Vulnerability Disclosure Policy

1. Purpose

This policy is intended to give security researchers clear guidelines for conducting vulnerability discovery activities directed at Canyon LTS web properties, and submitting discovered vulnerabilities to Canyon LTS.

2. Overview

Maintaining the security of our networks is a high priority at Canyon LTS.

The security researcher community regularly makes valuable contributions to the security of organizations and the broader Internet, and Canyon LTS recognizes that fostering a close relationship with the community will help improve our own security. So if you have information about a vulnerability in a Canyon LTS website or web application, we want to hear from you!

Information submitted to Canyon LTS under this policy will be used for defensive purposes – to mitigate or remediate vulnerabilities in our networks or applications, or the applications of our vendors.

Please review, understand, and agree to the following terms and conditions before conducting any testing of Canyon LTS networks and before submitting a report. Thank you.

3. Scope

Any public-facing website owned, operated, or controlled by Canyon LTS, including web applications hosted on those sites.

4. How to Submit a Report

Please provide a detailed summary of the vulnerability, including: type of issue; product, version, and configuration of software containing the bug; step-by-step instructions to reproduce the issue; proof-of-concept; impact of the issue; and suggested mitigation or remediation actions, as appropriate.

By submitting your report to security@canyonlegal.com you are indicating that you have read, understand, and agree to the guidelines described in this policy for the conduct of security research and disclosure of vulnerabilities or indicators of vulnerabilities related to Canyon LTS information systems, and consent to having the contents of the communication and follow-up communications stored on Canyon LTS information systems.

5. Guidelines

Canyon LTS will deal in good faith with researchers who discover, test, and submit vulnerabilities or indicators of vulnerabilities in accordance with these guidelines:

- Your activities are limited exclusively to –

    - Testing to detect a vulnerability or identify an indicator related to a vulnerability; or
    - Sharing with, or receiving from, Canyon LTS information about a vulnerability or an indicator related to a vulnerability.
- You do no harm and do not exploit any vulnerability beyond the minimal amount of testing required to prove that a vulnerability exists or to identify an indicator related to a vulnerability.
- You avoid intentionally accessing the content of any communications, data, or information transiting or stored on Canyon LTS information system(s) – except to the extent that the information is directly related to a vulnerability and the access is necessary to prove that the vulnerability exists.
- You do not exfiltrate any data under any circumstances.
- You do not intentionally compromise the privacy or safety of Canyon LTS personnel, or any third parties.
- You do not intentionally compromise the intellectual property or other commercial or financial interests of any Canyon LTS personnel or entities, or any third parties.
- You do not publicly disclose any details of the vulnerability, indicator of vulnerability, or the content of information rendered available by a vulnerability, except upon receiving explicit written authorization from Canyon LTS.
- You do not conduct denial of service testing.
- You do not conduct social engineering, including spear phishing, of Canyon LTS personnel or contractors.
- You do not submit a high-volume of low-quality reports.
- If at any point you are uncertain whether to continue testing, please engage with our team.

6. What You Can Expect From Us

We take every disclosure seriously and very much appreciate the efforts of security researchers. We will investigate every disclosure and strive to ensure that appropriate steps are taken to mitigate risk and remediate reported vulnerabilities.

Canyon LTS remains committed to coordinating with the researcher as openly and quickly as possible. This includes:

- Within three business days, we will acknowledge receipt of your report. Canyon LTS's security team will investigate the report and may contact you for further information.
- To the best of our ability, we will confirm the existence of the vulnerability to the researcher and keep the researcher informed, as appropriate, as remediation of the vulnerability is underway.
- We want researchers to be recognized publicly for their contributions, if that is the researcher's desire. We will seek to allow researchers to be publicly recognized whenever possible. However, public disclosure of vulnerabilities will only be authorized at the express written consent of Canyon LTS.

Information submitted to Canyon LTS under this policy will be used for defensive purposes – to mitigate or remediate vulnerabilities in our networks or applications, or the applications of our vendors.

7. Legal

You must comply with all applicable laws in connection with your security research activities or other participation in this vulnerability disclosure program.

Canyon LTS does not authorize, permit, or otherwise allow (expressly or impliedly) any person, including any individual, group of individuals, consortium, partnership, or any other business or legal entity to engage in any security research or vulnerability or threat disclosure activity that is inconsistent with this policy or the law. If you engage in any activities that are inconsistent with this policy or the law, you may be subject to criminal and/or civil liabilities.

To the extent that any security research or vulnerability disclosure activity involves the networks, systems, information, applications, products, or services of a non-Canyon LTS entity, that non-Canyon LTS third party may independently determine whether to pursue legal action or remedies related to such activities.

If you conduct your security research and vulnerability disclosure activities in accordance with the restrictions and guidelines set forth in this policy, (1) Canyon LTS will not initiate or recommend any law enforcement or civil lawsuits related to such activities, and (2) in the event of any law enforcement or civil action brought by anyone other than Canyon LTS, Canyon LTS will take steps to make known that your activities were conducted pursuant to and in compliance with this policy.

Canyon LTS may modify the terms of this policy or terminate the policy at any time.