Information Security Policy

Approved date	13 December 2023

1. POLICY STATEMENT

Meridian Energy Limited (Meridian) highly depends on information and information systems to achieve its mission. This dependency means that information assets must be protected to maintain a competitive advantage and protect the interests of our employees, customers, and other stakeholders.

Meridian adopts a pragmatic, risk-based approach to managing information security risks while leveraging opportunities. We are all individually and collectively responsible for the security of our information assets and services. Accordingly, it is mandatory that all staff read, understand, and comply with this information security policy and all supporting policies, standards, and guidelines.

Meridian Board of Directors and Executive Leadership Team fully endorses this policy, and will provide resources and support, to ensure compliance across the business. The Board of Directors and Executive Leadership Team expects the same level of commitment from all staff, contractors, and third parties acting on behalf of or for Meridian.

2. PURPOSE OF THIS POLICY

This policy aims to ensure that Meridian's information assets are protected from unauthorised access, use, disclosure, disruption, modification, or destruction. It establishes our security governance framework, defines key security roles and responsibilities, and clearly sets out our intent to safeguard our information assets and systems from unauthorised actions that affect their confidentiality, integrity or availability.

3. SCOPE AND FIT

This policy applies to all of Meridian's business units, staff, contractors, and third parties acting on behalf of or for Meridian.

Compliance with this policy will ensure that information security risk management is integral to business activities, operational risk management, and employee behaviour.

Information security risk management commonly interchanges the terms assets, information, or business assets. In this policy, an information asset is defined as the data, related processes, systems (physical or virtual) or services for achieving Meridian's business objectives.

4. INFORMATION SECURITY MANAGEMENT

Meridian's Security Management structure is designed to safeguard its information assets, including those of customers, investors, and employees against unauthorised activities and various threats while avoiding undue risk or obstruction to business advancement. Inadequate security measures pose significant risks to safety, operations, reputation, and competitive standing, highlighting the need for a well-balanced protective strategy.

4.1 An Information Security Policy (this document) and related standards must be developed and maintained to manage the risk of security threats to Meridian's Information Services.

4.2 An information security governance board (ISGB) with representation across all business units must be established and maintained to manage Meridian's security posture and take informed decisions when leveraging business opportunities.

4.3 Any exemptions to this information security policy must be reviewed and approved by the ISGB as per the process outlined in section 13.

5. ICT RISK MANAGEMENT

Meridian operates an active programme to ensure ongoing risk management across the business. Information security risk management is applicable to all business units at Meridian and should be consistent with the Risk Management Policy. To achieve Meridian's information security objectives, business units must apply security measures and/or mitigating controls to manage risks to an acceptable level.

5.1 Staff, contractors, and third parties acting on behalf of or for Meridian have a responsibility to manage information security risk in accordance with the Risk Management Policy and framework.

5.2 As per Meridian's Risk Management Policy, General Managers (GMs) are the risk owners of their business unit's information security risks. All risk owners and/or delegate of authority must ensure endeavours are made to identify, monitor, treat, and formally report on their business unit's information security risks.

5.3 An appropriate level of security risk assessment must be performed for all new and existing information services used by Meridian that handle sensitive and/or business critical information. The risk assessment should be regularly maintained or when major changes to the services occur. New services (in-house or cloud) must be assessed prior to their use to store, transmit or process business information.

5.4 Risk owners are accountable for ensuring that all information security risk assessments and security assurance processes are documented and available for internal and/or external audit and review when required (for example, using Meridian's enterprise risk management tool).

5.5 Risk owners are responsible for ensuring all information security measures and/or mitigating controls are in place within their business units.

6. SECURITY AWARENESS & CULTURE

Meridian's people are considered our strongest defence. Information security is a shared responsibility regardless of your role and level. Secure information practices are essential to protecting our people, information assets, reputation, and future development.

6.1 All Meridian people must act in accordance with acceptable use of ICT resources as outlined in the code of conduct.

6.2 Meridian must have a formal information security awareness programme that supports in upskilling and educating people on safe and secure business practices.

6.3 All Meridian people must participate in information security awareness programmes with the support of their people managers.

