Responsible Disclosure Guidelines

Born Digital supports the responsible disclosure of security vulnerabilities, as it is one of our top priorities to protect the privacy of our customer's data.

We will investigate legitimate reports and make every effort to quickly correct any vulnerability in our platform. To encourage responsible reporting, we will not take legal action against you nor ask local or international law enforcement to investigate you provided you comply with the following Responsible Disclosure Guidelines:

- Make a good faith effort to avoid privacy violations, destruction of data, and interruption or degradation of our services.
- Provide details of the vulnerability, including information needed to reproduce and validate the vulnerability and a Proof of Concept (POC).
- Do not modify or access data that does not belong to you.
- Public disclosures of any vulnerabilities (e.g. through social media or the press) can put our community at risk so please make sure you keep this confidential. Give Born Digital a reasonable time to correct the issue before making any information public.
- All submissions should be made via email at security@borndigital.co.nz
- None of the research you have undertaken when reporting a vulnerability should have been obtained by unlawful means such as:
    - Accessing, or attempting to access, accounts or data that does not belong to you
    - Attempts to use malware, viruses or similar harmful software
    - Sending unsolicited spam messages
    - Perform DDoS attacks

Bug bounty

We do not currently have a paid bug bounty program.