Cyber Security Policy for Third Parties

Approved date	13 December 2023

1 POLICY STATEMENT

Meridian Energy Limited (**Meridian**) highly depends on third-party suppliers to achieve its mission and protect the interests of our employees, customers, and other stakeholders.

As a supplier of Services to Meridian, you must apply Good Industry Practice to:

- continually assess your cyber risk using a recognised risk management framework;
- apply effective security controls and formal cyber risk governance processes to protect you and us from cyber threats;
- implement appropriate security controls that consider your and our cyber risk and, without limitation, ensure that the bypassing of a single control or protection does not result in a Security Incident;
- use appropriate technologies, processes and procedures to address current and emerging cyber threats and maintain a consistent baseline of controls to detect, prevent and respond to those threats;
- ensure that your personnel have the right level of cyber security awareness and training required to carry out their roles and responsibilities;
- notify us promptly of any Security Vulnerabilities, weaknesses or incidents that may impact us and the delivery of your Service; and
- apply any learnings from a Security Incident to improve cyber posture and resilience.

2 SCOPE

This policy applies to all third parties that provide services to Meridian and in addition to any agreement “Agreement” between you and Meridian.

3 DATA PROTECTION

3.1 If you generate, collect, process, hold, store or transmit Meridian Data or have access to any Meridian Systems, we may request that you:

a) provide a written report summarising the result of any technical security assessment, for example, penetration testing, which is relevant to the Services and any risks identified during the security assessment, including:
   i. a detailed description of any identified actual or potential Security Vulnerability;
   ii. any applicable compensating controls;
   iii. the corrective action proposed for any identified Security Vulnerability; and
   iv. the expected timeframe for you to correct the Security Vulnerability;

b) engage a reputable independent third party to undertake an audit covering the security controls relevant to the Services and provide us with the assurance report. If the report reveals significant deficiencies that result in a level of risk in relation to the Services that we consider unacceptable (acting reasonably), then you must promptly meet with us to discuss and agree on appropriate corrective steps and apply those steps without delay.

3.2 Ensure that Meridian Data, whether in transit or at rest, is encrypted using industry-standard encryption protocols such as TLS 1.2 or higher for data in transit and AES-256 for data at rest. Additionally, define clear data handling procedures that address data lifecycle management, including creation, storage, transmission, and destruction.

3.3 Where Meridian Data includes Personal Information, you must hold and process that Meridian Data per our obligations under the Privacy Act 2020 or any succeeding legislation and our privacy policy, available at https://www.meridianenergy.co.nz/legal-and-privacy/privacy-policy.

3.4 Where Meridian Data includes payment card information, as defined in the Payment Card Industry Data Security Standard (PCI DSS), you must handle that data per our obligations under PCI DSS v4.0 or any successor standard, available at https://www.pcisecuritystandards.org/standards/.

3.5 When an Agreement ends, as acknowledged by Meridian, you must securely delete, destroy or return (as required by the Agreement) all Meridian Data, except to the extent that you need the Meridian Data to perform obligations owed to us under another Agreement or to meet any regulatory obligations.

4 SECURITY CONTROLS

4.1 Ensure your staff are trained in and understand your information security policies, standards, procedures, and responsibilities.

4.2 Use and regularly monitor logical access controls with appropriate levels of identification, authorisation, authentication, and traceability to restrict access to the Services and Meridian Data to only those individuals who require access to meet your obligations under an Agreement and ensure that those controls are updated when individuals change roles or leave.

4.3 Notify us of the last working day of any of your personnel who have had access to the Services, Meridian Data or Meridian Systems as soon as possible and in any event no later than 20 working days prior to their last working day.

4.4 Apply secure password policies that:

a) requires passwords to be constructed with resistance to brute force or guessing attacks;

b) requires passwords to be changed immediately following a suspected breach or specific threat;

c) requires new passwords not to be based on a previous password (a new password is required each time it is changed), and

d) prohibits the use of generic user IDs, default passwords and shared passwords by your users and administrators who access the Services you provide, Meridian Data or Meridian Systems.

