Meridian

Meridian Responsible Disclosure Statement

Statement

At Meridian, we are committed to protecting the security and privacy of our information and services. This document outlines our statement on how we collaborate with the public to identify, validate, and fix security issues in our systems. In this document "Meridian", "we", "us" or "our" means or refers to Meridian Energy Limited and our related companies.

How you can help

If you believe you have found a security vulnerability in our systems, please let us know as soon as possible. We value your feedback and will work with you to understand and resolve the issue. Please act only in the scope of this document.

Note: Meridian does not offer financial rewards or 'bug bounties' for reported security issues.

Acting responsibly

By accessing our systems and websites, you agree to maintain the security of customers and stakeholders, and when testing or reporting security issues you agree to:

- **Protect Privacy:** protect people's privacy and not access, use, copy, store, or disclose personal information, in accordance with the Privacy Act 2020.
- **Protect Data Integrity:** only view the minimum information necessary to confirm the security issue and leave all Meridian data unchanged.
- **Prevent Disruption:** carry out all testing in a way that does not degrade, interrupt, or impact Meridian services.
- **Maintain Confidentiality:** keep all details of the security issue confidential and only share them with Meridian through the approved reporting channels until a coordinated disclosure has been agreed.

Our commitment to you

If you act in good faith and in accordance with this statement, subject to compliance with applicable law and Meridian's contractual obligations, Meridian commits to:

- **No action:** Not take action if in Meridian's reasonable opinion you have undertaken good-faith security research and have acted in accordance with this statement.
- **Communication**: Acknowledge your report within **7 days** and keep you updated on progress.
- **Protect confidentiality:** Treat your report as confidential and limit sharing to those who need to know to investigate and resolve the issue, unless we are required to act under the Privacy Act 2020.
- **Recognise your contribution**: Where we consider it appropriate, we will recognise your contribution as the first reporter of a valid issue that leads to security improvements.

Scope

In-scope:

- Online services under the meridianenergy.co.nz domain.
- Other domains and online services Meridian Energy or our related companies own or operate.
- If you do not know if a service is within scope, please email us at ResponsibleDisclosure@meridianenergy.co.nz.

Reporting Active Threats:
We encourage you to report any active or imminent threats to Meridian you may have observed or know of. If you have information regarding an ongoing attack, phishing campaign targeting Meridian or our customers, or leaked Meridian data, please notify us immediately on: ResponsibleDisclosure@meridianenergy.co.nz.

Out-of-scope (prohibited testing):
The following test types are strictly prohibited and are not within the scope of this statement:

- Network level Denial of Service (DoS/DDoS) attacks
- Social Engineering (e.g., phishing, spear phishing, whaling)
- Physical testing (e.g., office access, tailgating)
- UI/UX bugs or spelling mistakes

How to report a security issue

Please report your findings to: ResponsibleDisclosure@meridianenergy.co.nz.

Include the following details:

- The type and location of security issue.
- How you found the security issue.
- Whether the security issue has been published or shared with others.
- Affected configurations.
- Potential Exposure of any personal information.
- A detailed description of the steps required to reproduce the issue or risk, for example, proof of concept scripts, screenshots, and compressed screen captures are all helpful to us.
- Your name and contact details.

How to remain anonymous

The National Cyber Security Centre (NCSC) operate a coordinated vulnerability disclosure process where the finder of a security issue can use NCSC to notify affected vendors: https://www.ncsc.govt.nz/report/how-to-report-a-vulnerability/