OBRIST INTERIOR AG VULNERABILITY DISCLOSURE POLICY (VDP)

1. Introduction

At Obrist Interior AG, we take the security of our systems and data very seriously. We are committed to maintaining the highest level of security for our customers and partners. We understand the importance of working collaboratively with the security community to identify and address potential vulnerabilities in our systems. This Vulnerability Disclosure Policy (VDP) outlines the guidelines and procedures for responsibly reporting security vulnerabilities to Obrist Interior AG.

2. Scope

This policy applies to all Obrist Interior AG's online services, web applications, mobile applications, and related systems.

3. Responsible Disclosure

Obrist Interior encourages responsible disclosure of any security vulnerabilities found in our systems. If you discover a potential security issue, we request that you follow the guidelines below:

- Do not exploit the vulnerability or attempt to access, modify, or delete any sensitive data.
- Do not publicly disclose the vulnerability before it has been resolved.
- Promptly and privately report the vulnerability to us via the designated contact email: security@obrist-interior.ch.

4. How to Report a Vulnerability

When reporting a vulnerability, please provide us with the following information:

- A detailed description of the vulnerability, including the affected system and potential impact.
- The steps to reproduce the vulnerability, if applicable.
- Screenshots, proof-of-concept code, or any other supporting material that can help us understand and validate the issue.
- Your contact information, including your name and email address.

5. Response Time

Upon receiving your vulnerability report, we will acknowledge receipt of your report within two business days. Our security team will review the issue and respond to you as soon as possible,

usually within ten business days. If the report is well-founded and requires more time to address, we will keep you informed of the progress and expected resolution timeframe.

6. Coordination and Collaboration

Obrist Interior commits to work collaboratively and in good faith with the reporting party to address and resolve the reported vulnerability. We may need to seek additional information or clarification during the assessment and mitigation process.

7. Recognition and Reward

Obrist Interior appreciates the efforts of security researchers and individuals who responsibly disclose security vulnerabilities to us. As a token of our gratitude, we may offer recognition or rewards to individuals who report valid and original security vulnerabilities. The recognition and reward will be at the discretion of Obrist Interior AG and subject to compliance with this VDP.

8. Legal Considerations

Obrist Interior pledges not to pursue legal action against security researchers who make good faith efforts to comply with this VDP during their vulnerability disclosure process.

9. Exclusions

This VDP does not authorize any party to:

- Perform any denial-of-service (DoS) attacks or other disruptive actions.
- Access, download, or modify data on systems that do not belong to you.
- Conduct social engineering, phishing, or other attacks against Obrist Interior AG employees, users, or partners.

10. Changes to the Policy

Obrist Interior reserves the right to update or modify this VDP at any time without prior notice. The most recent version of this policy will be published on our website.

11. Contact

For any questions or to report a security vulnerability, please contact us via the designated email: security@obrist-interior.ch.

Thank you for helping us improve the security of Obrist Interior AG. Your cooperation and support are highly valued.