Vulnerability Disclosure Program

QuIRC PeopleInsight is committed to ensuring the safety and security of our customers. Towards this end, QuIRC PeopleInsight is formalizing a policy for accepting vulnerability reports in our products. We hope to foster an open partnership with the security community, and we recognize that the work the community does is important in continuing to ensure safety and security for all of our customers. We have developed this policy to both reflect our corporate values and to uphold our legal responsibility to good-faith security researchers that are providing us with their expertise.

Initial Scope

QuIRC PeopleInsight's Vulnerability Disclosure Program initially covers the following products:

- PeopleInsight Analytics (*analytics.yourpeopleinsight.com*)
- Your PeopleInsight (*yourpeopleinsight.com*)

We ask that all security researchers submit vulnerability reports only for the stated product list. We intend to increase our scope as we build capacity and experience with this process. Researchers who submit a vulnerability report to us will be given full credit on our website once the submission has been accepted and validated by our product security team.

Legal Posture

QuIRC PeopleInsight will not engage in legal action against individuals who submit vulnerability reports through our Vulnerability Disclosure Program. We openly accept reports for the currently listed products. We agree not to pursue legal action against individuals who:

- Engage in testing of systems/research without harming QuIRC PeopleInsight or its customers
- Engage in vulnerability testing within the scope of our vulnerability disclosure program and avoid testing against other systems not listed in this document
- Test on products without affecting customers, or receive permission/consent from customers before engaging in vulnerability testing against their devices/software
- Avoid exposing private corporate and customer data
- Adhere to the laws of their location and the location of QuIRC PeopleInsight. For example, violating laws that would only result in a claim by QuIRC PeopleInsight (not a criminal claim) may be acceptable as QuIRC PeopleInsight is authorizing the activity (reverse engineering or circumventing protective measures) to improve its system.
- Refrain from disclosing vulnerability details to the public before mutually agreed-upon timeframe expires (at least 60 days).

Preference, Prioritization, and Acceptance Criteria
We will use the following criteria to prioritize and triage submissions.

What we would like to see from you:

- Well-written reports in English will have a higher chance of resolution.
- Reports that include proof-of-concept code equip us to better triage.
- Reports that include only crash dumps or other automated tool output may receive lower priority.
- Please include how you found the bug, the impact, and any potential remediation.
- Please include any plans or intentions for public disclosure.

What you can expect from us:

- A timely response to your email (within 2 business days)
- After triage, we will send an expected timeline, and commit to being as transparent as possible about the remediation timelines as well as on issues or challenges that may extend it.
- An open dialog to discuss issues.
- Notification when the vulnerability analysis has completed each stage of our review.
- Credit after the vulnerability has been validated and fixed.

If we are unable to resolve communication issues or other problems, QuIRC PeopleInsight may bring in a neutral third party to assist in determining how best to handle the vulnerability.

How to Submit a Vulnerability Report
To submit a vulnerability report to QuIRC PeopleInsight's product security team, please provide all details here.

When a Vulnerability Report is Received
QuIRC PeopleInsight's internal process for addressing an issue disclosed to us:

- The receiving member of our IT team will review the issue with the IT Director
- The issue will be assigned to the relevant IT team member who is responsible for creating a plan to address the disclosure.
- Upon approval of the plan, the plan will be implemented.
- We will contact the individual who submitted the disclosure within 2 business days and remain transparent throughout the process.