6.4 Meridian must implement processes to ensure all staff, contractors, and third parties acting on behalf of or for Meridian:

A. Are appropriately screened in accordance with the People Policy or Master Service Agreement (MSA) before beginning employment or a contract of work, and on a regular basis thereafter;
B. Are suitably trained and have the relevant experience and/or certifications;
C. Are monitored for security and/or privacy implications related to changes in behaviour (and changes in circumstances), business practices, and/or process change;
D. When contractual obligations end with Meridian a person's access rights should cease immediately.

7. SECURE ICT ASSET MANAGEMENT

Meridian's information assets (data, personnel, devices, systems (physical or virtual), services, and facilities) are essential in achieving our business purposes and objectives. Therefore, these assets must be identified and managed consistent with their relative importance.

7.1 All information assets must be identified, accounted for, and registered in a central asset or configuration management system. The register must contain details of the risk owner accountable for the service, the type of information that is stored, processed, and/or transmitted, as well as any other systems the asset or technology supports. Assets must also be traceable to either physical or logical locations.

7.2 All services (in-house or cloud) must have a formally assigned risk owner who is accountable for the service.

7.3 All technology and information assets must be proactively monitored and maintained to protect Meridian's information throughout its life cycle in accordance with business needs.

7.4 All technology and significant information assets must have threats, mitigating controls, and security measures identified and documented in line with Meridian’s Risk Management Policy.

7.5 All technologies and information assets that have reached their end of life must be appropriately decommissioned in line with Meridian’s E-Waste ICT guidelines.

8. INFORMATION MANAGEMENT

Information should be classified and labelled throughout its life cycle by its owners and according to the security protection needed to ensure it is protected appropriately.

8.1 Meridian must classify the sensitivity of our data stored within Information Services so as to protect its confidentiality, integrity, and availability.

8.2 Using a risk-based approach, protective security controls must be developed and maintained to protect data based on its sensitivity.

9. IDENTITY AND ACCESS MANAGEMENT

Meridian depends on information and physical assets to deliver its business objectives. Implementing and managing secure identity and access controls to these resources is essential in protecting all Meridian information and technology confidentiality, integrity, availability, and personnel safety.

9.1 All technologies, information assets, and devices used to access Meridian data must be protected with access controls in accordance with Meridian standards or in the absence of these industry or vendor best practices.

9.2 All Meridian people must be aware of and act on their responsibilities for using and maintaining effective access controls as outlined in the code of conduct (e.g., Multi-Factor Authentication (MFA), strong passphrases, and keeping access control information confidential). People must not act in any way to circumvent these controls without applying for a formal exception.

9.3 All Meridian people managers are responsible for ensuring access privileges are clearly defined based on a person's assigned role and demonstrated need for access.

9.4 Access to Information Services must be reviewed when an employee or contractor changes roles or their existing role is modified.

9.5 Access rights to Information Services must be revoked upon the last date of work or as contractually agreed for employees and contractors. This right also extends to the removal of access in the event of a security investigation.

10. OPERATIONAL SECURITY MANAGEMENT

Protecting Meridian's information assets from unauthorised access is essential to maintaining effective, efficient, and safe business operations. Software configuration on operational systems should be hardened and controlled, and networks should be secured.

10.1 Risk owners must ensure that security procedures are implemented to verify the integrity of operational software and firmware and to control the installation of the verified software and firmware on operational systems.

10.2 Operating Systems, configurations, and applications must be hardened as per the relevant Meridian standard. If a Meridian standard is unavailable, the relevant CIS Security Benchmark, Open Web Application Security Project (OWASP), and/or vendor-supplied hardening guidelines must be followed and documented.

10.3 Network Controls must be implemented such that access to information systems is restricted to authorised use only. Information Services and users must be segregated appropriately on the network based on risk assessment or Service Owner requirements.

11. SECURITY INCIDENT MANAGEMENT

Maintaining the capabilities to detect and quickly respond to information security incidents helps prevent further damage to Meridian and reduces adverse financial, reputational, and operational impact. Therefore, Meridian must effectively manage security incidents and the associated risks.

11.1 Risk owners are responsible for ensuring controls are in place to detect, prevent, and recover from security incidents and events. People must not act in any way to circumvent these controls.

