IQSIGHT Responsible Disclosure Policy

IQSIGHT offers products of the best quality and reliability. This also includes to provide cybersecurity and protect our customers' privacy throughout the entire product life cycle. The IQSIGHT Product Security Organization supports this by helping to resolve security issues in IQSIGHT products reported by external security researchers, partners, or customers.

IQSIGHT Product Security Organization coordinates measures in case of potential security vulnerabilities or incidents with the responsible engineers and development teams, including establishing an appropriate response plan, and maintaining regular communication with the reporting party. IQSIGHT encourages coordinated disclosure of vulnerabilities, and we kindly ask the reporting party to keep the vulnerability confidential until we make a fix available.

We welcome and encourage vulnerability reports directly from researchers, industry groups, CERTs (Computer Emergency Response Teams), partners and any other source. We respect the interests of the reporting party (anonymous reports are also welcome) and agree to address any vulnerability that is reasonably believed to be related to our products or services. We strongly urge reporting parties to perform a coordinated disclosure, as immediate public disclosure puts our customers' systems at unnecessary risk.

IQSIGHT currently does not offer any monetary compensation for vulnerability reports. Requests or demands for monetary compensation in connection with any identified or alleged vulnerability are non-compliant with the IQSIGHT Vulnerability Disclosure Program.

We appreciate and acknowledge the efforts made by reporting parties in identifying and reporting vulnerability and working with us to ensure the safety of IQSIGHT customers and the broader community.

IQSIGHT Commitment

We kindly ask the reporting party to not share or publicize an unresolved vulnerability with/to third parties.

By following the IQSIGHT Responsible Disclosure Policy, the IQSIGHT Product Security Organization and associated development teams will use reasonable efforts to:

- Respond quickly and acknowledge receipt of the vulnerability report
- Provide an estimated time frame for addressing the vulnerability report
- Notify the reporting party when the vulnerability has been fixed

Our standard response time to acknowledge receipt of vulnerability reports is typically 2 working days. Status updates of reported vulnerabilities are given when relevant information becomes available.

IQSIGHT agrees not to pursue claims against reporting parties related to disclosures submitted to us providing the following:

- The reporting party does not cause harm to IQSIGHT, our customers, or others.
- The reporting party does not compromise the privacy or safety of our customers or the operation of our services.
- The reporting party does not violate any criminal law.
- The reporting party publicly discloses vulnerability details only after IQSIGHT confirms completed remediation of the vulnerability.