InstaGroup Vulnerability Disclosure Policy

This is InstaGroup's (the "organisation") Vulnerability Disclosure Policy.

We recommend reading this disclosure policy fully before you report any vulnerabilities. This helps ensure that you understand the policy, and act in compliance with it.

Reporting

If you believe you have found a security vulnerability, please submit your report to us using the following email: **compliance@instagroup.co.uk**

In your report please include:

Vulnerability Details:

- Asset (web address, IP Address, product or service name) where the vulnerability can be observed
- When the vulnerability was identified
- Title of vulnerability
- Description of vulnerability (this should include a summary, supporting files and possible mitigations or recommendations)
- Impact (what could an attacker do?)
- Steps to reproduce. These should be a benign, non-destructive, proof of concept. This helps to ensure that the report can be triaged quickly and accurately. It also reduces the likelihood of duplicate reports, or malicious exploitation of some vulnerabilities, such as sub-domain takeovers.

Optional contact details:

- Name
- Email Address

What to expect

After you have submitted your report, we will respond to your report within 5 working days and aim to triage your report within 20 working days (the resolution time varies depending on the severity of the issue).

Priority for remediation is assessed by looking at the impact, severity and exploit complexity. Vulnerability reports might take some time to triage or address.

We will notify you when the reported vulnerability is remediated, and you may be invited to confirm that the solution covers the vulnerability adequately.

Guidance

DO NOT:

- Break any applicable law or regulations
- Disrupt the organisation's services or systems
- Modify data in the organisation's systems or services
- Use invasive or destructive scanning tools to find vulnerabilities
- Access unnecessary, excessive or significant amounts of data
- Attempt or report any form of denial of service, e.g. overwhelming a service with a high Volume of requests
- Disclose any vulnerabilities prior to InstaGroup confirming that those vulnerabilities have been mitigated and rectified.