4.5 In addition to a secure password policy in 4.4, implement Multi-Factor Authentication (MFA) for all accounts with administrative or privileged access to the Services you provide, Meridian Data or Meridian Systems.

4.6 Implement appropriate controls to detect and prevent Malicious Code or other Security Vulnerabilities on your systems and ensure that any third-party systems you use to provide the Services and communicate with Meridian Data or Meridian Systems do so.

4.7 Promptly apply patches or mitigations designed to address Security Vulnerabilities per the recommendation of the supplier of hardware or software that you use to provide Services to us.

4.8 Detect, prevent and monitor actual or suspected security breaches on any network, infrastructure or systems you use to provide Services to us, and document and regularly test a formal process for responding and recovering from such events.

4.9 Ensure that any remote connection to Meridian Systems is secure and complies with any specific security requirements we notify you of for third-party connections, including when you connect using an interface or specification we provide.

4.10 If you become aware of a Security Incident that has impacted or may significantly impact the delivery of any Service, the confidentiality of Meridian Data, or the integrity of Meridian Systems, you must:

a) Notify us within 24 hours of security incident discovery. 'Discovery' shall mean the moment when any employee of your organisation becomes aware or reasonably suspects a security incident has occurred that impacts or may impact Meridian services or data.

b) Promptly provide all information we reasonably request in relation to the incident, its manner of introduction, known indicators of compromise (IoCs) and the impact that the incident has had or is likely to have.

c) Provide regular status updates for the incident until resolved.

d) Provide as soon as practicable, but in any event within 7 days following resolution of the incident, a written report including (1) the date the incident occurred; (2) the length of

any outage; (3) a summary of the incident; (4) details such as individuals involved in any aspect of the incident handling, how/when the incident was detected, what was impacted, and any containment strategies; (5) the root cause of the incident; and (6) what corrective action(s) was taken to prevent reoccurrence.

5 SECURE DEVELOPMENT PRACTICES

This section applies if you supply to Meridian Services that include software or software development.

5.1 You must take all precautions in accordance with Good Industry Practice necessary to prevent the introduction of Malicious Code and Security Vulnerabilities to, or that impact on, the software you provide or develop, Meridian Data or Meridian Systems, including:

a) using best endeavours to ensure that, when you provide us with software, it does not contain any Malicious Code or Security Vulnerabilities and that you do not otherwise introduce Malicious Code or Security Vulnerabilities into any Meridian Systems; and

b) taking appropriate action when a Security Incident occurs, or Malicious Code or Security Vulnerabilities are discovered, such as quarantining the affected file, code, or hardware or software component (where applicable).

5.2 If you become aware of any Security Incident that involves the discovery or introduction of Malicious Code or Security Vulnerabilities, you must:

a) identify the Malicious Code or Security Vulnerabilities and the corrective actions required to contain and resolve the incident;

b) provide us with a software patch to fix, remedy, or remove the Malicious Code or Security Vulnerability as soon as reasonably practicable and in any case within one month or such other timeframe as we agree;

c) if requested by us, take all necessary and reasonable corrective action to eliminate the Malicious Code or Security Vulnerabilities and prevent reoccurrence (including implementing appropriate processes to prevent further occurrences) and rectify any consequence capable of rectification; and

d) if the Malicious Code or Security Vulnerabilities cause a loss of operational efficiency or loss of data, provide all necessary assistance that we request to mitigate the losses and restore the efficiency and/or data as quickly as practicable.

5.3 Before providing any software to us you must run your tests using the most recent version of a reputable, commercially available software program to ensure, to the extent possible, that the software:

a) meets the requirements of the applicable Agreement;

b) does not contain any Malicious Code or Security Vulnerabilities; and

c) will pass any acceptance testing conducted under that Agreement.

