Entered by Board Secretary

AGENDA ITEM 19.2 | BOARD DECISION PAPER	
To:	The Board
From:	Ryan Marshall
Reviewed:	Kerry Bakkerus, Head of Risk & Assurance Mark Laing, Chief Financial Officer and Director Corporate Services Dean Kimpton, Chief Executive
Date:	9 December 2025
Title:	**Tier 1 Policies**

Aronga / Purpose

1. To seek approval of certain Tier 1 policies.

Tuku mana / Delegation

2. Tier 1 policies require approval for any updates and reclassifications.

Ngā tūtohunga / Recommendations

That the Auckland Transport Board (board):

a) Approve the Procurement Policy.

b) Approve the Asset Management Policy.

c) Approve the Information Security Policy.

d) Note management’s decision not to update the:

i. Sustainability Policy.

ii. Revenue Generating Policy.

Te whakarāpopototanga matua / Executive summary

3. The Procurement and Information Security policies have been updated as part of Auckland Transport’s (AT’s) policy review cycle.

4. The Asset Management Policy has been updated to include intangible and other assets, which was requested at the Finance and Assurance Committee (committee) meeting on 6 May 2025.

Ngā tuhinga ō mua / Previous deliberations

Date	Report Title	Key Outcomes
6 May 2025 (committee)	Tier 1 Policies	The committee endorsed the Asset Management Policy for approval by the board, and requested that management update the policy to reflect intangible assets.
24 June 2025 (board)	Tier 1 Policies	The board approved the Asset Management Policy.
18 November 2025 (committee)	Tier 1 Policies	The committee endorsed and recommended that the board approves the Procurement Policy, Asset Management Policy and Information Security Policy.

Te horopaki / Background

5. AT regularly reviews and updates its policies to ensure that they are fit-for-purpose, reflect leading practice, address key risk areas in the organisation and align to Auckland Council’s (council’s) direction.

6. Policies that are strategic in nature, have reputational impact or provide direction on areas of significant risk have been classified as Tier 1 policies. Tier 1 policies are approved by the board.

7. Policies that provide direction on operational matters that impact the entire organisation have been classified as Tier 2 policies and are approved by the Chief Executive.

Te hononga ki te "Statement of Intent 2025-2028"/ Alignment to Statement of Intent 2025–2028

8. While AT's policies do not align to specific principles in the Statement of Intent, they help to address strategic and operational risks across the organisation and provide guidance on what, why and how we do our work. This enables the business to carry out its activities which align to the Statement of Intent.

Me mōhio koe / What you need to know

Procurement Policy

9. The Procurement Policy has had a significant rewrite that aligns to our refreshed policy style. We have included a copy of the policy as Attachment1.

10. The policy has been updated to provide more detail on AT's six key procurement principles. These six principles are the same as the Government's procurement principles (which were updated in October 2025) and are also adhered to by New Zealand Transport Agency Waka Kotahi and council.

11. The policy also outlines AT's broader approach to procurement and details AT's expectations around its Plan, Source and Manage approach, while also outlining the importance of our Spend Category Strategy and Supplier Relationship Management.

12. A new section has been added relating to assurance and quality control in procurement (see "*How does AT ensure its procurement approach is fair to suppliers?*" in the policy), and definitions and roles and responsibilities have been refreshed.

Asset Management Policy

13. The Asset Management Policy has been updated to reflect that both intangible and other assets are also covered by the Policy.

14. We have included the updated policy as Attachment 3. Changes from the Asset Management Policy that were approved by the board in June 2025 have been highlighted.

Information Security Policy

15. The Information Security Policy has been re-written to better align with AT's updated policy style.

16. While the core policy principles and the areas of information security that have been referred to remain the same, the wording and language used throughout the policy has been updated to make the principles easier to understand, expectations clarified, and roles and responsibilities more clearly understood.

17. We have also compared our Information Security Policy with council's Information Security Policy. While the approaches taken by AT and council differ, the principles and objectives outlined in the respective policy documents are largely aligned.

18. We have included a copy of the updated Information Security Policy as Attachment 4.

Sustainability Policy and Revenue Generating Advertising Policy

19. Given the proposed legislative changes arising from the Transport Reform, AT proposes to defer updating the Sustainability and the Revenue Generating Advertising Policy until there is greater clarity on the need for the policies, accountability and council's position or expectations with respect to them.

Ngā ritenga-ā-pūtea me ngā rauemi / Financial and resource impacts

20. N/A.

Ka whaiwhakaaro ki te Tiakanga Taiao / Climate change and sustainability considerations

21. N/A.

Ngā whakaaweawe atu anō / Other impacts

Relationship	Consulted Y/N	Views and Perspectives Received
Māori	Yes: ☐ No: ☒	N/A
Elected members	Yes: ☐ No: ☒	N/A
Council Controlled Organisations	Yes: ☐ No: ☒	N/A

Ā muri ake nei / Next steps

22. If approved by the board, we will publish the final versions of all three policies on AT’s intranet and notify AT staff of the changes to the policies in internal communications.

Ngā whakapiringa / Attachments

Attachment #	Description
1.	Procurement Policy **[Available through Resource Centre]**
2.	Contract Lifecycle Framework **[Available through Resource Centre]**
3.	Asset Management Policy **[Available through Resource Centre]**
4.	Information Security Policy **[Available through Resource Centre]**

Te pou whenua tuhinga / Document ownership

Submitted by	Recommended by	Approved for submission
Ryan Marshall **Compliance Manager**	Kerry Bakkerus **Head of Risk & Assurance**	Dean Kimpton **Chief Executive**

Procurement Policy

1. What is this policy about?

1.1 The purpose of this policy is to ensure that a robust and consistent procurement practice is applied across all Auckland Transport (AT) procurement activities. This policy provides a set of guidelines and rules to achieve specific procurement goals and ensure consistent decision making. It supports Auckland Transport's (AT's) Procurement Strategy that provides the overall direction and plans that outline how we will reach our procurement objectives.

1.2 AT is a significant procurer in value, scale and complexity, and is ultimately accountable to the ratepayers of Auckland and taxpayers of New Zealand, through its funding arrangements with Auckland Council (AC) and New Zealand Transport Agency Waka Kotahi (NZTA).

1.3 Effective procurement helps us deliver better outcomes and less cost of doing business for all involved. Effective procurement can improve productivity and support supplier innovation.

