Infratil's Information Security, Cyber Risk & Responsible AI Policy

Overview

Infratil does not operate standalone information technology systems, infrastructure, or internal technology workforce. Therefore, information technology platforms, systems, and cyber security capabilities supporting Infratil are provided, managed, and governed by its Manager, Morrison, under a managed operating model.

Accordingly, as at the date of this policy, information security, cyber risk management, and responsible use of artificial intelligence (AI) for Infratil are governed through Morrison's enterprise-wide frameworks, policies, and control environment, as described below.

Each portfolio company is independently responsible for managing risks within its own operations.

1. Information Security and Cyber Risk

1.1 Governance and Oversight

Oversight of information security and cyber risk is embedded within Morrison's enterprise risk management framework and Information Security Management System (ISMS).

Governance is exercised through established forums, including:

- Operations, Risk and Compliance Committee
- Audit, Risk and Compliance Committee
- Escalation to senior leadership and Board as required

These forums oversee:

- Risk exposure and control effectiveness
- Information security incidents and responses
- Audit findings and remediation activities

1.2 Information Security Framework

Information security is managed through Morrison's Information Security Management System (ISMS), aligned with internationally recognised standards including ISO/IEC 27001 good practice.

This framework:

- Applies a risk-based approach to managing threats
- Protects confidentiality, integrity and availability of information
- Supports compliance with legal, regulatory, and contractual obligations across jurisdictions

1.3 Policy Framework and Controls

Infratil's information security environment is governed through Morrison policies and supporting controls, including:

- Information Security Policy
- Acceptable Use Policy
- Data protection and privacy controls
- Supplier and third-party security requirements
- Incident management and business continuity processes

These controls:

- Establish minimum security standards
- Define responsibilities across all personnel
- Promote consistent and secure handling of information assets

1.4 Roles, Responsibilities and Culture

Morrison maintains defined roles and responsibilities for information security, including executive accountability through the Head of Information Technology (acting as Information Security Officer).

Information security is a shared responsibility across the organisation:

- All personnel are to comply with security policies
- Potential incidents are to be reported promptly
- Regular training supports awareness and secure behaviours

1.5 Incident Management and Resilience

Information security incidents are managed through formal processes that include:

- Identification and reporting of incidents
- Escalation and investigation
- Remediation and continuous improvement

Morrison maintains:

- Business continuity and disaster recovery plans
- Periodic testing (including scenario and tabletop exercises)
- Operational resilience capabilities, including the ongoing identification, assessment and prioritisation of vulnerabilities across systems, applications and infrastructure, supported by periodic internal and independent testing, and remediation activities aligned to its risk management framework

1.6 Third-Party Risk and Assurance

Information and cyber security risks associated with third-party service providers and technology vendors are managed through Morrison's third-party policy, risk management and due diligence processes. These include, as appropriate, security assessments prior to engagement, contractual requirements relating to confidentiality and information security, and ongoing monitoring of critical suppliers.

For material service providers, Morrison reviews business continuity arrangements, recovery objectives and information security controls, and undertakes periodic audits and assurance activities, including internal audits, technical reviews and process reviews, to support the effectiveness and continual improvement of the ISMS.

Morrison maintains a programme of internal audit, assurance and periodic independent testing activities, including external audit reviews and third-party assessments where appropriate, to support the effectiveness and continuous improvement of its information security and risk management frameworks.

2. Responsible Use of Artificial Intelligence

The use of artificial intelligence (AI) in relation to Infratil is governed through the enterprise policies, frameworks and control environment of Morrison in its capacity as Manager.

Morrison maintains an AI governance framework designed to support the responsible, secure and ethical use of AI technologies across its operations. The AI Governance Group oversees the use of AI at Morrison.

Morrison is a participant in the Sustainable Digitalisation Project (SDP), a collaborative initiative aimed at embedding responsible, ethical, and sustainable digital practices across the built environment, including the evolution of governance approaches relevant to information security and responsible AI.

2.1 Governance and Principles

Morrison's AI Use Policy establishes principles and governance requirements for the adoption and use of AI tools.

These include:

- Privacy and data protection – AI use is to be consistent with the protection and appropriate use of personal, confidential and commercially sensitive information
- Cybersecurity and system integrity – AI tools are assessed and used in a manner that protects internal systems and data
- Fairness and bias mitigation – reasonable steps are taken to identify, reduce and manage potential bias and discriminatory outcomes
- Human oversight and control – AI does not replace human judgement or oversight, particularly in material or high-risk decisions
- Transparency and explainability – appropriate visibility over the use of AI and the provenance of outputs is maintained
- Accountability – clear responsibility for decisions and outcomes supported by AI tools is maintained
- Defined boundaries of use –guidance and boundaries are established on inappropriate or high-risk uses of AI tools

2.2 Risk Management and Controls

The use of AI tools is subject to formal governance and risk management processes, including:

- Pre-use due diligence and assessment of AI tools and providers
- Maintenance of an approved tools register
- Ongoing monitoring, periodic review and lifecycle management of AI tools
- Defined controls over the types of data that may be used in AI tools
- Alignment with applicable legal, regulatory and contractual obligations

Where appropriate, controls limit or prohibit the use of AI in high-risk scenarios or where adequate safeguards are not in place.

2.3 Security, Privacy and Incident Management

The use of AI is integrated into Morrison's broader information security and risk management frameworks.

This includes:

- Restricting use of sensitive, personal or confidential information to assessed enterprise AI tools
- Using established mechanisms for reporting, escalating and managing AI-related incidents including concerns on accuracy, appropriateness and potential bias
- Integrating the AI framework with existing information security incident management processes including to report inappropriate AI use, material errors, or adverse outcomes

AI-related risks are managed consistently with Morrison's overall information security and operational risk frameworks.

2.4 Training and Responsible Use

Under the Policy, personnel are to:

- Use only approved AI tools for business purposes
- Review and, where appropriate, validate outputs before use
- Use AI tools in a lawful, ethical and responsible manner
- Comply with Morrison policies, including information security, privacy and conduct requirements

Training and awareness activities are designed to promote safe and effective use of AI technologies across the organisation.

3. Approval, Governance and Review

This policy is approved by the Infratil Board. This policy is reviewed and approved as required for regulatory developments but is scheduled to be reviewed every two years.