NASSTAR

Responsible Disclosure Policy

Level 1

POL052

NASSTAR

Contents

1 Scope & Purpose

This Policy relates to the Nasstar group of companies (including Modality and Nasstar) and all operating Divisions in the UK and overseas, hereafter referred to as the "Group" or "we".

This policy covers all Nasstar owned systems and applications and has been created to provide a transparent approach to the management of disclosure of any vulnerabilities identified.

The Policy applies to both internal and external individuals or groups.

2 Policy Statement

Nasstar understands that protection of customer data is a significant responsibility and requires our highest priority. We therefore take the security of our systems extremely seriously, and we genuinely value the assistance of security researchers and others in the security community to assist in keeping our systems secure.

Nasstar constantly monitors and tests its infrastructure and applications to ensure that they remain secure, but appreciates that as an international organisation, we will always be a target for cyber criminals.

The responsible disclosure of security vulnerabilities helps us ensure the security and privacy of all our users.

If you find any indications of a vulnerability in any of our systems, we kindly ask you to inform us as soon as possible and not to disclose externally until you have done so. This is to ensure that we protect our users by preventing a malicious actor from taking advantage of the situation.

3 Disclosure

Please follow these steps to make a report:

- Report any indications for a potential security vulnerability to Nasstar by emailing infosec@nasstar.com. You can submit this information anonymously.
- Provide as much information as you can about your findings (including available indications, for example, IP addresses, logs, screenshots).
- Do not take advantage of the vulnerability or the problem you have discovered, (for instance, attempt to capture, change, or delete any more data than necessary to demonstrate the vulnerability).
- Do not disclose information about the vulnerability publicly until we have taken action to remediate it.

Once you report a vulnerability to us, we will respond as soon as reasonably practicable to evaluate the issue and determine next steps.

- We will handle your report with strict confidentiality and will not pass any of your details to any third party without your explicit permission.
- We will keep you informed of progress as we resolve the issue.

4 Guidance

Security researchers must not:

- Access unnecessary amounts of data. For example, 2 or 3 records is enough to demonstrate most vulnerabilities, such as an enumeration or direct object reference vulnerability
- Use high-intensity invasive or destructive technical security scanning tools to find vulnerabilities
- Violate the privacy of Nasstar users, employees, customers, members of the public, contractors, suppliers, services, or systems. For example, by sharing, redistributing and/or not properly securing data retrieved from our systems or services.
- Communicate any vulnerabilities or associated details using methods not described in this Policy, or with anyone other than their assigned Nasstar security contact
- Modify data in Nasstar systems or services which does not belong to the researcher
- Disrupt Nasstar services or systems
- Social engineer, 'phish' or physically attack Nasstar employees, customers, members of the public, contractors, suppliers, services, systems, or infrastructure
- Disclose any vulnerabilities in Nasstar systems or services to third parties or the public, prior to the Nasstar confirming that those vulnerabilities have been mitigated or rectified
- Require financial compensation to disclose any vulnerabilities

We ask you to delete securely all data retrieved during your research as soon as it is no longer required or within one month of the vulnerability being resolved, whichever occurs first.

5 Legalities

This Policy is designed to be compatible with common good practice among well-intentioned security researchers. It does not give you permission to act in any manner that is inconsistent with the law, or which might cause Nasstar to be in breach of any of its legal obligations, including in respect of computer use, data protection and privacy, third party intellectual property rights and confidentiality (including official secrecy).

Nasstar affirms that it will not seek prosecution of any security researcher who reports any security vulnerability on a Nasstar service or system, where the researcher has acted in good faith and in accordance with this disclosure policy.

If at any time you are unsure if your intended or actual actions are acceptable, contact Nasstar for guidance at infosec@nasstar.com.

6 Document Control

This document is the property of Nasstar Group.

It will not be reproduced wholly or in part without the permission of the author.

Any suggested changes or amendments must be communicated through the author for consideration and inclusion if suitable.

7 Document Details & Change Summary

Document Name:	Responsible Disclosure Policy	
Document Number:	POL052	
Issue:	V3.0	
Owner:	GRC Team	
Approved by:	***Position***	***Date***
	Chief Information Security Officer	07/12/2021
Release Date:	07/12/2021	

Issue	Change Description	Date	Created By
1.0	New document created, reviewed, approved & released	28/01/2020	GMT
2.0	Document reviewed; minor amends made. No new content added.	13/01/2021	GMT
3.0	Document reviewed and rebranded to reflect the change from GCI to Nasstar. No new content added, minor grammar changes made.	07/12/2021	GMT