1.4 The purpose of this policy is to:

- Explain our approach to procuring assets, services and goods at AT;
- Ensure a robust and consistent procurement practice is applied across all AT procurement activities, while effectively managing risk and complying with the rules set by our funders partner NZTA, in alignment with the New Zealand Government Procurement (NZGP) rules and Auckland Council Group Procurement Policy;
- Commit to delivering a transparent and fair procurement process that ensures value for money for all stakeholders.

2. Who does it apply to?

2.1 This policy applies to all AT employees - permanent and temporary - and to all procurements carried out by or on behalf of AT. It also applies to representatives (such as contractors, secondees, agency temps, interns, and graduate trainees), as well as to the AT Board.

2.2 Where this policy uses pronouns like "you", "your", "we", or "us", it is referring to anyone who this policy applies to.

3. What principles do I need to follow?

3.1 Our key principles related to procurement are outlined below:

Plan and manage for great results

Be proportionate and right-size the procurement

Be fair to all suppliers

Get the right supplier

Get the best deal for everyone

Play by the rules

Our six key principles should be applied consistently across all phases of the procurement lifecycle to ensure effective and responsible procurement:

Plan and manage for great results

- Identify what you need and then plan how to get it.
- Set up a team with the right mix of skills and experience.
- Involve suppliers early - let them know what you want and keep talking.
- Take the time to understand the market and your effect on it. Be open to new ideas and solutions.
- Encourage e-business.

Be proportionate and right-size the procurement

- Make it easy to do business with Auckland Transport.
- Design and run an efficient end-to-end process that is proportional to the value, complexity and risk.
- Reduce the time, cost and complexity for suppliers participating in procurement processes.
- Make documentation and communication clear and concise to minimise impacts on resources and only ask for information from suppliers that is essential and relevant.

Be fair to all suppliers

- Create competition and encourage capable suppliers to respond.
- Treat all suppliers equally – we don't discriminate (this is part of our international obligations).
- Seek opportunities to involve Auckland businesses including diverse suppliers.
- Be open to subcontracting opportunities in big projects.
- Clearly explain how you will assess proposals – so suppliers know what to focus on.
- Talk to unsuccessful suppliers so they can learn and know how to improve next time.

Get the right supplier

- Be clear about what you need and fair in how you assess suppliers – don't string suppliers along.
- Choose the right supplier who can deliver what you need, at a fair price and on time.
- Choose suppliers that comply with the AT Supplier Code of Conduct.
- Build demanding, but fair and productive, relationships with suppliers.
- Make it worthwhile for suppliers – encourage and reward them to deliver great results.
- Identify relevant risks and get the right person to manage them.

Get the best deal for everyone

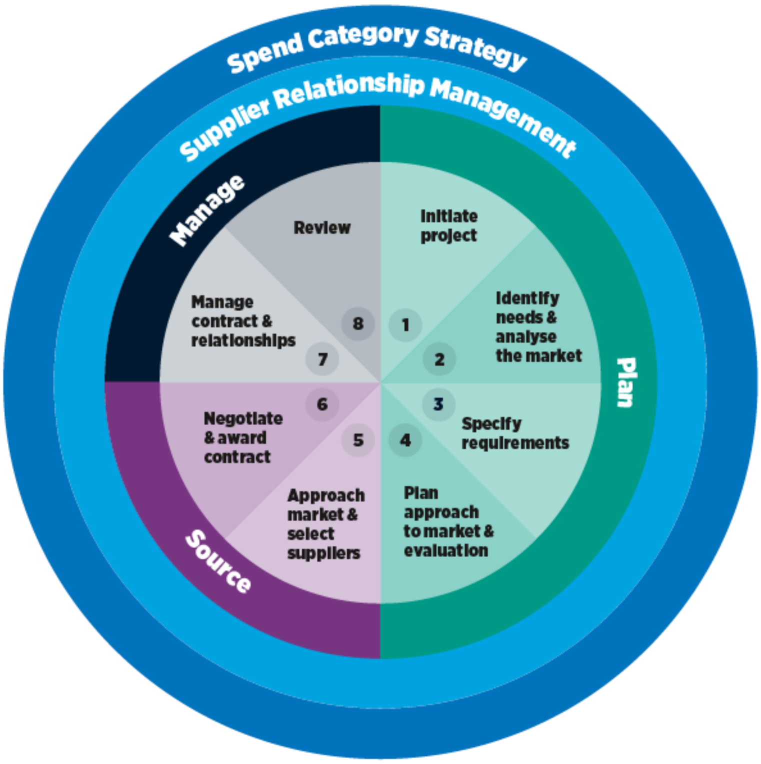
- Get best public value – account for all costs and benefits over the lifetime of the goods or services.
- Make balanced decisions – consider the possible economic benefits to Auckland.
- Encourage and be receptive to new ideas and ways of doing things – don't be too prescriptive.
- Take calculated risks and reward new ideas.
- Have clear performance measures – monitor and manage to make sure you get great results.
- Work together with suppliers to make ongoing savings and improvements.
- It's more than just agreeing the deal – be accountable for the results.

Play by the rules

- Be accountable, transparent and reasonable.
- Make sure everyone involved in the process acts responsibly, lawfully and with integrity.
- Stay impartial – identify and manage conflicts of interest.
- Protect suppliers' commercially sensitive information and intellectual property.

4. What is our approach and the procurement lifecycle?

4.1 AT's procurement approach is summarised in the model below. It ensures that all aspects of the procurement lifecycle are appropriately managed, from spend category strategy and supplier relationship management, through to the planning, sourcing and management of individual procurement needs.


Spend Category Strategy
Supplier Relationship Management
Plan
Source
Manage
1 Initiate project
2 Identify needs & analyse the market
3 Specify requirements
4 Plan approach to market & evaluation
5 Approach market & select suppliers
6 Negotiate & award contract
7 Manage contract & relationships
8 Review

AT's Procurement Lifecycle

Spend Category Strategy

4.2 A Spend Category Strategy is a structured approach to managing procurement by grouping similar goods or services into categories and developing tailored procurement strategies for each. This helps organisations optimise value, reduce costs, and improve supplier relationships by aligning purchasing decisions with market dynamics and business needs.

4.3 AT's Spend Category Strategies align expenditures with business requirements and risk mitigation. Category Plans will link to broader business strategies, directing procurement requirements, supplier relationship arrangements, appropriate resource allocation, measures and the reporting requirements throughout the Plan, Source and Manage phases.

