Responsible Vulnerability Disclosure Program

Summit Solutions Group, LLC

Revised: 1/23/2026

Introduction

Purpose

The purpose of this document is to outline the program implemented by Summit Solutions Group, LLC to establish a mechanism for non-employees to safely report vulnerabilities.

Scope

As Summit Solutions Group does not currently develop, maintain nor distribute software products, the program will not take effect until such products are developed and distributed. Once effective, this program shall apply to said software and this program may be revised in that event.

Section I – Authorized Activities

The following section describes the nature of activities used to detect a vulnerability.

1. Testing shall be performed through the intended interface of the software
2. All activities shall be non-intrusive and non-destructive
3. Modifications of source code is not allowed
4. Methods prohibited by law are not allowed
5. All activities that go beyond testing are not allowed
6. Payment may not be demanded for the vulnerability report nor used for extortion

Section II – Safe Harbor

If you comply with this program and report vulnerabilities responsibly, we will:

1. Not pursue legal action
2. Not contact law enforcement unless mal-intent it evident
3. Reserve the right to contact you to confirm and resolve the vulnerability

Section III - Reporting

To report a vulnerability, please email rvdp@summitssgllc.com with the following information:

1. A description of the vulnerability
2. Steps to reproduce the vulnerability

3. How the vulnerability may be exploited
4. A proof of concept demonstrating the issue
5. The name of the software the vulnerability was found within
6. Contact information, including name, email address. A phone number may also be included.

Section IV - Response

The following response times can be expected.

1. Acknowledgement – 7 days
2. Triage – 14 days
3. Resolution Development – will be determined based on the severity of the vulnerability
4. Updates – Every 12 days until resolved
5. Disclosure Coordination – to be mutually agreed upon prior to public announcement

Section V - Disclosure

Vulnerabilities will be disclosed in the following manner.

1. Public announcement may be made within 90 days of the vulnerability being reported
2. If we resolve a vulnerability prior to the normal 90-day window, we may request to shorten the window early
3. For critical vulnerabilities we may expedite the resolution and disclosure process
4. The vulnerability must be reported promptly (as defined in Section III) and must not be otherwise disclosed.