Vulnerability Disclosure Policy

IT & Security

Class 1 – General B2B Use / Public

Version 5.0 - 15/06/2026

Contents

Version Control

Current Version

Parameter	Value
Current Version	5.0
Release Date	15/06/2026
Author	Shannon Huxley, Head of Risk & Compliance

Version History

Version	Date	Author	Description of Changes
1.0	28/01/2020	GMT	New document created, reviewed, approved & released
2.0	13/01/2021	GMT	Document reviewed; minor amends made. No new content added.
3.0	07/12/2021	GMT	Document reviewed and rebranded to reflect the change from GCI to Nasstar. No new content added, minor grammar changes made.
4.0	04/01/2023	GMT	Document review completed, no changes made
5.0	15/06/2026	Shannon Huxley, Head of Risk & Compliance	New format, additional controls and updated address for reporting

1 Purpose & Objectives

The purpose of this Policy is to establish a clear, structured, and transparent approach for the identification, reporting, and management of security vulnerabilities affecting Nasstar systems and services.

The objectives of this Policy are to:

- Protect customer data and organisational assets
- Enable responsible reporting of vulnerabilities by internal and external parties
- Ensure vulnerabilities are assessed, managed, and remediated effectively
- Reduce the risk of exploitation and associated business impact
- Support compliance with legal, regulatory, and industry requirements
- Promote collaboration with the security research community

2 Scope

This Policy applies to:

- All entities within the Nasstar Limited

- All business units and operating divisions (UK and international)
- All Nasstar-owned systems, applications, infrastructure, and services

The Policy applies to:

- Employees and internal users
- External parties, including security researchers and the public

2.1 Compliance Obligations

This Policy supports Nasstar's obligations under applicable:

- Data protection and privacy laws (e.g. UK GDPR)
- Computer misuse and cybercrime legislation
- Contractual and customer security requirements
- Industry standards and frameworks (e.g. ISO 27001, ISO 29147, SOC 2)

3 Breach Management, Exceptions & Escalations

Any confirmed vulnerability that presents a material risk may be treated as a security incident and managed in accordance with Nasstar's Incident Management and Breach Response processes.

This includes:

- Investigation and impact assessment
- Containment and remediation
- Notification where required (e.g. regulatory or customer)

Exceptions

Any deviation from this Policy must be:

- Formally documented
- Risk assessed
- Approved by the appropriate authority (e.g. Information Security leadership)

Escalations

Escalation is required where:

- A vulnerability presents high or critical risk
- Active exploitation is suspected
- There is potential regulatory or customer impact

Escalations will follow Nasstar's defined governance and incident escalation processes.

4 Policy Statement

Nasstar recognises that protecting customer data is a critical responsibility and takes the security of its systems extremely seriously.

Nasstar:

- Actively monitors and tests its infrastructure and applications
- Acknowledges that it operates in a continuously evolving threat landscape
- Values the support of security researchers and the wider security community

Individuals identifying vulnerabilities are expected to:

- Report findings promptly via **compliance@nasstar.com** (anonymous reporting permitted)
- Provide sufficient detail (e.g. logs, screenshots, reproduction steps)
- Avoid exploiting vulnerabilities beyond proof-of-concept
- Refrain from public disclosure until remediation is confirmed

Nasstar commits to:

- Reviewing all legitimate reports in good faith
- Responding as soon as reasonably practicable
- Maintaining confidentiality of reporters, where requested
- Keeping reporters informed of progress where appropriate

5 Roles and Responsibilities

First Line – Doing the work	Second Line – Setting the rules and checking	Third Line – Independent assurance

Business Units and IT & Security
• Maintain secure systems and services
• Identify and report vulnerabilities
• Remediate vulnerabilities within agreed timelines
• Implement controls to reduce risk
	Risk, Compliance & IT & Security
	• Define and maintain this Policy and related standards
	• Monitor adherence and effectiveness
	• Assess and prioritise reported vulnerabilities
	• Provide oversight of remediation activities
	• Ensure alignment with regulatory and compliance requirements
		Internal Audit
		• Provide independent assurance on:
		  ○ Effectiveness of the vulnerability disclosure process
		  ○ Compliance with Policy and controls
		• Identify gaps and recommend improvements

6 Policy Governance

This policy is to be reviewed on a minimum of an annual basis or in line with business or regulatory landscape changes.

All stakeholders under the scope of this policy are obligated to promptly report any breaches by emailing Compliance@nasstar.com

Definition of non-adherence includes, but is not limited to:

- Failure to follow any stated rule, procedure, or protocol outlined within this policy.
- Deliberate circumvention of control measures, processes, or systems established to support this policy.
- Negligent actions or omissions that result in a breach or violation of the policy's intent or requirements.

Any confirmed instance of non-adherence to this policy, regardless of whether it results in immediate loss or harm to the Company, will be treated as a serious matter of misconduct and may result in the trigger of the Nasstar's formal Disciplinary Procedure.

7 Definitions & Acronyms

- **Responsible Disclosure** - process for reporting security vulnerabilities in a controlled and ethical manner.
- **Vulnerability** - A weakness in a system, application, or process that could be exploited.
- **Security Researcher (internal or external)** - Identifying potential vulnerabilities.
- **Proof-of-Concept (PoC)** - Limited demonstration of a vulnerability without exploitation.
- **Safe Harbour** - Assurance that individuals acting in good faith under this Policy will not face legal action.
- **Incident** - A confirmed event that compromises confidentiality, integrity, or availability.
- **Three Lines of Defence** - Risk model defining responsibilities across business (1st), oversight (2nd), and assurance (3rd).