5.4 If you fail to run such tests, without limiting our other rights or remedies, you must cooperate fully with us and reimburse all reasonable costs incurred by Meridian in relation to that failure, including eliminating or reversing any adverse effects of any destructive element.

6 SUPPLY CHAIN SECURITY

6.1 In addition to the requirements in this policy, you will actively manage and mitigate all security, business continuity, and other security risks in your supply chain.

6.2 You must perform regular security reviews and compliance audits of your subcontractors to ensure adherence to good industry practices that align with Meridian's security policies and standards. Findings should be documented and made available to Meridian upon request.

6.3 You must maintain transparency in your supply chain by providing Meridian with a list of all subcontractors involved in the delivery of services, including details of their roles and the measures in place to manage associated cyber risks.

6.4 Ensure that any subcontractors you engage, who are our fourth parties, adhere to the same security requirements as outlined in this policy. You should have a third-party risk management program that includes regular security assessments, compliance audits, and remediation tracking to manage the security risks posed by fourth parties.

6.5 All subcontractors you engage must be bound by contractual obligations that align with Meridian's security and business continuity requirements, including breach notification and remediation clauses.

6.6 You must commit to continuous improvement in managing supply chain cyber risks and adapt to evolving security threats and regulatory changes.

6.7 In the event of a security incident within your supply chain that may impact Meridian, you must promptly report the incident to Meridian in accordance with 4.10 of this policy and provide necessary assistance by working collaboratively in the response and mitigation efforts.

6.8 Meridian reserves the right to monitor your performance in managing supply chain risks associated with your subcontractors and third-party services and may request performance reports and improvement plans as deemed necessary.

7 DEFINITIONS

Term	Definition
Agreement	The agreement between Meridian and you.
Good Industry Practice	Exercising that degree of skill, diligence, prudence and foresight which would reasonably be expected from a skilled, reasonable and experienced operator in the same or similar circumstances and aligned with recognised industry and standards.
Meridian Data	All data, information, and meta data (including Personal Information) in any form (whether written, electronic, or otherwise) owned, held, used or created by or for Meridian, including: a) all information and data related to Meridian's operations or Meridian's customers which is generated by you in connection with this Agreement or the performance of the Services; and b) all information, data or business knowledge which is provided or made available by Meridian to you, in each case, whether relating to Meridian's business, operations, facilities, customers, employees or otherwise.
Personal Information	Has the meaning given in applicable data protection laws including to the term 'personal information' in the Privacy Act 2020.
Meridian (and we, us and our)	Meridian Energy Limited and/or the Meridian group company that is a party to that Agreement.
Meridian Systems	The electronic information systems including hardware, equipment, software, peripherals and communications networks owned, controlled, operated or used by Meridian.
Risk	Means any reasonably foreseeable internal or external event or issue (whether relating to Personnel, process, cost, technology, laws or otherwise) that is likely to or could adversely affect the delivery, timing or performance of the Services or the reputation of Meridian.
Security Incident	Any actual or suspected unauthorised or accidental access to, or disclosure, alteration, loss, or destruction of Personal Information which is Meridian Data, and includes any action that prevents Meridian from accessing Personal Information which is Meridian Data on either a temporary or permanent basis;
Services	The services to be provided by you to Meridian under the Agreement.
Security Controls	Also known as a security measure or safeguard, is the technical, organisational, physical and personnel controls relevant to the security, availability, processing integrity, confidentiality, safety, and privacy of the Services and Meridian Data (as applicable) and any other security controls or requirements agreed between the parties from time to time
Malicious Code	Any virus, bomb, Trojan horse or other malicious software or computer programming code that could impair, deny or otherwise adversely affect the Services, you, us or any Meridian Data or Meridian Systems.
Security Vulnerability	A weakness at the network, operating system, database or application software level, or within associated functions (such as a physical vulnerability at the location where Meridian Data is stored), or a weakness in an information security control that could allow a security incident to occur.
Subcontractor	Means a subcontractor of Supplier appointed to perform any of Supplier's obligations under agreement.