

## EP Cube Vulnerability Disclosure and Reporting Policy

At EP Cube, safeguarding the security of our energy systems and supporting cloud architecture is paramount. This policy stands as a cornerstone of our security program, underscoring our belief that collaboration with the security industry accelerates the identification and resolution of security issues. We actively encourage responsible investigation and reporting of security concerns directly to EP Cube. Kindly report all security issues via our dedicated email: [cybersecurity@epcube.com](mailto:cybersecurity@epcube.com).

### Scope of Policy

This policy encompasses all identified security issues—known or potential—in any EP Cube device or system. This spans across WIFI/RTU modules, EP Cube app, web monitoring portal, websites and systems.

### Expectations for Disclosers

Contributing to the global good, we kindly request adherence to the following guidelines:

**Act Promptly:** Notify us as soon as possible upon discovering a real or potential security issue.

**Give Us Time:** Refrain from disclosing issues to others until we've had adequate time to address them.

**Respect Confidentiality and Privacy:** Avoid retaining or disclosing confidential information to others, including EP Cube's or others' confidential information and personal details.

**Do No Harm:** Abstain from actions affecting user experience, systems, or the confidentiality, integrity, or availability of data. This includes avoiding excessive attempts impacting server availability, viewing or extracting information exposing it to further security issues, attempting unauthorized access to systems, altering public-facing material, and engaging in non-technical testing dependent on the actions of people.

**Provide Complete Information:** Furnish us with as much relevant information as possible.

**Be Honest:** Share only accurate information; refrain from providing false or misleading information, misrepresenting your identity, or presenting inaccurate technical details.

### Our Commitment to the Cyber Security Community

In alignment with this policy, EP Cube commits to:

**Respond Promptly:** Acknowledge your initial report within one week.

**Collaborate as Necessary:** Work with you to understand the issue if not apparent from your initial report.

**Remediate Promptly:** Prioritize and remediate vulnerabilities based on their severity.

### Legal Framework

EP Cube adhere to all applicable laws, rules, and regulations and expect the same from you. This policy does not establish private obligations or form a contract between EP Cube and any other party. While EP Cube retains sole discretion to decide whether to compensate for disclosures, no compensation will be provided to individuals on a government sanctions list or in a country on such a list.