1. Purpose and application

1.1. Purpose

1.1.1. Cyferd is committed to protecting the confidentiality and integrity of its digital platform including its applications. Please read this Vulnerability Disclosure Policy ('Policy') fully, before you report a vulnerability and always act in accordance with this Policy.

1.1.2. Cyferd highly values those professionals who take the time and effort to report security weaknesses (such as vulnerabilities) in accordance with this Policy. Unfortunately, we do not offer monetary rewards for vulnerability disclosures at this moment in time, but should we in the future, this will be structured on a per case submittance.

1.2. Application

This Cyferd Vulnerability Disclosure Policy applies to any vulnerabilities you, being a person or organisation who is not an employee or authorised agent of Cyferd, are considering reporting to our Security Operations Department.

2. Policy Statement

2.1. Reporting

2.1.1. If you believe you have found a security vulnerability, please submit your report to us using the following email: SecOps@cyferd.com.

2.1.2. In your report, please include details of the following:

2.1.2.1. The website URL, IP or page where the vulnerability can be observed.

2.1.2.2. A brief description of the type of vulnerability, for example, "Buffer Overflow vulnerability".

2.1.2.3. Steps to replicate. These should be a benign, non-destructive, proof of concepts. This helps to ensure that the report can be triaged quickly and accurately, reducing time delays. It also reduces the likelihood of duplicated reports, or malicious exploitation of some vulnerabilities, such as sub-domain hijacking.

2.2. What to expect from Cyferd

2.2.1. After you have submitted your report via email, we will make every effort to respond to your report in a timely manner, usually 24hours. We'll also aim to keep you informed of our progress and steps of remediation (if required).

2.2.2. Priority for remediation is assessed by looking at the impact, severity, and exploit complexity. Vulnerability reports might take some time to triage or address. You are welcome to enquire on the status but should avoid doing so more than once every 14 days.

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

2.2.4. Once your vulnerability has been resolved, we welcome requests to disclose your own report to Cyferd via the Security Operations Department using the following email: SecOps@cyferd.com.

2.3. **Guidance**

2.3.1. You must not:

2.3.1.1. Break any applicable law or regulations in your residential country.

2.3.1.2. Access unnecessary, excessive or significant amounts of data.

2.3.1.3. Modify data in our hosted systems or services.

2.3.1.4. Use high-intensity, invasive or destructive scanning tools to find vulnerabilities, this will be seen as an act of unlawful penetration testing.

2.3.1.5. Attempt or report any form of denial of service including distributed denial of service, e.g. overwhelming a service with a high volume of requests or exhaustive flooding of broken handshakes (Syn flooding).

2.3.1.6. Disrupt our hosted services or systems.

2.3.1.7. Submit reports detailing non-exploitable vulnerabilities, or reports indicating that the services do not fully align with “best practice”, for example missing security headers or X frame options.

2.3.1.8. Social engineer, ‘phish’ or spear attack our staff, infrastructure or Cyferd in whole or part.

2.3.1.9. Demand monetary compensation in order to disclose any vulnerabilities.

2.3.1.10. Disclose any vulnerabilities or any material (relating in any way and in any form to Cyferd) to any third party and/or the public, in whole or part, until confirmed in writing by Cyferd that you may make such a disclosure.

2.3.1.11. You must not, for example, share, redistribute or fail to properly secure data retrieved from the systems or services.

2.3.2. **You must:**

2.3.2.1. Always comply with data protection legislation and must not violate the privacy of our users, staff, contractors, services or systems.

2.3.2.2. Securely destroy all data, in whatever form, retrieved during your research as soon as it is no longer required or within 5 days of the vulnerability being resolved, whichever occurs first (or as otherwise required by data protection law).

2.4. **No authorisation**

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 Cyferd to be in breach of any legal obligations.

Cyferd Inc.
Email: info@cyferd.com