

# COORDINATED VULNERABILITY DISCLOSURE POLICY



## INTRODUCTION

If you believe you have discovered a vulnerability in any of our digital assets covered by this policy, i3logix would like to hear from you. This policy demonstrates the process for disclosing vulnerabilities to us. This policy applies to all digital assets owned and operated by i3logix, 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.

## GUIDELINES

### **i3logix requires that you:**

- Please abide by the rules.
- Report any vulnerability you've discovered to i3logix or BallotTrax.
- Do not violate the privacy of users, disrupt the i3logix systems, destroy/delete any data, and/or violate user experience.
- Use only the Official Channel (listed below) to communicate vulnerability information with us.
- We ask that you keep vulnerabilities discovered for at least 90 days or unless instructed otherwise.
- Testers are only allowed to interact with test accounts that you own or accounts with explicit permission from the account owner. Please provide account holder's permission to i3logix prior to testing.
- If a vulnerability provides unintended data access STOP and report vulnerability immediately. If you encounter any Personally Identifiable Information (PII), or proprietary information while testing, we ask that you stop testing and submit a report immediately. To submit a vulnerability report, please email [vulnerability@i3logix.com](mailto:vulnerability@i3logix.com) with all relevant information. The more details you provide, the easier it will be for us to research and resolve the vulnerability.

## VULNERABILITY DISCLOSURE POLICY

---

---

## OUR COMMITMENT

### **Our commitment in working with you:**

- You will receive an acknowledgement within 3 business days.
- Keep you updated about the progress of remediating the vulnerability.
- You will be exempt from the Digital Millennium Copyright Act (DMCA), and we will not bring a claim against you for vulnerability research of security 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
- You are expected to comply with all federal/state 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 [vulnerability@i3logix.com](mailto:vulnerability@i3logix.com) before going any further.