Grinning Dog Records Vulnerability Disclosure Policy

Grinning Dog Records are committed to addressing and reporting security issues through a coordinated and constructive approach designed to provide the greatest protection for Grinning Dog Records customers, partners, staff and all Internet users.

A security vulnerability is a weakness in our systems or services that may compromise their security. This policy applies to security vulnerabilities discovered anywhere by both Grinning Dog Records staff and by others using Grinning Dog Records services. The responsibility for this policy is with the senior management team of Grinning Dog Records who will review it on an annual process. All day-to-day staff must follow this policy and will receive regular training on how to follow it.

Reporting vulnerabilities:

If you believe you have discovered a vulnerability in one of our services or have a security incident to report, please email info@grinningdogrecords.com or fill out the contact form. Or use the KeeperChat application to use encrypted communication between yourself and the relevant team member.

Once we have received a vulnerability report, Grinning Dog Records takes a series of steps to address the issue:

1. We will provide prompt acknowledgement of receipt of your report of the vulnerability
2. We request the reporter keep any communication regarding the vulnerability confidential
3. We will work with you to understand and investigate the vulnerability
4. We will provide a timeframe for addressing the vulnerability.
5. We will notify you once the vulnerability has been resolved, to allow retesting by the reporter if needed.
6. We publicly announce the vulnerability in the release notes of the update. We may also issue additional public announcements, for example via social media.
7. Release notes (and blog posts when issued) will include a reference to the person/people who reported the vulnerability, unless the reporter(s) would prefer to stay anonymous.

Grinning Dog Records will endeavour to keep the reporter apprised of every step in this process as it occurs.

We greatly appreciate the efforts of security researchers and discoverers who share information on security issues with us, giving us a chance to improve our services, and better protect our customers. In line with general responsible disclosure good practice, we ask that security researchers:

- Allow Grinning Dog Records an opportunity to correct a vulnerability within a reasonable time period before publicly disclosing the identified issue.
- Provide sufficient detail about the vulnerability to allow us to investigate successfully including steps required to reproduce the issue

- We appreciate the use of the Common Vulnerability Scoring System when reporting a vulnerability:
- Do not modify or delete data, or take actions that would impact on Grinning Dog Records customers
- Do not carry out social engineering exercises or to attempt to find weaknesses in the physical security of Grinning Dog Records offices or other locations.