POLICY DI DIVULGAZIONE RESPONSABILE

Dentsu Aegis Network (DAN) believes that everybody should be safe and secure on the Internet. DAN is committed to maintaining the security of our assets, systems, and customers' information. If any potential vulnerabilities are identified in any product, system, or asset belonging to DAN, we encourage security researchers to contact us as soon as possible. If you believe you have identified a potential security vulnerability, please submit it in accordance with our **Responsible Disclosure Program**.

Thank you in advance for your submission. DAN does not operate a public bug bounty program and will not provide a reward or compensation in exchange for reporting potential issues.

Responsible Disclosure Program Guidelines

Researchers shall ensure that when in the process of disclosing potential vulnerabilities they:

- Do not engage in any activity that can cause potential or actual harm to DAN, DAN customers, or DAN employees.
- Do not engage in any activity that can potentially or actually degrade DAN services or assets or cause them to stop entirely.
- Do not engage in any activity that violates (a) applicable laws or regulations or (b) the laws or regulations of any country where (i) data, assets or systems reside, (ii) data traffic is routed or (iii) the researcher is conducting research activity
- Do not engage in any activity that puts DAN in violation of any (a) applicable laws or regulations or (b) the laws or regulations of any country where (i) data, assets or systems reside, (ii) data traffic is routed or (iii) the researcher is conducting research activity.
- Do not store, share, compromise or destroy DAN or any customer data. If any Personal Information is identified, you should immediately stop the activity, remove related data from your system, and immediately contact DAN. This is important for protecting any potentially vulnerable data, and you.
- Do not initiate a fraudulent financial transaction.
- Do not disclose any reported issues to third parties, or publish such reported issues publicly

By acting in accordance with the guidelines above and responsibly submitting your findings to DAN, DAN agrees not to pursue legal action against you unless it is compelled to do so by a regulatory authority, other third party, or applicable laws

Once a report is submitted, DAN commits to provide prompt acknowledgement of receipt of all reports (in any event, within 5 business days of

submission). Where possible, DAN shall use commercially reasonable endeavours to keep you reasonably informed of the status of any validated vulnerability that you report through this program

Submission Format

When reporting a potential vulnerability, please include a detailed summary of the vulnerability. This shall include the following:

- The target
- The steps
- The tools
- The artefacts
- You may include screen captures to illustrate detail.

Out of Scope Vulnerabilities

Certain vulnerabilities are considered out of scope for our Responsible Disclosure Program. Out-of-scope vulnerabilities include, but are not limited to:

- Physical testing of premises
- Social engineering. For example, attempts to steal cookies, fake login pages to collect credentials
- Phishing
- Denial of service attacks
- Resource Exhaustion Attacks

Please submit your report to: ResponsibleDisclosure@Dentsuaegis.com