HGF Limited

Vulnerability Disclosure Policy

Public

Document owner	Head of IT Operations & Security
Audience	Public — security researchers, customers, suppliers, members of the public
Version	1.0
Effective date	[To be confirmed on publication]
Review cycle	Annual, or sooner if material changes occur
Contact	security@hgf.com

1. Introduction

HGF Limited ("HGF", "we", "our") takes the security of our systems, our clients' information, and the wider public seriously. We welcome reports from the security research community and members of the public who identify potential security vulnerabilities in our products, services, or infrastructure.

This policy explains how to report a vulnerability to us, what you can expect from us in return, and the conditions under which we ask researchers to operate. It is designed to align with the principles of ISO/IEC 29147 (vulnerability disclosure), ISO/IEC 30111 (vulnerability handling), and the UK National Cyber Security Centre's Vulnerability Disclosure Toolkit.

2. Scope

In scope

This policy applies to vulnerabilities discovered in any public-facing system owned or operated by HGF Limited, including but not limited to:

- Our primary website and any sub-domains of hgf.com
- Client-facing portals, extranets, and document exchange services operated by HGF
- Email and authentication services where misconfigurations are externally observable
- Mobile or web applications that HGF publishes under its own name

Out of scope

The following are explicitly out of scope and should not be tested or reported under this policy:

- Third-party services, platforms, or websites not operated by HGF (please report these to the relevant vendor)

- Physical attacks against HGF offices, staff, or property
- Social engineering of HGF staff, clients, or contractors (including phishing, vishing, or pretexting)
- Denial-of-service attacks, volumetric testing, or any activity that may degrade service for other users
- Findings from automated scanners that have no demonstrable security impact (e.g. missing security headers without a working exploit)
- Reports of outdated software versions without a working proof-of-concept exploit
- Issues relating to email standards (SPF, DKIM, DMARC) where no active exploitation is demonstrated
- Self-XSS, clickjacking on pages with no sensitive actions, or other low-impact theoretical issues

3. How to report a vulnerability

If you believe you have identified a security vulnerability in a system within scope, please contact us at **security@hgf.com**.

To help us triage and respond as quickly as possible, please include the following in your report:

- A clear description of the vulnerability and its potential impact
- The affected URL, endpoint, or system
- Step-by-step reproduction instructions, including any required payloads or scripts
- Screenshots, request/response captures, or proof-of-concept code where helpful
- Your name or handle (if you wish to be credited) and a preferred method of contact

Reports may be submitted in English. We will accept anonymous reports, but this may limit our ability to ask follow-up questions or recognise your contribution.

4. Our commitments to you

When you submit a report in good faith and in line with this policy, HGF commits to the following:

- **Acknowledgement** — we will acknowledge receipt of your report within five (5) UK working days.
- **Triage** — we will validate and assess the report and provide an initial response within ten (10) UK working days.
- **Communication** — we will keep you informed of progress at reasonable intervals as we investigate and remediate.
- **Resolution** — we will work to remediate confirmed vulnerabilities in a timeframe proportionate to their severity, typically within 90 days for high or critical issues.
- **Recognition** — with your consent, we will acknowledge your contribution. HGF does not currently operate a paid bug bounty programme.
- **Safe harbour** — see Section 6 below.

5. What we ask of you

To protect our clients, our staff, and the integrity of any investigation, we ask that researchers acting under this policy:

- Make a good-faith effort to avoid privacy violations, degradation of user experience, disruption to production systems, and destruction or modification of data
- Only interact with accounts you own or with explicit permission from the account holder
- Do not access, modify, retain, or share any data belonging to HGF, our clients, or other users beyond what is strictly necessary to demonstrate the vulnerability
- Stop testing and contact us immediately if you encounter personal data, client confidential information, or any indication of pre-existing compromise
- Allow HGF a reasonable period to investigate and remediate before any public disclosure (we typically request a coordinated disclosure window of 90 days from the date of acknowledgement)
- Do not engage in extortion, threats, or any attempt to leverage findings for commercial gain outside of this policy

6. Safe harbour

HGF considers security research and vulnerability disclosure activities conducted in accordance with this policy to be authorised. We will not pursue civil action or initiate a complaint to law enforcement against researchers who:

- Act in good faith and follow the terms of this policy
- Do not exploit the vulnerability beyond what is necessary to confirm its existence
- Report the vulnerability to HGF promptly and do not disclose it publicly before agreed remediation

If legal action is initiated by a third party against you for activities conducted in accordance with this policy, we will take reasonable steps to make it known that your actions were authorised under this disclosure programme.

This safe harbour does not extend to activity that is malicious, unlawful, or outside the scope of this policy. HGF reserves the right to take all appropriate action to protect its systems, staff, and clients, including referral to law enforcement, where activity falls outside this policy.

7. Confidentiality and personal data

Information you provide as part of a vulnerability report will be handled in line with HGF's Privacy Notice and applicable data protection law, including the UK GDPR and Data Protection Act 2018. We will use the information solely for the purpose of investigating, resolving, and where appropriate disclosing the reported vulnerability.

We ask researchers not to include client personal data, client confidential information, or third-party credentials in their reports. If such information is encountered during testing, it must not be retained, copied, or shared, and should be reported to HGF immediately so we can take appropriate action.

8. Coordinated disclosure

HGF supports the principle of coordinated vulnerability disclosure. Where a researcher wishes to publish details of a confirmed vulnerability, we ask that publication is delayed until remediation is in place and affected parties have been notified, normally within 90 days of acknowledgement. We are happy to coordinate timing of any joint disclosure or public statement with researchers on request.

9. Policy maintenance

This policy will be reviewed at least annually by the Head of IT Operations & Security, or sooner where there is a material change to HGF's services, threat landscape, or applicable regulation. The current version of this policy is published at https://hgf.com/security.

Document control

Owner: Head of IT Operations & Security • **Classification:** Public • **Version:** 1.0