

Responsible Vulnerability Disclosure Policy

At Old Republic Title, we are committed to maintaining the security and privacy of our users, systems, data, and services. We recognize the valuable role that independent security researchers (researchers) and the broader cybersecurity community play in identifying vulnerabilities. This Vulnerability Disclosure Policy (VDP) outlines how to responsibly report potential security issues to us.

1. Scope

This policy applies to:

- All publicly accessible Old Republic Title websites and digital services.
- Internet-facing systems owned or operated by Old Republic Title or its subsidiaries.

2. Reporting a Vulnerability

If you believe you have discovered a security vulnerability in an Old Republic Title system, please report it by emailing: applicationsecurity@oldrepublictitle.com

You must be 18 years old or older to submit a vulnerability for consideration.

Include the following in your report:

- A detailed description of the vulnerability.
- Steps to reproduce the issue.
- Potential impact/security implications.
- Any relevant screenshots, logs, or proof-of-concept code.
- Your contact information (optional, but helpful for follow-up).

Please do not transmit any sensitive information via e-mail. If you need to send information, please contact us by e-mail first to receive instructions on secure transmission.

3. Our Commitment to Researchers

If you responsibly disclose a vulnerability in accordance with this policy, Old Republic Title commits to:

- Acknowledging your report: We will acknowledge your submission within five (5) business days.
- Providing a timely response: We will investigate and may provide a status update on the vulnerability, including any expected resolution timeline, if possible.
- Honoring responsible disclosure: We will not pursue legal action against researchers who adhere to this policy.

4. Guidelines for Researchers

To protect users and systems, Old Republic Title asks for the following:

- Do not access, modify, or delete data that does not belong to you.
- Do not disrupt services or degrade user experience.
- Do not use automated scanning tools that generate significant traffic.
- Do not publicly disclose the vulnerability before it has been resolved and coordinated with us.
- Do not introduce malicious or monitoring software.
- Do not access or extract confidential information.

5. Legal Safe Harbor

Old Republic Title will not pursue legal action against researchers who:

- Engage in good faith testing within the scope of this policy.
- Report vulnerabilities promptly.
- Avoid privacy violations, data destruction, or service disruption.
- Comply with all applicable laws.

This policy does not authorize access to data or systems beyond what is necessary to demonstrate the vulnerability. Old Republic Title reserves all legal rights in the event of any non-compliance.

6. Policy Updates

This policy may be updated periodically. The latest version will always be available at: <https://cdn.oldrepublictitle.com/files/VulnerabilityDisclosurePolicy.pdf>