11.2 Meridian must have a formal security incident management capability that enables each business unit to manage security incidents and associated risks that could lead to adverse outcomes on privacy, confidentiality, integrity, and availability of its information and services.

11.3 All people using Meridian's information services must report any observed or suspected information security incidents through the defined support channels as quickly as possible in accordance with Meridian's Information Security Incident Management process.

11.4 Knowledge gained from analysing and resolving information security incidents must be documented and used to reduce the likelihood or impact of future incidents.

12. SECURE SOLUTION DEVELOPMENT

Establishing and maintaining information security across the entire lifecycle of ICT and Operational Technology (OT) systems is essential to security risk management and assurance. Therefore, all Meridian security requirements, legal, and regulatory compliance obligations must be met during the acquisition, development, and maintenance of information assets.

12.1 The establishment of all information assets, services, and technologies must be done securely in accordance with Meridian's policies, standards and guidelines. All people must ensure they do not introduce security risks through inappropriate procurement or design practices.

12.2 All information assets, services, and technologies should be installed secure by design and by default.

12.3 Risk owners and/or a stated delegate of authority are responsible for ensuring that all information assets and services comply with Meridian's regulatory and legal obligations.

12.4 Employees must fulfil ICT security requirements in the planning, acquisition, development, and/or update of information assets. Any changes to systems during its life cycle must be managed and controlled through Meridian's formal change control process.

12.5 Production data used for testing purposes must be protected and controlled in accordance with Meridian policy and best practices.

12.6 The resiliency of all new information assets and services must be formally assessed and understood to align with Meridian's business strategy and support crisis management, business continuity, disaster recovery (DR) plans and processes, as well as service exit.

13. POLICY EXCEPTIONS

13.1 All Meridian data, information assets, services, staff, contractors, and third parties acting on behalf of or for Meridian must comply with this policy, unless granted an exception. All exceptions must be:

A. granted by the ISGB after acknowledging and documenting the associated risks identified by the information security team
B. time bound to the required exception period stated in the request for exception
C. associated with a clear business justification approved by the Risk Owner
D. considerate of Meridian's risk management policy and appetite
E. recorded in the policy exceptions register maintained by the information security team
F. reviewed regularly.

14. DEFINITIONS

Term	Definition
Availability	Ensuring that authorised users have access to information and associated assets when required.
Confidentiality	Ensuring that information is accessible only to those authorised to have access.
Information and Communications Technology	An umbrella term that includes any communication device, encompassing radio, television, cell phones, computer and network hardware, satellite systems and so on, as well as the various services and appliances with them such as video conferencing and distance learning.
Information Asset	The data, and related processes, services, systems (physical and virtual) and networks for achieving business objectives.
Information Security	The protection of information assets from unauthorised access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
Integrity	Safeguarding the accuracy and completeness of information and processing methods.
Multi-Factor Authentication	An authentication method where a user is only allowed to log on after successfully presenting two or more pieces of evidence (or factors) to the authentication mechanism.
Operational Technology	Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment).
Risk	The likelihood and consequence of a potential loss, disaster or other undesirable event.
Risk Owner	All risks have a designated owner and all treatments have designated owners. All enterprise level risks are owned by a general manager or, where the risk is extreme, by the CEO. Where services are outsourced, treatment actions can be undertaken by the supplier but exposure to the risk remains with Meridian and must be managed as such.

15. POLICY INFORMATION TABLE

Name	Information Security Policy
Description	This policy establishes our security governance framework, defines key security roles and responsibilities, and clearly sets out our intent to safeguard our information assets and systems from unauthorised actions that affect their confidentiality, integrity or availability.
Type	Policy
Owner	Chief Information Officer
Approval	Audit and Risk Committee on Behalf of the Board
Last Approval Date	12 December 2023
Review Frequency	Annually
Next Review Date	12 December 2024
Applies To	Meridian Energy NZ
Linked Policies, Standards, Guidelines, Processes or Procedures	Information Classification & Protection Policy Cyber Security Policy for Third Parties Cyber Security Standard
SharePoint Reference	Resource Hub – Policies, Procedures and Guidelines - Policies