Responsible Vulnerability Disclosure Policy

1. Introduction and Objectives

We take the security of our products and services seriously and we welcome feedback from security researchers, experts and users in order to improve the security of our products and services.

This disclosure policy aims to provide a clear framework for responsibly reporting vulnerabilities and to ensure their effective and secure remediation.

2. Coordinated Disclosure

We are committed to improving the security of our products and services and publish validated and relevant vulnerabilities through security advisories. To protect our customers and support coordinated vulnerability remediation, we ask that discovered vulnerabilities are kept confidential and not publicly disclosed until Gantner has assessed the issue and appropriate remediation measures have been implemented or communicated.

3. Reporting Channel

If you have identified any issue that potentially can affect the security of our products or services, please send an email to:

securityalert@gantner.com

4. Vulnerability Handling Procedure

We strive to acknowledge receipt of your vulnerability report within 7 business days and to complete the triage process within 14 business days. Throughout the process, we will keep you updated on our progress and the completion of any remediation efforts.

If additional information is needed, we may reach out to you for clarification. The remediation of reported vulnerabilities is prioritized based on factors such as impact, severity, and exploit complexity. Given these considerations, some reports may require additional time for triage or resolution. You are welcome to check in on the status; however, we kindly request that you do so no more than once every 14 days to allow our teams to focus on remediation activities.

5. Principles for Security Researchers

We require that all researchers take into account the respect for the law. Vulnerability scanning could not serve as a pretext for attacking a system or any other target. Several actions must be avoided. For example:

- Using social engineering
- Compromising the system and persistently maintaining access to it
- Changing the data accessed by exploiting the vulnerability
- Using malware
- Using the vulnerability in any way beyond proving its existence. To demonstrate that the vulnerability exists, the reporter could use non-intrusive methods. For example, listing a system directory
- Using brute force to gain access to systems

> Sharing vulnerability with third parties
> Performing DoS or DDoS attacks

6. Intigriti Bug Bounty and Vulnerability Dislosure Program

We also encourage ethical hackers to report vulnerabilities via our Intigriti Vulnerability Dislosure Program.

In addition, for some of our products, we're inviting ethical hackers to find vulnerabilities through our SALTO WECOSYSTEM Bug Bounty Program on Intigriti.

Get rewarded for making us stronger! Sign up here.