QATARENERGY RESPONSIBLE DISCLOSURE POLICY

1. About this Policy

QatarEnergy recognizes the importance of maintaining the security of its information technology systems and infrastructure. As part of our commitment to security, we have established this Responsible Disclosure Policy to convey our expectations for the safe, secure, and responsible reporting of discovered vulnerabilities within our systems.

The purpose of this Policy is to provide a framework that allows for vulnerabilities to be reported responsibly and remediated or patched, in order to maintain the integrity, continuity, and security of our services. If you are a security researcher and you encounter a vulnerability, we would like to cooperate with you to fix the vulnerability before it is disclosed to the outside world and can be misused. This is known as “responsible disclosure”.

2. Scope

We request that you communicate any findings related to vulnerabilities in our systems as soon as reasonably possible, in the manner described below. We are interested in the following categories of vulnerabilities: remote code execution, SQL injection vulnerabilities, authentication or authorization flaws, server-side code execution, bugs, encryption vulnerabilities

The following are considered out of scope:

- Reports on service complaints (please contact your local QatarEnergy office)
- Reports on potential fraud or compliance issues (please contact the QatarEnergy Global Helpline)
- Reports on phishing campaigns or emails, viruses, or malware (please report to CyberIncidentReport@qatarenergy.qa)

3. Reporting a vulnerability responsibly

If you have discovered a vulnerability, please describe it in detail with supporting evidence if possible, so that our information risk experts can analyze the finding. To the extent possible, please include the following in your report:

- Type of vulnerability or issue
- Service, product, or URL affected
- Special configuration or requirements to reproduce the issue
- Information necessary to reproduce the issue
- Impact of the vulnerability, together with an explanation of how an attacker could find it and exploit it

We prefer communications to be in English or Arabic. You can send the report to CyberIncidentReport@qatarenergy.qa. We welcome anonymous reports but please note that, if anonymous, we will not be able to share updates on the follow-up of the report with you.

The size of the email communication should not exceed 10MB. Please contact us in advance via the email address above should you need to send an attachment that is larger than this size.

Our information risk analysts will assess the finding and respond as soon as reasonably possible. Each case will be analyzed individually. We request that you provide us with a reasonable opportunity and time for analysis keep the information confidential, and not disclose the vulnerability to others without consultation with our analysts.

Any personal details that we have received from your side will be processed by us in accordance with the Qatar Energy global privacy notice for business customers, partners, and counterparties. Your data will be processed for the purposes of responding to your report and addressing the reported vulnerabilities. We will retain your data for as long as your report is investigated and up to one year thereafter.

4. Ethical engagement rules

We take the security of our systems and infrastructure seriously, and we appreciate the efforts of security researchers who responsibly disclose any vulnerabilities they find. To ensure that our systems are secure and to prevent any harm to our employees, customers and stakeholders, we ask that you follow these rules of ethical engagement when reporting a vulnerability:

- Report the vulnerability to us at CyberIncidentReport@qatarenergy.qa.
- Report the vulnerability as soon as possible to prevent any potential harm.
- Keep the information (and any data obtained as a result of the issue) confidential, avoid storing confidential data, and do not disclose it to others.
- Make every effort to avoid compromising the privacy of third party or personnel data;
- Do not exploit the vulnerability for your benefit or the detriment of QatarEnergy, our employees, customers, and stakeholders.
- Do not use social engineering to gain access to our systems or infrastructure.
- Do not install any backdoors or modify any data in our systems.
- Do not copy, modify, or remove any data from our systems.
- Do not negatively impact the confidentiality, integrity, or availability of our services.
- Do not use any denial of service attacks or brute force access technology.
- Do not use any automated scanning.

5. Reporting a vulnerability

If you believe you have found a vulnerability in any of our systems or infrastructure, please report it to us by emailing CyberIncidentReport@qatarenergy.qa. We ask that you provide us with as much detail as possible, including:

- The type of vulnerability or issue you discovered.
- The service, IP or URL affected.
- Any special configuration or requirements needed to reproduce the issue.
- Information necessary to reproduce the issue.
- The impact of the vulnerability and an explanation of how an attacker could exploit it.

Our security team will review your report as soon as possible and work to remediate the vulnerability in a timely manner. We will keep you informed of our progress, and we appreciate your cooperation in helping us maintain the security of our systems and infrastructure.

6. Questions

If you have any questions about our Responsible Disclosure Policy or the reporting process, please email us at CyberIncidentReport@qatarenergy.qa. We appreciate your commitment to responsible disclosure and look forward to working with you to keep our systems and infrastructure secure.