Supplier Relationship Management (SRM)

4.4 Supplier Relationship Management (SRM) focuses on building strong, collaborative partnerships with key suppliers to improve performance, reduce risk, and create long-term value for both parties.

4.5 SRM is essential for fostering strong, mutually beneficial relationships with suppliers who have the capability to provide and maintain strategic value for stakeholders. Through the development of an SRM framework, AT aims to cultivate strong relationships with suppliers built on trust, open communication, and shared success.

Plan, Source and Manage

4.6 The content below highlights key considerations across the steps in the procurement lifecycle phases: Plan, Source, and Manage. Following these helps to ensure that the principles in this policy are applied consistently to all procurements.

Plan	**1. Initiate project**	Align with strategic and compliance requirements, including the AT Māori Outcomes Plan, property, resource consents, and health and safety. Establish project team, set up accountability and governance measures and engage with key stakeholders.
	2. Identify needs & analyse the market	Assess community impact and engage early with suppliers to understand market capabilities and potential innovations. Analyse the market and maintain awareness to support value for money outcomes and long-term supplier relationships.
	3. Specify requirements	Clearly define requirements considering the total cost of ownership, expected outcomes, and sustainability goals and describe how to achieve best value for money. Ensure the approach reflects the project's scope and identifies any subcontracting or SME involvement opportunities.
	4. Plan approach to market & evaluation	Select a procurement model proportionate to the project's size, complexity, and risk. For emergency procurement, see the Definitions section of this document and follow the procurement guidelines. Develop and document a clear evaluation methodology and prepare to engage suppliers transparently and fairly.

Source	**5. Approach market & select suppliers**	Apply suitable delivery models and supplier selection methods, considering existing government or Council Group contracts where appropriate. Ensure fair and competitive processes, giving all suppliers equal opportunity and conduct a detailed evaluation of financial, social, and environmental costs across the full lifecycle of goods, services, or works.
	6. Negotiate & award contract	Use approved procurement templates, negotiate fair pricing and contract terms, and establish clear deliverables. Ensure regulatory compliance by securing purchase orders before commencement.

Manage	**7. Manage contract & relationships**	Apply a standardised contract management approach (using the **Contract Lifecycle Framework**) to streamline processes, minimise risks, and ensure strong governance, support compliance & risk mitigation by aligning contracts with business needs and clarifying staff responsibilities. Establish performance measures to monitor compliance and ensure suppliers meet expectations. Foster collaborative relationships by recognising supplier contribution and working together on continuous improvement.
	8. Review	Conduct value and benefit tracking to assess contract performance and supplier impact. Use review insights to inform future procurement decisions and strengthen sustainable supplier relationships.

How we procure at AT?

4.7 AT procures a variety of goods, services and assets. How we procure them varies, depending on the value, complexity and risk involved.

4.8 AT has sourcing standards, procedures and guidelines (AT Procurement Framework) that must be followed, which are available on the AT Procurement Hub. These support the application of the most appropriate approach for each procurement, promote fair and competitive processes wherever possible, and ensure we achieve the best Value for Money (VFM).

4.9 The purchase order cycle (ordering, obtaining and paying for the goods or services the business requires) is core part of the procurement lifecycle. Purchase Orders must be issued to the appointed vendor before any services commence, or goods are ordered. Failure to do this is a breach of this policy and will likely result in delayed payment to the vendor. Prompt payment is a fundamental commitment to the way we procure at AT and is consistent with guidance we have on the Engine Room here: Purchase Order (PO).

4.10 The Auckland Transport Delegations Register sets out principles and thresholds for the exercise of all delegations (financial & non-financial) by AT employees.

4.11 AT's practices and decisions must be able to withstand public scrutiny at all times. Throughout all phases of the procurement lifecycle (Plan / Source / Manage), AT should:

- Clearly record our planning, processes and decisions so they can be easily understood and audited;
- Document and effectively manage conflicts of interest;
- Identify risks and develop appropriate mitigation strategies to manage them;
- Act lawfully, ethically and responsibly.

4.12 Our AT Supplier Code of Conduct also sets out minimum expectations applicable to all suppliers and contractors providing goods and services to AT. We all have a role in AT to ensure suppliers adhere to these principles.

Where can I get more information on procurement?

Procurement Hub

4.13 AT is committed to smart buying that delivers sustainable value for money spent. The **Procurement Hub** has been developed as a key resource to effectively support all stakeholders throughout the procurement lifecycle and process.

4.14 The Procurement Portal provides essential guidance and outlines the mandatory rules we must adhere to. It should be consulted for every procurement to ensure compliance, access to the latest templates and forms, and ensuring adherence to best practices.

Procurement Business Partner (PBP)

4.15 **Procurement Business Partners** are available to support and assist with AT's procurement needs. Alternatively, the business can reach out to procurement@at.govt.nz or ask Presto, the online procurement 'chatbot'.

How does AT ensure its procurement approach is fair to suppliers?

4.16 The AT Procurement Team are committed to support and provide the best guidance aligned with the policy principles.

4.17 For procurements with more significant risks, additional oversight may be required, such as probity measures during procurement activities, to ensure fairness, integrity in procurement documents, processes, and arrangements, and transparency in outcomes and decisions.

4.18 For any procurement of significant risk and/or value, probity will provide the assurance as below:

- Ensure there is an independent or impartial Probity Auditor and/or Fairness Advisor;
- Undertake inquiries where procurement concerns are raised by stakeholders, suppliers and participants, summarise results and recommend remedies if appropriate;
- Maintain an independent hotline for staff, suppliers and the public to report issues or concerns with our procurement approach or processes;
- Provide escalation processes to fairly investigate concerns and make recommendations to address issues or concerns.

4.19 AT has a zero tolerance for fraud and encourages everyone to report any complaints, concerns and allegations. There are various ways to do this included in Section 7 Non-Compliance.

4.20 The Head of Risk & Assurance is also available to carry out an independent review and provide remedies if appropriate.

4.21 Make sure you keep the AT Procurement team involved and informed – they are there to support you and help ensure that the procurement approach taken is suitable for the type and risk of spend.

