Vulnerability Disclosure Policy
V1.0

DOCUMENT CONTROL

Document Information

Document Title	Vulnerability Disclosure Policy
Version	1.0
Publication Date	06 February 2024
Status	Approved
Review Date	13 January 2027

Revision History

Version	Date	Author/Reviewer	Details
1.0	06 February 2024	Q.Sheikh	Initial Release
1.0	08 January 2025	Q.Sheikh	Initial Release
1.0	09 October 2025	J.Hudson	Minor edits
1.0	14 January 2026	Q Sheikh	Review

Classification

PROTECT - OFFICIAL

Legal Notice

This policy is designed to be compatible with common vulnerability disclosure good practice. It does not give you permission to act in any manner that is inconsistent with the law, or which might cause the Organisation or partner organisations to be in breach of any legal obligations.

Introduction

This vulnerability disclosure policy applies to any vulnerabilities you are considering reporting to us (the "Organisation").

We recommend reading this vulnerability disclosure policy fully before you report a vulnerability and always acting in compliance with it. We value those who take the time and effort to report security vulnerabilities according to this policy. However, we do not offer monetary rewards for vulnerability disclosures.

Reporting

If you believe you have found a security vulnerability, please submit your report to us using the following email: security@neighbourhoodalert.co.uk In your report please include details of:

- The website, IP or page where the vulnerability can be observed.
- A brief description of the type of vulnerability, for example, “XSS vulnerability”.
- Steps to reproduce. These should be a benign, non-destructive, proof of concept. This helps to ensure that the report can be triaged quickly and accurately. It also reduces the likelihood of duplicate reports, or malicious exploitation of some vulnerabilities, such as sub-domain takeovers.

What to expect

After you have submitted your report, we will respond to your report within five working days and aim to triage your report within ten working days. We’ll also aim to keep you informed of our progress. Priority for remediation is assessed by looking at the impact, severity and exploit complexity. Vulnerability reports might take some time to triage or address. You are welcome to enquire on the status but should avoid doing so more than once every 14 days. This allows our teams to focus on the remediation. We will notify you when the reported vulnerability is remediated, and you may be invited to confirm that the solution covers the vulnerability adequately. Once your vulnerability has been resolved, we welcome requests to disclose your report. We’d like to unify guidance to affected users, so please do continue to coordinate public release with us.

Guidance

You must NOT:

- Break any applicable law or regulations.
- Access data beyond what is necessary – especially sensitive information.
- Modify, delete or alter any data in the Organisation's systems or services.
- Use high-intensity invasive or destructive scanning tools to find vulnerabilities.
- Attempt or report any form of denial of service (DoS) vulnerabilities, including overwhelming systems with traffic or requests.
- Disrupt or degrade the Organisation's services or systems.

- Submit reports detailing non-exploitable vulnerabilities or general best-practice gaps (e.g., missing security headers).
- Submit reports detailing TLS configuration weaknesses (e.g., support for older cipher suites or TLS 1.0)
- Share vulnerability details outside of the approved reporting method (as described in our published security.txt).
- Engage in social engineering, phishing, or physical attacks against staff or infrastructure.
- Request or demand financial compensation in exchange for disclosing vulnerabilities.

You must:

- Always comply with data protection rules and must not violate the privacy of the Organisation's users, staff, contractors, services, or systems. You must not share, redistribute or fail to properly secure data retrieved from the systems or services.
- Securely delete all data retrieved as soon as it is no longer required or within one month of the vulnerability being resolved, whichever occurs first (or as otherwise required by data protection law).