Noggin Vulnerability Disclosure Policy

V1.0

15th November | 2021

Document Control

Version:	1.0
Created by:	Gary Lansdown
Approved by:	Owen Prime
Date of version:	15th November 2021

Change history

Date	Version	Created by	Description of change
15/11/2021	10	Gary Lansdown	Initial version

TABLE OF CONTENTS

1 Purpose

As part of Noggin's ongoing efforts to ensure the confidentiality, integrity and availability of data and platforms, Noggin has established a Vulnerability Disclosure Programme (VDP) to encourage the responsible reporting of suspected vulnerabilities or weaknesses in IT services, systems, resources and/or processes which may potentially affect internet-accessible applications. Our VDP is one part of a broader vulnerability management strategy which includes internal code review, vulnerability scanning and penetration testing.

Noggin values and supports the work undertaken by the security research community and appreciate it when researchers take the time to report potential security vulnerabilities to us. The Noggin Vulnerability Disclosure Program provides security researchers a mechanism to directly submit research findings if they believe they have found a potential security vulnerability within the Noggin Platform. We look forward to working with the cybersecurity research community and members of the public to keep our services safe for all users.

1.1 About this policy

The confidentiality, integrity and availability of Noggin Platforms is our highest priority, and we take every care to keep them secure. Despite our efforts, there may still exist some vulnerabilities.

We would like to engage with the security community and our VDP allows security researchers to report their findings. If you think you have found a potential vulnerability in any of our systems, services, or products, please notify us as soon as practical.

You are expected to act responsibly at all times. If you have questions about the proposed course of conduct, please contact us immediately via email at support@noggin.io.

Please note that the VDP does not authorise or permit the taking of any action which may contravene applicable laws and regulations. For the avoidance of doubt, attempts to exploit or test suspected vulnerabilities (e.g., gaining unauthorised access to any computer program or data) are prohibited.

1.2 Guideline Summary

- You cannot cause any harm, hinder application fluency or act against our Terms of Service agreed with customers.
- Remember to provide a detailed summary of the vulnerability, including the target, steps, tools, and artifacts used during the discovery that will allow us to reproduce the vulnerability.

- Do not intentionally access non-public Noggin data or system any more than is necessary to demonstrate the vulnerability.
- You shall be aware that you cannot compromise the privacy or safety of our customers and the operation of our services. Such activity will be treated as illegal.
- You are obliged to comply with applicable laws and regulations.

1.3 Scope

The Noggin VDP covers:

- The Noggin 2.0 Platform and underlying or related systems owned and operated by Noggin.

The Noggin VDP does not cover:

- social engineering or phishing
- denial of service (DoS)
- physical attacks
- attempts to modify or destroy data

2 Responsible Disclosure

- Act responsibly for the sole purpose of reporting suspected vulnerabilities and safeguarding users from damage, harm or loss
- Avoid causing any kind of damage, harm or loss to individuals or organisations (e.g., you should not attempt to test, reproduce or verify the suspected vulnerability, or take any action which may cause interruption to or degradation of any services)
- Conduct yourself in accordance with applicable laws and regulations at all times. If you have any doubt about such laws or regulations, please seek professional legal advice. Under no circumstances should you attempt to exfiltrate any computer data or publish details of any suspected vulnerability

2.1 Reporting a Suspected Vulnerability

1. Upon detection of a suspected vulnerability, please notify us immediately or as soon as possible by submitting a report to us at email support@noggin.io
2. Where applicable, provide your name, email address and mobile/cell number in the suspected vulnerability report so that we may contact you for clarifications.

Include the name(s) and email(s) of other person(s) to whom you may have disclosed the suspected vulnerability

3. Provide adequate information in the suspected vulnerability report so that we may work with you on validating the suspected vulnerability. Please include these details (where available):
    a. Description of the suspected vulnerability
    b. IP address and/or URL of the service
    c. Configuration and version of the subject software
    d. Description of the circumstances, including date(s) and time(s), leading to your reporting of the suspected vulnerability
    e. Description of the reason(s) why you believe the suspected vulnerability may impact the subject service and the extent of such suspected potential impact (e.g. describe how you believe the suspected vulnerability might potentially operate)
    f. How to replicate the discovery
    g. Any non-public data and/or system that was accessed

2.2 What NOT to do

- Act in any way which may contravene applicable laws and regulations
- Publish or publicly disclose any suspected vulnerability to any third party before it is resolved. Malicious actors may exploit the suspected vulnerability to cause damage, harm or loss to individuals and organisations
- Deploy destructive, disruptive or other unlawful means to detect vulnerabilities (e.g., attacks on physical security, social engineering, denial of service, brute force attacks)
- Exploit, test or otherwise use any suspected vulnerability (e.g., taking any step(s) to access, copy, create, delete, modify, manipulate or download any data, build system backdoor(s), modify system configuration(s), facilitate or share system access)

If you have any doubts about the proposed course of conduct, please contact us immediately at email support@noggin.io

2.3 What happens next

We will:

1. Respond to your report within 5 business days.
2. Keep you informed of our progress.

3. Agree upon a date for public disclosure.
4. Credit you as the person who discovered the vulnerability unless you prefer us not to.

2.4 Timing

Except under exceptional circumstances, Noggin agrees that the maximum period for which a vulnerability can remain private before being published by the person(s) responsible for discovering it shall be 90 business days.

Please note that Noggin does not and will not in any way:

- Accord or provide you with any kind of exemption, immunity, indemnity or shield from civil or criminal liability (if any) under applicable laws and regulations
- Be liable for any expense, damage or loss of any kind which you may incur due to any action taken or not taken by us in relation to any suspected vulnerability you may report
- Accept or assume any responsibility for the contents of any suspected vulnerability report submitted by you, nor shall our acknowledgment or processing of such report constitute any kind of acceptance or endorsement of the contents therein
- Be obliged to consult you for any media or public statement that we and/or may decide to publish or release in relation to the suspected or validated vulnerability
- Provide you with any cash reward or financial incentive of any kind for the detection and/or resolution of the validated vulnerability