Vulnerability Disclosure Policy

INTRODUCTION

ES&S welcomes feedback from security researchers to help improve its security. 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 digital assets owned and operated by ES&S, including corporate IT networks and public facing websites. This policy does not give authorization to test state and local government election related networks or assets and researchers should follow guidance from those entities for security research opportunities and conditions. For ES&S products not owned or operated by ES&S, we will accept reports as a result of research under this policy.

*Note: ES&S may offer special security research projects involving developmental or preproduction ballot marking devices, tabulators, electronic pollbooks, voter registration technology or other ES&S products. Interested researchers may contact ES&S at security@essvote.com to learn more.

GUIDELINES

In participating in our VDP, we require that you:

- Play by the rules. This includes following this policy, as well as any other relevant agreements. If there is any inconsistency between this policy and any other relevant terms, the terms of this policy will prevail.
- Promptly report any vulnerability you've discovered to ES&S.
- Do not violate the privacy of others, disrupt our systems, destroy any data, and/or harm user experience.
- Use only the Official Channels (listed below) to discuss vulnerability information with us.
- Keep the details of any discovered vulnerabilities confidential until either they are fixed or at least 90 days have passed.
- Perform testing only on the in-scope systems listed above.
- To the maximum extent possible, only interact with test accounts you own or accounts with explicit permission from the account owner.
- 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), Personal Healthcare Information (PHI), credit card data, or proprietary information while testing, we ask that you cease testing and submit a report immediately.

REPORTING

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

OUR COMMITMENT

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

- Acknowledge reports within 3 business days
- Work in good faith with you to understand the details around the discovery of the vulnerability
- Strive to keep you informed about the progress of remediating a vulnerability as it is processed
- Work to 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 the Internet, and conducted in good faith.

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 at security@essvote.com before going any further.