5. Definitions

Term	Definition
AT Procurement Framework	AT’s Procurement Framework includes the procurement strategy, policy, standards, procedures, guidelines and templates.
Contract Management	Contract management is the process that enables AT and suppliers to meet their obligations to deliver the objectives required from a contract, on time, to quality and specification and within budget.
Emergency Procurement	An emergency procurement may only be made when the existence of an emergency situation creates an immediate and serious need for goods/services/works that cannot be met through normal procurement methods. An 'emergency' is a sudden unforeseen event. It can result in injury, loss of life or critical damage to property or infrastructure. Emergency situations may include: • Natural or manmade disasters, failures of critical infrastructure or equipment; • Critical health or environmental emergencies; • Political emergencies; • Critical security emergencies; • Unanticipated events that make it impossible for AT to perform a statutory or critical function in the necessary timeframe.
Probity	Probity oversight during procurement activities ensures the fairness and integrity of documents, processes and arrangements, and the transparency of procurement outcomes and decisions.
Procurement	All aspects of planning, acquiring and delivering goods, services and works. Beginning with identifying the need and finishing with either the end of a service contract or the end of the useful life and disposal of an asset.
Procurement Thresholds	AT's standard procurement processes are based on monetary thresholds and risk. The thresholds are detailed in the Plan set of procedures and guided by AT’s DFA.
Value for Money (VFM)	Value for money means getting the best possible result from our procurement, using resources effectively, economically and without waste, and taking into account: • The total costs and benefits of a procurement (total cost of ownership), and; • Its contribution to the results AT is trying to achieve.

6. Roles and responsibilities

Role	Accountability & Responsibility
All employees and representatives	- Adherence and compliance with the Procurement Policy and related systems, standards, procedures, guidelines and templates.
AT Board (Policy approver)	- Approves the Procurement Policy. - Promote the principles of the Procurement Policy.
Chief Executive (Policy Endorser)	- Endorses the Procurement Policy. - Promotes the principles of the Procurement Policy.
CFO and Director Corporate Services (Policy Owner)	- Consult and seek approval of the Procurement Policy from the AT Board. - Accountable for the efficient and effective implementation and compliance of the Procurement Policy. - Ensuring accurate and reliable procurement performance information is provided to the Chief Executive (CE) and Executive Leadership Team (ELT). - Promoting the principles of the Procurement Policy. - Ensuring there are adequate and competent resources available for meeting procurement objectives and planned outcomes. - Managing foreseeable procurement risks and ensuring adequate controls are in place. - Approving or endorsing individual procurement strategies and plans, monitoring their results and outcomes, and providing direction when improvements are required.
Delegated Financial Authority (DFA)	- Appropriate AT employee who has relevant delegated financial authority to approve a procurement activity.
Executive Leadership Team (ELT)	- Promoting the principles of the Procurement Policy. - Adherence and compliance with the Procurement Policy and related strategy and systems within their respective Divisions.
Group Manager Procurement	- Develop, consult, and seek approval of the Procurement Policy and Procurement Strategy. - Responsible for the efficient and effective implementation, maintenance and compliance of the Procurement Policy and Procurement Strategy. - Develop and embed an accountability framework and monitoring key risk, controls and performance indicators, and providing direction when improvements are required. - Develop and implement an effective training and development programme to ensure sufficient resource capability and performance for procurement practitioners across the Procurement and business functions.

Role	Accountability & Responsibility
	- Adopting a cross-functional view, and resolving differences between business units when necessary, and providing procurement leadership and support to achieve the benefits sought by AT. - Governance oversight and accountability for quality control, Procurement Governance Framework, and service delivery. - Approving updates or variations to, standards, procedures and guidelines. - Reporting procurement performance and taking remedial action where deficiencies are identified. - Ensuring ongoing policy compliance with all applicable legislation and guidance, including the NZTA Procurement Manual and Auckland Council Group Procurement Policy. - Ensuring all AT Procurement team are aware of and follow the requirements of the Procurement Policy.
Procurement Team	- The procurement function comprises distinct roles, such as senior procurement specialists and procurement advisors, each with responsibilities defined in their job descriptions to support the organisation’s procurement objectives. Collectively, the procurement team is generally responsible for the activities outlined below; - Acquiring the competency to adequately undertake procurement responsibilities. - Providing specialist guidance and support, including strategic sourcing, facilitation of end-to-end procurement process. - Supporting contract development and management. - Owns and manages risks and controls and implements corrective actions to address process and control deficiencies. - Providing quality and compliance assurance with procurement business partners providing procurement service to the customers and the business, and management providing expertise and support, monitoring and challenge or risk-related matters. - Providing training to staff on good practice procurement. - Identifying and report on emerging procurement risks. - Providing periodic reporting on procurement process and initiatives. - Responsible for ensuring all public facing procurement documentation is fit for purpose, meets transparency, quality standards and probity requirements.
Probity Advisor	- Providing proactive advice during a process to help maintain fairness, transparency, and ethical compliance.
Probity Auditor	- Providing independent review after a process to confirm it was conducted according to ethical and legal standards.
Risk & Assurance	- Supports effective governance by identifying, assessing, and monitoring organisational risks while providing independent assurance that controls and processes are operating as intended.

7. Supporting information

Legislative compliance	This policy supports AT's compliance with the following legislation: • Commerce Act 1986 • Contract and Commercial Law Act 2017 • Electronic Transactions Act 2002 • Fair Trading Act 1986 • Health and Safety at Work Act 2015 • Land Transport Management Act 2003 • Local Authorities (Members' Interests) Act 1968 • Local Government Act 2002 • Local Government (Auckland Council) Act 2009 • Local Government Official Information and Meetings Act 1987 • Official Information Act 1982 • Public Records Act 2005
Supporting documents	• Auckland Transport Procurement Framework • Auckland Transport Supplier Code of Conduct • Auckland Transport Sustainability Strategy
Related documents	• Auckland Council Group Procurement Policy • Capital Project Management Policy • Climate Change Technical Policy • Code of Conduct Policy • Conflicts of Interest Policy • Contract Lifecycle Framework • Delegations Register • Expenditure Policy • Fraud Policy • Gifts and Hospitality Policy • Information and Records Management Policy • NZ Government Procurement (NZGP) Rules • NZ Transport Agency Waka Kotahi Procurement Manual • Office of the Auditor General: Procurement Guidance for Public Entities • Protected Disclosures Policy • Purchasing Card Policy • Safety, Health and Wellbeing Policy • Sustainable Procurement Action Plan

8. Non-Compliance

8.1 Non-compliance with this Policy may compromise AT's ability to achieve value for money or expose AT to financial and reputational risk. Failure to comply with this Policy is considered an act of misconduct and may lead to disciplinary action taken against employees, up to and including dismissal, or the termination of a representative's agreement with AT.

