (CISA), the Federal Bureau of Investigations (FBI), the Multi-State Information Sharing & Analysis Center (MS-ISAC), the Elections Infrastructure Information Sharing & Analysis Center (EI-ISAC), Ohio National Guard, Ohio Department of Administrative

Services (DAS), and the State of Ohio Chief Information Officer, and State of Ohio Chief Information Security Officer (CISO), as well as any affected vendors or open source projects.

ACKNOWLEDGEMENT OF REPORTS

We will acknowledge your report within seven business days of receiving it. We will work with you to understand the report and validate the vulnerability you are reporting. We aim to provide you with periodic updates while working with you.

When a vulnerability has been resolved, we will notify you. We will offer you the opportunity to test and verify that the remediation has been successful. The “Coordinated Disclosure” section below specifies our commitment to publishing vulnerabilities after reporting. We are not offering financial compensation or “bug bounties” as part of our program.

COORDINATED DISCLOSURE

The Tuscarawas Board of Elections is committed to resolving vulnerabilities in 120 days or less, and may disclose the details of those vulnerabilities when they have been resolved. We believe that public disclosure of vulnerabilities is an essential part of the vulnerability disclosure process, and that one of the best ways to make software better is to enable everyone to learn from each other's mistakes.

At the same time, we believe that disclosure in absence of a readily available remediation tends to increase risk rather than reduce it, accordingly you may not share your report with others during the 120-day window while we work to resolve the vulnerability. If you believe there are others that should be informed of your report before it has been resolved, please let us know.

We support coordinated disclosure that advances the security of our systems. Once a known vulnerability is remediated or the 120 days has passed we may coordinate a public advisory with you. Before you release any information related to the vulnerability please contact us to ensure you are not releasing sensitive information. Thanks for supporting this innovative and important program to help secure Tuscarawas Board of Elections systems.

1. Under Ohio’s public records law we may be required to release records related to your research and disclosure. If you wish to remain anonymous you may use a pseudonym and contact SOS with a "throw-away" email account.