Vulnerability Disclosure Policy for Reporters

The purpose of this policy is to help customers, security researchers, and reporters (collectively, "Reporters") responsibly research and disclose potential security vulnerability in our products and services. Our primary goals are to protect our customers' privacy, safety, information systems, and operations, to work with you, and to provide transparency into the process. We will not engage in legal action against any Reporter who reports in good faith and adheres to this policy.

If you need to perform testing that is not provided for in this policy, please contact Qualitrol so that we can work with you and provide the necessary information to help you achieve effective test results.

Reporters MUST adhere to the following guidelines.

General

- Reporters MUST comply with all applicable laws and regulations in connection with all activities under this policy.
- Reporters MUST abide by this policy as well as all Qualitrol Terms and Conditions of Sale, Terms of Service, End User License Agreements, and other applicable licenses, policies, regulations and laws.

Scope of Authorized Testing

- The scope of authorized testing includes Qualitrol's products, software, web services, and mobile applications ("Authorized Qualitrol Products and Services").
- Reporters MAY ONLY test Authorized Qualitrol Products and Services to detect a vulnerability for the sole purpose of providing Qualitrol information about that vulnerability.
- Reporters SHOULD only test against test accounts or products owned by the Reporter or with explicit written permission from the account holder or product owner.
- Reporters MUST avoid harm to Qualitrol's and its customers' information systems and operations.
- Reporters MUST make every effort to avoid privacy violations, degradation of user experience, disruption to production systems, and destruction or manipulation of data.
- Reporters MUST stop testing once that testing has established that a vulnerability exists, or sensitive data has been encountered. Sensitive data includes personally identifiable information, financial information (e.g., account numbers), proprietary information or trade secrets.
- Reporters MUST NOT test any Qualitrol products and services not available through a normal purchasing agreement.

- Reporters MUST NOT exploit any vulnerability beyond the minimal amount of testing required to prove that the vulnerability exists or to identify an indicator related to that vulnerability.
- Reporters MUST NOT intentionally access the content of any communications, data, or information transiting or stored on Qualitrol's 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.
- Reporters MUST NOT exfiltrate any data under any circumstances.
- Reporters MUST NOT intentionally compromise the privacy or safety of Qualitrol's personnel, customers, the general public, or any legitimate third parties.
- Reporters MUST NOT use any exploit to compromise, alter, or exfiltrate data.
- Reporters SHOULD NOT establish command line access and/or persistence.
- Reporters MUST NOT exploit any vulnerabilities found to pivot to other systems.
- Reporters MUST NOT intentionally compromise the intellectual property or other commercial or financial interests of any Qualitrol's personnel or entities, customers, or any legitimate third parties.
- Reporters MUST NOT cause a denial of any legitimate services in the course of their testing.
- Reporters MUST NOT perform physical access testing (e.g. office access, open doors, tailgating, or other trespass).
- Reporters MUST NOT conduct social engineering in any form of Qualitrol personnel or contractors.
- Reporters SHOULD contact Qualitrol at security@qualitrolcorp.com if at any point you are uncertain of whether to proceed with testing.

Coordination with Qualitrol

- Reporters SHOULD submit vulnerability reports to Qualitrol via Qualitrol web page https://www.qualitrolcorp.com/about-qualitrol/product-security/ .
- Reporters SHOULD include sufficient descriptive details to permit Qualitrol to accurately reproduce the vulnerable behavior.
- Reporters SHOULD NOT report unanalyzed crash dumps or fuzzer output unless accompanied by a sufficiently detailed explanation of how they represent a security vulnerability.

- Reporters SHOULD report other vulnerabilities found incidental to their in-scope testing even if those vulnerabilities would be otherwise considered out-of-scope. For example, while testing an in-scope system the reporter finds it to be exposing data from out-of-scope system. These are still reportable vulnerabilities.
- Reporters MUST keep confidential any information about vulnerabilities discovered regarding service levels provided in purchase agreements after you have notified Qualitrol.
- Reporters MAY include a proof-of-concept exploit if available.
- Reporters MAY request that their contact information be withheld from all affected vendor(s).
- Reporters MAY request not to be named in the acknowledgements of Qualitrol's public disclosures.
- Reporters MUST NOT require Qualitrol to enter into a customer relationship, non-disclosure agreement (NDA) or any other contractual or financial obligation as a condition of receiving or coordinating vulnerability reports.
- Reporters MUST NOT demand compensation in return for reporting vulnerability information reported outside of an explicit bug bounty program.
- Qualitrol SHALL confirm receipt of the vulnerability report with the Reporter.
- Qualitrol MAY investigate the vulnerability report and inform the Reporter through the means defined in the report submission.
- Qualitrol MAY contact the Reporter for more information if Qualitrol cannot validate the reported vulnerability.
- Qualitrol MAY communicate with the Reporter on the mitigation status.
- Qualitrol MAY communicate with the Reporter when a mitigation has been validated and when it will be released to Qualitrol customers.
- Qualitrol MAY attribute the Reporter in any security advisories Qualitrol publishes about the vulnerability the Reporter discovered. The Reporter will have the option to opt-out of being attributed, at the Reporter's discretion.

Disclosure to third parties

- Reporters MUST NOT disclose any information about any active Qualitrol system vulnerability to any third party without Qualitrol's written permission, including confidential information rendered available by the vulnerability.

- Reporters MAY disclose to third parties the prior existence of vulnerabilities already fixed by Qualitrol, including details of the vulnerability, indicators of vulnerability, and the nature (but not content) of information rendered available by the vulnerability.
- In the event the Reporter finds a vulnerability in a Qualitrol system consequent to a vulnerability in a third party product or service, the Reporter MAY report that third party vulnerability to the provider of that third party product or service or a third party vulnerability coordination service in order to enable the third party product or service to be fixed.