8.2 AT encourages anyone to raise any non-compliance or probity concerns relating to this policy. To enable this, AT:

- Encourages the use of AT’s internal Speak Up Hub to find more information about areas of concern and how to raise concerns;
- Maintains an independent hotline for staff, suppliers and the public to report issues or concerns with our procurement processes (0800 AT REPORT / at.report@pwc.com).

9. Approval & review

Policy Owner:

CFO and Director Corporate Services

Policy Contact:

Group Manager Procurement

Endorsed by:

Chief Executive

Approved by:

AT Board Chair

Approval date: dd/mm/yyyy

Next Review date: dd/mm/yyyy

Effective date: dd/mm/yyyy

AT reserves the right to review, amend or add to this policy at any time upon reasonable notice to employees and representatives.

Auckland Transport Contract Lifecycle Framework (CLF)

December 2023

Change History and Approval

Approval indicates an understanding of the purpose and content described in this document. By signing this document everyone agrees work should be initiated on this project and necessary resources should be committed as described herein.

PREPARED BY:	REVIEWED BY:	ENDORSED BY:	APPROVED BY:
DocuSigned by: Tereza Smazik 6A3039613A0444D...	DocuSigned by: Jonathan Day 9CDADDD5A9C4484...	Endorsed on the day noted below	DocuSigned by: E3DBEB75726C4D8...
Tereza Smazik	Jonathan Day	Various	Andy Richards
SENIOR PROCUREMENT SPECIALIST (EXCELLENCE)	PROCUREMENT MANAGER (EXCELLENCE)	PROCUREMENT STEERING COMMITTEE	GROUP MANAGER PROCUREMENT PROJECT SPONSOR
DATE:	DATE:	DATE:	DATE:
19 December 2023	19 December 2023	29th November 2023	19 December 2023

Revision	Revision Date	Details
6	18/12/2023	Final Draft

Contents

Tables

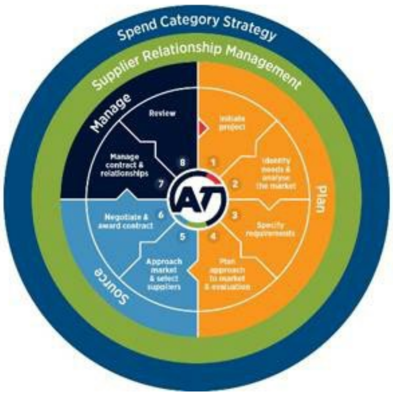
1 Introduction

Contract management is a critical component of managing delivery and associated risks in the contract lifecycle. Contracts need to be fair and provide Auckland Transport (AT) and Auckland ratepayers with value-for-money while reducing costs and managing risk.

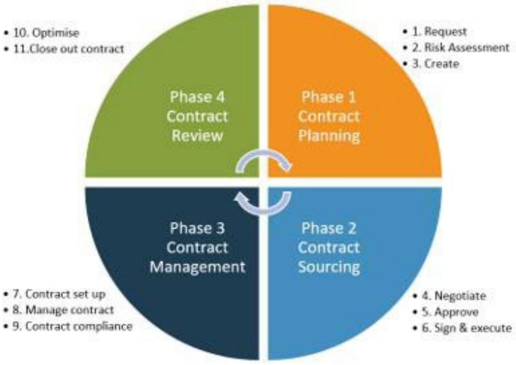
The Framework refers to a set of steps and activities that are required to responsibly manage our contracts in the entire contract lifecycle.

To improve the contract lifecycle, we need a standardised approach to managing and administering contracts, be fair and do not leave AT or the public exposed to operational, legal, financial, or reputational risks. The contract lifecycle is closely aligned with the procurement lifecycle and covers contract planning, sourcing, management, and review phases.

Picture 1: Procurement Lifecycle


Spend Category Strategy
Supplier Relationship Management
Manage
Plan
Source
Review
Initiate project
1
Identify needs & analyse the market
2
3
Specify requirements
4
Plan approach to market & evaluation
5
Approach market & select suppliers
6
Negotiate & award contract
7
Manage contract & relationships
8
AT

Picture 2: Contract Lifecycle



1.1 Audience and scope

This document is written for both AT Procurement teams and business stakeholders and is intended to support AT Contract Owners in their activities related to the contract lifecycle.

AT Contract Owners may hold multiple roles and responsibilities as defined in Section 4 (Roles and Responsibilities) depending on the type and complexity of the contract / project.

1.2 Definition of contract management

Contract management includes tracking and monitoring delivery and costs, managing risks and relationships, conducting reviews, and resolving problems. This ensures that the contract delivers, as agreed. For the purposes of this document, we define Contract Lifecycle as the direct, explicit, hands-on planning, sourcing, management, and review of a specific contract according to the terms and conditions of the agreed legal contract (which can be either specific contract terms or general terms and conditions of a purchase order).

Contracts are the foundation of all AT's business relationships. Hence, the need for robust procurement management practices from initial planning, through sourcing and supplier engagement, hands on contract management, to a final close-out.

Good contract management will complement the goals set in the AT Procurement Strategy by maximising Value for Money, fostering good relationships with our suppliers, and managing risk between AT and third parties.

1.3 Purpose of this document

The purpose of the AT Contract Lifecycle Framework is to highlight the key steps to support the activities related to the contract lifecycle phases (contract planning, sourcing, management, and review).

The key benefit of this process is that it ensures that both AT's and Contractor's performance meet the requirements in terms of the legal agreement.

This document is not a guide to procurement processes, roles, or strategy. It represents the core activities that are undertaken as per the contract lifecycle – for more detailed guidance accompanying this framework, see the Guideline to Auckland Transport Contract Lifecycle Framework.

2 Contract lifecycle

2.1 Contract lifecycle phases

AT contract lifecycle has four phases that are closely aligned with our procurement lifecycle. This includes eleven key steps that form activities required to deliver great value, predictable outcomes and maximise benefit to our ratepayers and funding partners. The goal is to enable AT to be a customer of choice demonstrating leading supplier relationship management via robust contract management practices.

The following table summarises the four phases and eleven individual key steps to the contract lifecycle.

Table 1: Contract lifecycle phases and key steps

Contract lifecycle phase	Key steps
1. Planning	1. Request 2. Risk Assessment 3. Create
2. Sourcing	4. Negotiate 5. Approve 6. Award
3. Management	7. Set Up 8. Manage 9. Compliance
4. Review	10. Optimise 11. Close Out

2.1.1 Phase 1 – Contract Planning

The contract planning phase defines three key steps (Request, Risk Assessment, Create) that need to be initiated and planned for at the early stages of the contract lifecycle process. This is to ensure better accountability and ownership of AT's supplier contracts, and to clearly identify what is expected to be delivered over the contract term, in order to achieve the best value for money. Please refer to a brief description of the key steps below:

- **Request** – This step is a critical part of the contract lifecycle, and you will learn how to complete a contract request using our Contract Management System (CMS).

