RESPONSIBLE DISCLOSURE POLICY

1. Introduction
Inside Ideas Group Ltd ("IIG" consisting of Oliver Marketing Ltd, Dare Digital Ltd, Aylesworth Fleming Ltd, Adjust Your Set Ltd and Oliver Inhouse India Pvt. Ltd) appreciates and values the identification and reporting of security vulnerabilities carried out by well-intentioned, ethical security researchers ("You").his responsible disclosure policy encourages collaboration with security researchers to enhance cybersecurity and applies to any vulnerabilities you are considering reporting to us. We recommend reading this vulnerability disclosure policy thoroughly before submitting a report and always following its guidelines.

2. Reporting
If you believe you have found a security vulnerability, please submit your report to us using the following email address: Cybersecurity@brandtechglobal.com

Your report should include details of:

- The website, domain, IP or page where the vulnerability can be observed.
- Steps to reproduce the issue, which should be a benign, non-destructive proof of concept.
- The type of vulnerability and any potential impact on our systems and/or customers.

If you have any concerns or questions about reporting, please email us for advice.

3. What to expect
We aim to confirm receipt of your vulnerability report within five working days and to triage it within ten working days. We also aim to keep you updated on our progress and the completion of any remediation activities. We may contact you if we need further information regarding your report.

Remediation of any reported vulnerabilities will be evaluated based on their impact, severity, and exploit complexity. Vulnerability reports may take some time to triage or address. You are welcome to inquire about the status of your report, but no more than once every 14 days, to allow our teams to focus on remediation.

4. Guidance
You must NOT:

- Break any applicable laws or regulations, e.g. GDPR, Computer Fraud and Abuse Act, Computer Misuse Act, etc.
- Access, modify, delete, store or transfer significant amounts of data or modify data in our systems or services
- Disrupt our services or systems, use high-intensity invasive or destructive scanning tools to find vulnerabilities or attempt any form of denial of service
- Submit reports detailing non-exploitable vulnerabilities, or reports indicating that the services do not fully align with "best practice," for example, missing security headers
- Submit reports detailing TLS configuration weaknesses, for example, "weak" cipher suite support or the presence of TLS1.0 support
- Social engineer, "phish" or physically attack our staff or infrastructure
- Demand financial compensation to disclose any vulnerabilities

5. Legalities
This policy is designed to be compatible with common vulnerability disclosure good practice. It does not give you permission to act in any manner that is inconsistent with the law, or which might cause us to be in breach of any legal obligations.

You must:

- Always comply with data protection rules and must not violate the privacy of our users, staff, contractors, services or systems. You must not, for example, share, redistribute or fail to properly secure data retrieved from the systems or services
- Securely delete all data retrieved during your research as soon as it is no longer required or has been reported to us, regardless of whether the data was accessed directly (via an API) or indirectly (required by data protection law)