Vulnerability Disclosure Policy

1 Purpose of this Policy

The purpose of this Vulnerability Disclosure Policy is to provide a clear and responsible framework for reporting, assessing, and resolving security vulnerabilities affecting our systems, services, and products.

It is intended to support early identification of potential security issues, reduce risk to users and infrastructure, and ensure that vulnerabilities are handled in a controlled and coordinated manner. It also aims to give assurance to individuals who report vulnerabilities that their concerns will be taken seriously and managed appropriately.

2 Our Approach to Security

We recognise that, despite appropriate safeguards, vulnerabilities may still arise. What tends to matter more in practice is how quickly and responsibly those issues are identified and addressed.

We welcome reports from security researchers, customers, and members of the public. Responsible disclosure plays an important role in maintaining the security and integrity of our services, and we are committed to engaging constructively with those who bring issues to our attention.

3 Scope of this Policy

This policy applies to vulnerabilities identified in systems and services that we own or operate, including:

- Public-facing websites and applications
- Customer portals and online services
- Network infrastructure and associated platforms

There may be situations where the applicability of this policy is not immediately clear. In such cases, reports are still encouraged, and we will assess them accordingly.

The following activities are not permitted under this policy:

- Testing that may disrupt services (e.g. denial-of-service activity)
- Social engineering or attempts to manipulate staff
- Access to or testing of third-party systems not under our control
- Any activity that would be unlawful or cause harm to users or systems

4 Reporting a Vulnerability

Vulnerabilities should be reported via:

Email: security@netbeam.com

Reports should, where possible, include:

- A description of the issue
- Steps required to reproduce the vulnerability
- The potential impact
- Supporting evidence such as screenshots or logs

It is not necessary to provide extensive technical documentation; however, sufficient detail should be included to allow the issue to be understood and assessed.

Where a vulnerability may involve sensitive or personal data, this should be handled with care and not unnecessarily accessed, copied, or shared.

5 Our Response and Handling Process

All reports will be reviewed by our security team.

We aim to:

- Acknowledge receipt as a matter of urgency at the earliest possible opportunity
- Provide an initial assessment within ten working days
- Investigate and validate reported vulnerabilities
- Prioritise remediation based on risk and potential impact

While we aim to remediate confirmed vulnerabilities within 90 days, it is recognised that certain issues—particularly those involving infrastructure or third-party dependencies—may require additional time. Where this is the case, remediation timelines will be determined on a risk-based basis.

We will communicate with the reporting party where appropriate, although there may be limitations on the level of detail that can be shared during ongoing investigations.

6 Coordinated Disclosure

We support coordinated vulnerability disclosure and recognise that, in some circumstances, public disclosure may be appropriate.

We ask that individuals do not publicly disclose details of a vulnerability until we have had a reasonable opportunity to investigate and remediate the issue. Where appropriate, we will work with the reporting party to agree a suitable disclosure timeline.

7 Good Faith and Safe Harbour

We will not take legal action against individuals who identify and report vulnerabilities in accordance with this policy, provided they:

- Act in good faith

- Do not exploit vulnerabilities beyond what is necessary to demonstrate their existence
- Avoid actions that would compromise data, privacy, or service availability
- Provide reasonable time for remediation before disclosure

Activities that fall outside these principles may not be considered authorised.

8 Data Protection Considerations

Where a vulnerability involves personal data, individuals should cease testing and report the issue promptly.

We will assess any potential personal data breach in accordance with applicable data protection legislation and, where required, notify the Information Commissioner's Office.

9 Recognition

We recognise the value of responsible disclosure and may, at our discretion, acknowledge individuals who report valid vulnerabilities. Where applicable, recognition or rewards may be offered based on the nature and impact of the issue.

10 Policy Review

This policy is reviewed periodically to ensure it remains effective and aligned with current security practices and regulatory expectations. Feedback is welcomed and may inform future updates.

11 Service and Support Period

The service and support period for this product shall be 5 years from the date of its first placing on the market. Throughout this period, we will provide security vulnerability patches, firmware updates and relevant technical support.

12 Contact

For all vulnerability reports or queries:

security@netbeam.com