- **Risk Assessment** - In this step you will learn how to complete a Value Risk Assessment (VRA) to classify your contract. The VRA will help you to assess your contract classification based on a value and risk analysis. Auckland Transport recognises four contract classifications (Low, Moderate, High and Very High).

- **Create** - depending on the contract classification, our activities, focus and amount of effort required can vary. This step includes creating a contract draft and may include drafting a Contract Management Plan (CMP), that confirms contract management roles and responsibilities. This step includes seeking internal approval / endorsement for the draft contract.

2.1.2 Phase 2 – Contract Sourcing

The next three steps in the contract sourcing phase (Negotiate, Approve, Award) are important to ensure the right process and DFA approval are sought throughout the procurement activity. Wrong choices or bad decisions that can cause operational, legal, financial, and reputational damage and can often be avoided if the right people are involved and the correct process is followed. Please refer to a brief description of the key steps of this phase below.

- **Negotiate** – Negotiation is a critical part of the contract lifecycle and includes communicating with the supplier to mutually agree all aspects of the contract. This step may also include finalizing the CMP and agreeing on a Transition Plan (TP), if the project / contract is complex enough to warrant it.

- **Approve** – The most critical part of this step is to involve the right people following financial and non-financial delegations of authority (DFA) as per Delegations. DFA approval must be sought throughout the procurement process, including the contract award.
- **Award** – After a successful negotiation and approval, the contract can be signed and executed between the parties. If required, this step also includes onboarding the supplier into SAP.

2.1.3 Phase 3 – Contract Management

The contract management phase is crucial in the contract lifecycle and includes another three key steps (Set Up, Manage, Compliance). Contract management includes tracking and monitoring delivery, costs and compliance to the agreed deliverables. It is also critical to manage risks, relationships, conducting reviews and resolving issues. Below are the key steps in the contract management phase that must be considered.

- **Set Up** – Setting up the contract in the Contract Management System (CMS) is the key step for a successful delivery and management of the contract. The system will track all the contractual commitments and is designed to help the Contract Owner and other people involved to monitor and manage the day-to-day activities.

- **Manage** – This step includes mobilisation and implementation of the contract. The requirements may vary depending on the contract classification and a contract type and may also include management of contract extensions, renewals, and variations.
- **Compliance** – Managing contract compliance requires a good knowledge of the key contractual deliverables. It may also include, but is not limited to, reviewing the contract responsiveness and proactiveness, monitoring delivery and meeting KPIs, administering insurance certification and Supplier Code of Conduct (SCoC), monitoring Safety, Health & Wellbeing and measuring sustainable outcomes.

2.1.4 Phase 4 – Contract Review

The contract review phase is the last phase of the contract lifecycle with two important steps (Optimise, Close Out). Understanding the contract effectiveness and highlighting the lessons learnt can improve future contracts and can help to build the relationship with the current or future suppliers. The two steps highlight the summary of the contract review process.

- **Optimise** – This step allows us to determine future opportunities, feed into category spend plans and review effectiveness of the contract.
- **Close Out** – Before the contract can be completely closed out in the system it is important to remember that, where applicable, we will be able to manage any warranties and defects, ensure return of all AT's property, approve a final payment, manage retentions, and bond release and check that there are no outstanding invoices.

2.2 Contract classifications and contract types

Depending on contract classification our activities, focus and amount of effort required can vary based on risk and value of the contract. To determine the contract classification AT uses Value Risk Assessment (VRA) Tool (link here: Value Risk Assessment (VRA) - Open in Desktop App for full functionality). The tables below describe contract classifications and types of contracts used at AT.

Table 2: Contract classifications

Contract Classification	Description
Low	Low value, low risk contracts with the value less than $25K. A Standard Purchase Order (PO) can be used, except for restricted spend categories e.g., Legal Services, Physical Works, Engineering Professional Services etc.
Moderate	Contracts usually valued between $25K and $300K with a moderate risk profile, as determined by the VRA.

High	Contracts usually valued between $300K and $5M with a high-risk profile. Contract Management Plan (CMP) is likely required together with a relevant Contract and Contract PO.
Very High	Contracts usually valued greater than $5M with a very high-risk profile. CMP is likely required together with a relevant Contract, Contract PO. A Probity, Safety and/or Sustainability Plan may also be required.

Table 3: Types of contracts

Contract type	Covers	Business units	Notes
Standard Purchase Order	Low risk, low value goods and services (<$25k)	All	Not to be used in moderate, high, and very high-risk situations or for multiple engagements of a single higher-value contract.
Supply of Goods Agreement	Supply of Goods only	All	Use this template for Supply of Goods only (e.g., supply of office furniture). Used when a standard PO is not appropriate.
Contract Supply of Goods and Related Services	One-off procurements or ongoing deliveries	All	Use this template for supply of goods and related services (e.g. supply and installation of CCTV cameras). Used when a standard PO is not appropriate.
Term Service Agreement	One-off procurements or ongoing deliveries	All	This template can be used for all types of services (one-off procurement and/or ongoing delivery of services). Do not use this template for services associated with the construction industry. Used when a standard PO is not appropriate.
Professional Services Agreement	Contract Non-Engineering Professional Services	All	All non-engineering contracts, not dependent on the value.
	Contract Engineering Professional Services Short Form		Contracts under $100k.
	Contract Engineering Professional Services (CCCS)		Contracts over $100k. AT PACE used to measure performance.

