# Information Security Management System

## Everbridge Responsible Disclosure Policy

### Content/Purpose

This policy defines the Vulnerability Disclosure process with the intent of encouraged responsible vulnerability disclosure and making security researchers feel comfortable reporting vulnerabilities they've discovered so that Everbridge can fix them and keep Everbridge and its client's information secure.

### Document Information

| | |
|---|---|
| **Document Name:** | Everbridge Responsible Disclosure Policy |
| **Document Owner:** | Munya Kanaventi |
| **Executive Approvers:** | Elliot Mark, SVP and General Counsel |
| **Functional Approvers:** | Munya Kanaventi, Senior Director Information Security |
| **Compliance Scope:** | NIST SP800-53 R4<br>ISO 27001:2013 |
| **Classification:** | PUBLIC |
| **Audience:** | All Everbridge Employees, Contractors and General Public |
| **Version:** | 1.0 |
| **Date Last Reviewed:** | November 12, 2019 |
| **Effective as of:** | November 12, 2019 |

## Change History

| Version | Author | Date | Description |
|---|---|---|---|
| 0.1 | Jason Andress | May 2, 2019 | Initial Draft |
| 0.2 | David Muchineripi | May 9, 2019 | Incorporate Policy template and feedback from respective stake holders |
| 1.0 | Jason Andress | November 12, 2019 | Incorporate feedback from legal |

## Approval

This document requires the following approvals. Signed approval forms should be filed appropriately in the project filing system.

| Name | Title | Approval | Date |
|---|---|---|---|
| Elliot Mark | SVP and General Counsel | DocuSigned by: Elliot Mark E7406D2BAF23438... | December 10, 2019 |
| Munya Kanaventi | Senior Director, Information Security | DocuSigned by: Munya Kanaventi 752863F658B44A5... | November 13, 2019 |

**Contact information:**

**Everbridge**

Munya Kanaventi, Sr. Director Information Security

Email: Munya.kanaventi@everbridge.com
Phone: +1 952-484-7795

## Table of Contents

# 1 Introduction

Everbridge takes seriously its responsibility to protect the confidentiality, integrity and availability of all information produced by, on behalf of or entrusted to Everbridge.

This policy defines a responsible process in which vulnerabilities can be reported to Everbridge. The purpose of this policy is to ensure security researchers and vulnerability reporters have a responsible process to report and are comfortable with reporting vulnerabilities they've discovered so that Everbridge can address the reported vulnerabilities and keep Everbridge and Everbridge client information secure.

This policy describes what systems and types of research are covered, how to report vulnerabilities to Everbridge, and the length of time reporters need to wait before publicly disclosing vulnerabilities.

## 1.1 Scope

This policy applies to the following systems:

- everbridge.com and all subdomains of everbridge.com
- everbridge.net and all subdomains of everbridge.net
- everbridge.eu and all subdomains of everbridge.eu
- evbg.io and all subdomains of evbg.io
- eb-github.com and all subdomains of eb-github.com
- hipaachat.com and all subdomains of hipaachat.com
- nixle.com and all subdomains of nixle.com
- nixle.us and all subdomains of nixle.us
- planetrisk.com and all subdomains of planetrisk.com
- ums.no and all subdomains of ums.no
- nc4.com and all subdomains of nc4.com

**Any services not expressly listed above, such as any connected services, are excluded from scope** and are not authorized for testing. Additionally, vulnerabilities found in non-Everbridge systems from our vendors fall outside of this policy's scope and should be reported directly to the vendor according to their disclosure policy (if any). If you aren't sure whether a system or endpoint is in scope or not, contact us at responsibledisclosure@everbridge.com before starting your research.

# 2 Guidelines

Everbridge requires that you:

- Make every effort to avoid privacy violations, degradation of user experience, disruption to production systems, and destruction or manipulation of data.
- Only use exploits to the extent necessary to confirm a vulnerability. Do not use an exploit to compromise or exfiltrate data, establish command line access and/or persistence, or use the exploit to "pivot" to other systems. Once you've established that a vulnerability exists, or encountered any of the sensitive data outlined below, you must stop your test and notify us immediately.
- Keep confidential any information about discovered vulnerabilities for no less than 90 calendar days after you have notified us.

## 2.1 Authorization

If you make a good faith effort to comply with this policy during your security research, we will consider your research to be authorized, will work with you to understand and resolve the issue quickly, and Everbridge will not initiate or recommend legal action related to your research.

## 2.2 Prohibited Testing

The following test types are not authorized:

- User interface bugs or typos.
- Network denial of service (DoS or DDoS) tests.
- Physical testing (e.g. office access, open doors, tailgating), social engineering (e.g. phishing, vishing), or any other non-technical vulnerability testing.
- Testing in a manner that would result in sending bulk unsolicited or unauthorized email, notifications, or other duplicative or unsolicited messages.

If you encounter any of the below on Everbridge systems while testing within the scope of this policy, stop your test and notify Everbridge **immediately**:

- Personally, identifiable information (PII). PII is any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered PII.
- Financial information (e.g. credit card or bank account numbers)
- Proprietary information or trade secrets of companies of any party
- Any issues which would result in sending unauthorized emergency notifications

# 3 Reporting a Vulnerability

Everbridge accepts and discusses vulnerability reports via email at responsibledisclosure@everbridge.com. Reports may be submitted anonymously. **Note: We do not support PGP-encrypted emails.**

Reports should include:

- Description of the location and potential impact of the vulnerability.
- A detailed description of the steps required to reproduce the vulnerability, including screenshots and proof of concept (POC) scripts/code. Please use extreme care to properly label and protect any exploit code.
- Any technical information and related materials Everbridge would need to reproduce the issue.

Please be advised that results from automated scanning tools will not be accepted.

Please keep your vulnerability reports current by sending Everbridge any new information as it becomes available.

# 4 Everbridge Commitments

Everbridge will provide a timely response to your email (within five business days), will notify you when the vulnerability analysis has completed each stage of our review, and will provide an expected timeline for patches and fixes.

Everbridge is committed to patching confirmed vulnerabilities within 90 days or less.

Everbridge may share your vulnerability reports with any affected vendors or open source projects.

# 5 Coordinated Disclosure

Everbridge believes that disclosure in absence of a readily available patch increases risk rather than reduces it, and so asks that you refrain from sharing your report with others while we work on our patch. If you believe there are others that should be informed of your report before the patch is available, please let Everbridge know so we can discuss with you and agree upon an appropriate, coordinated course of action.

# 6 Bounties

You will qualify for a bounty if you were the first eligible person to alert Everbridge to a previously unknown in-scope issue and the issue triggers a code or configuration change. Bounties may be monetary (USD) and/or “swag”, at the discretion of Everbridge. Each submission’s bounty amount is based on the business impact, severity, and creativity of the issue.

If you are eligible for a monetary award you may need to:

- provide additional verification and tax information,
- fulfill eligibility requirements
- agree to additional terms and conditions with a third-party payment processor.

Taxes on bounties paid to you are your sole responsibility.