Physical Works Supplier Panel	Panel One (PW1)	Infrastructure	$5M and above to maximum value of $50M.
	Panel Two (PW2)		Estimated value under $5M.
	Panel Three (PW3)		PW3 no new contract only old contracts that will be closed in the system (SAP).
	Safety Panel (PW4)		Panel for delivery of Safety projects under $4M.
Professional Services Panel	TEPS (Transport Engineering Professional Services)	All	Service order types. AT Pace used to measure performance over $100k. Procurement approval required for engagements $50 and over.
	ADSIP (Asset Database Support and Improvement Projects)		
	PAQ (Property Acquisitions)		
	TMSIS (Transport Monitoring Services and Innovative Solutions)		
NZS391(x)	NZS3910 – Construction	Infrastructure	Refer to PMO Guide to Contract Management
	NZS3916 - Design & construct including maintenance		
	NZS3917 - Building & Civil engineering works		
Information Technology	IT Software License and Services Agreement	BT	Intended for use with any third part supplier which offers software and services, which include an ongoing support and maintenance requirement.
	IT Master Services Agreement	BT	Intended as a full MSA covering Hardware, Software and Services. Should only be used with supplier expected to have multiple engagement across a wide range of services.
	IT Services and Deliverables Agreement	BT	This template should be used, when contracting with a supplier for a service (not consultancy) and they are delivering a finished product/services with defined deliverables.
	IT Hosted Solution Agreement	BT	This template is intended to be used when a supplier is hosting the solution (e.g. software or hardware services provided externally).

Public Transport Operating Model (PTOM)	Public Transport participation and unit agreements.	AT Metro / Integrated Network Enablement	National public transport contracts with specific partnership and engagement criteria.
General	SaaS Supplementary Terms	All	Must be used as supplementary terms when signing a suppliers own templated contract.
	Confidentiality Agreements and Memorandum of Understanding	All	Including One Way, Mutual and Understanding.
	Funding Agreement	All	Including KiwiRail.
Others	Others	All	External Communications Services SoW, Creative and Media Services, SOW Consultancy Services, External Legal Services.

3 Objectives

The Table below highlights some of the key objectives of contract management.

Table 4: Objectives of contract management

Key objectives	Description
Value for money	Enable savings opportunities identified during the procurement or contract management process, enable further benefits through ongoing performance reviews, service/supply chain improvements, innovation, sustainability outcomes etc.
Risk management	Reduce contractual risks through robust contract management practices and early identification of issues.
End-user outcomes	Maximise outcomes to end-users / customers by managing supplier performance, maintaining quality, improving productivity, and identifying opportunities for improvement including innovative and sustainable options.
Consistency	A clear and standardised approach across the business and suppliers are treated in a consistent manner by all AT stakeholders.

4 Roles and responsibilities

Contract management involves many skills and sometimes one person can be delegated to multiple roles and responsibilities. The requirements will vary depending on the complexity, category, and type of contract.

All roles are expected to declare any potential and/or actual conflicts of interest.

The table below provides examples of Roles and responsibilities in the contract lifecycle.

Table 5: Roles and responsibilities

Role	Responsibility
Contract Owner (CO)	• Manages the contract through post-award lifecycle as the single point of contact for the supplier on all contract matters including variations, development/implementation/compliance of the CMP, TP, Contract Risk Register. • Captures lessons learned, provides oversight of contractual commitments and supplier performance. • Depending on the contract type, the CO may also undertake audits, supplier meetings, monitor and provide reports as required. Recommended to be a representative within the business unit with the relevant commercial and operational skills and experience.
Contract Approver (CAP)	• Responsible for the AT internal contract DFA signature. • May be accountable for budget / cost centre that funds the contract. • Has the delegation to approve contracts, contract payments and variations. • May approve the Contract Management Plan (CMP) and/or Transition Plan (TP).
Delegated Financial Authority (DFA)	• Has the financial delegation authority (according to the Delegations Register) to sign off RFx documentation, approval to go to market, contract award and contract variations.
People Leader (PL)	• Appoints CO role(s) and ensures the resource is fit for purpose, appropriately skilled, trained and supported. • CAP and PL may be the same person in certain situations.

Project / Service Manager **(PM/SM)**	• Where there is a complex contract and the role of Contract Owner must be supported, or for construction projects, the Project / Service Manager is responsible for activities as determined by the Contract Owner in the CMP.
Engineer to the Contract (ETC)	• ETC (their representative, the representative's assistant, or BT Project Managers), monitors claims and variations, which will be audited by the Project Manager (when an ETC is in place) to ensure that changes to the project and scope are limited and communicated to the Project Sponsor, Client, and team.
Procurement Business Partner (PBP)	• A member of the AT Procurement team, responsible for engaging the market on any procurement/proposals and/or contract negotiations. • Leads the final process of awarding the contract following the procurement/proposal negotiation process. • Responsible for contract mobilization.
Procurement Support (PS)	• Provides support in relation to the lifecycle of contracts from contract set-up through to contract closure, especially with regards to the management of contracts in SAP. • Assists with the contract formation processes, setting up and maintaining contract details in SAP.
Suppliers / Partners (S/P)	• The organization with which the contractual commitment exists, responsible for fulfilling their obligations as set out in the contract.
Key Stakeholders (KS)	• Any AT team member who has a vested interest in the success of the contract and engagement with the suppliers/partners. • Often being referred to as 'users' and may or may not be in the same department as the CO and/or CAP.

5 Phases and key steps in contract lifecycle

The table below summarises the key steps and activities in each phase of contract management and how the approach can vary, depending on the result of value and risk assessment (Step 2 – Risk Assessment).

The Value Risk Assessment (VRA) approach determines the contract management classification (Low, Moderate, High or Very High), and the management requirements for each classification.

The requirements are split into three main groups as below:

- **R – Required** – the activity **must** be performed for the specific contract classification
- **A – Applicable, if required** – an **optional** activity for the specific contract classification
- **N/A – Not Applicable** – the activity is **not required** for the specific contract classification ~~type~~

The accompanying Guideline to Auckland Transport Contract Lifecycle Framework contains detailed information on how to carry out each activity, including supporting information, and identifies appropriate templates and tools to be used in each step, activity, and related tasks of the contract lifecycle.

Table 6: Phases, key steps, and activities in contract lifecycle

Key Steps	#	Activities	Low	Moderate	High	Very High
Phase 1 - Planning						
1 Request	1.1	Complete contract request form to clearly identify scope and outcomes required	R	R	R	R
2 Risk Assessment	2.1	Complete Value Risk Assessment (VRA) to classify contract	R	R	R	R
3 Create	3.1	Create contract draft (review T&Cs and specific contract conditions)	R	R	R	R
	3.2	Draft Contract Management Plan (CMP)	N/A	A	R	R
	3.3	Confirm contract management roles	N/A	A	R	R
	3.4	Seek internal approval/endorsement for draft contract	N/A	A	R	R
Phase 2 - Sourcing						
4 Negotiate	4.1	Present to supplier and mutually agree on all aspects of the contract	N/A	R	R	R
	4.2	Finalise CMP	N/A	A	R	R
	4.3	If required, agree a Transition Plan (TP)	A	A	A	A
5 Approve	5.1	Finalise contract and seek Delegated Financial Authority (DFA) approval to award	R	R	R	R
6 Award	6.1	Sign & execute between parties	R	R	R	R
	6.2	If required, onboard supplier into SAP	A	A	A	A
Phase 3 - Management						
7 Set Up	7.1	Set up contract in Contract Management System (CMS)	N/A	R	R	R
8 Manage	8.1	Mobilise	R	R	R	R
	8.2	Implement	R	R	R	R
	8.3	Manage contract extension, renewal, and variations	A	A	A	A
9 Compliance	9.1	Monitor compliance	A	A	R	R
Phase 4 - Review						
10 Optimise	10.1	Review contract effectiveness	A	A	A	R
11 Close Out	11.1	Close out activities	A	A	A	A
	11.2	Close contract in the system	R	R	R	R

Asset Management Policy

1. What is this policy about?

This policy establishes Auckland Transport's (AT's) expectations for the asset management practices to enable AT to contribute to an effective, efficient, and safe Auckland transport system in the public interest – now and into the foreseeable future.

2. Who and what does it apply to?

This policy applies to all AT employees and AT representatives (such as contractors, consultants, agency temps, external staff on secondment and volunteers) and AT Directors

This policy must be adhered to while you are at work as well as in any time that someone else might reasonably assume you are acting in your AT role.

Where this policy uses pronouns like "you", "your", "we", or "us", it is referring to anyone listed above, who this policy applies to." This policy covers the management of:

- The physical assets and systems that make up the AT transport infrastructure network including **road network assets** and **public transport assets**, as defined in this policy (refer to definitions).
- **Intangible assets** and **other assets** as defined in this policy (refer to definitions).

3. Policy Principles / What you need to know

In managing these assets, AT recognises the fundamental principles of asset management as set out in ISO 55000 Series International Asset Management Standard 2024 (ISO55000), namely:

- Value - Assets exist to provide value to the organisation and its stakeholders. Asset management does not focus on the asset itself, but on the value that the asset can provide to the organisation.
- Alignment - Asset management translates the organisational objectives into technical and financial decisions, plans and activities.
- Leadership - Leadership and workplace culture are determinants of realisation of value.

When it comes to asset management, AT expects that we:

- Always prioritise the health and safety of employees, contractors and the public.
- Comply with applicable statutory and regulatory obligations, as well as internal policies, processes, and procedures.
- Align our Asset Management System with the industry standard asset management practices of ISO55000.
- Align with Auckland Council Group Asset Management guidance, provided it does not conflict with AT Board directives.
- Optimise the total lifecycle costs of AT assets while ensuring they are safe, reliable, resilient, efficient, and affordable.
- Apply good industry practices – including risk management, computer modelling, detailed analytics, and market insights to make quality decisions that are in the long-term public interest. This includes considering sustainability and the impacts of climate change on AT's assets.
- Improve the resilience and adaptation of our services to the adverse effects of natural disasters, climate change, and economic events, while meeting customers' evolving expectations.
- Manage the impact of AT assets on the environment while supporting both AT and our customers' restorative and decarbonisation objectives.
- Continuously improve our asset management capabilities and capacity and measure the effectiveness of our efforts.

Asset Management System

AT will establish, implement, maintain, and continuously improve an Asset Management System (as defined in this policy). The Asset Management System will be run in accordance with the requirements of ISO55000 series.

The Asset Management System is not a standalone system. AT will progressively integrate asset management processes, activities, and data with other organisational functions such as operations, maintenance, quality, finance, safety, risk, and human resources.

AT will accurately document and regularly report on the effectiveness of the Asset Management System.

Note: Responsibility for the management of intangible assets and other assets will reside with the business unit responsible for creating, utilising and maintaining the assets (the Intangible and Other Asset Owners). Affected business units will need to familiarise themselves with the requirements of the ISO 55000 series with advice from AT's Strategic Asset Manager.

Asset Management Maturity

Improving asset management maturity is a key focus of continuous improvement for AT. AT will regularly review asset management practices and measure asset management maturity against nationally and internationally recognised frameworks, including the Commerce Commission Asset Management Maturity Assessment Tool (AMMAT) and the International Infrastructure Management Manual (IIMM).

AT will conduct regular, independent reviews of the asset management functions, using both external asset management specialists and/or government agencies. AT will use these reviews to identify gaps and develop plans to invest in and improve asset management practices to improve stakeholder confidence and trust.

4. Key terms

Term	Definition
Asset Management System	Integrated set of policies, processes, activities, procedures, tasks and information systems that comprise AT's approach to asset management.
Public Transport Assets	Infrastructure assets that enable the provision of scheduled public transport services, including: • Rail stations and depots/stabling • Rolling stock (trains) • Ferry terminals and wharves (including electrical charging infrastructure/landside assets) • Ferries (where owned by AT) • Buses (where owned by AT) • AT HOP machines • Bus stations and shelters • Public transport information systems & signage • Airstrips/Airfields
Road Network Assets	Infrastructure assets that enable the movement and journeys of private, public or freight vehicles, including: • Road carriageway pavements • Road network storm water assets • Footpaths and cycleways • Bridges and major culverts • Tunnels

Term	Definition
	- Walls (retaining walls, seawalls, and noise walls) - Parking buildings and on and off-street parking assets - Traffic systems (signals, signs, CCTV, markings & intelligent transport systems/connected devices) - Street lighting (including light towers and masts) - Corridor structures and fixtures (e.g. road furniture, gantries)
Intangible Assets	Non-physical items that provide potential or actual value and/or items that confer a right including: - Intellectual Property (e.g. patents, licences, trademarks, copyrights). - Resource consents for construction, operation and maintenance. - Land use rights. Easements & designations, leases. - Software & applications (AT developed & third party). - Data. Note: data linked or relating to a physical asset is managed as part of the physical asset.
Other Assets	Other AT assets that are not considered Public Transport, Road Network or Intangible Assets. For example, this includes: - Properties held for future roading purposes - Computer and network hardware - Furniture and fittings

5. Roles and Responsibilities

Role	Responsibility
All employees and representatives	• Adherence and compliance with this policy and related procedures. • Utilise an integrated Asset Information Management System appropriately for asset management tasks
Finance & Assurance Committee	• Set AT asset management policy and strategy for Board approval • Approve AT's asset management plans and monitor outcomes • Recommend agreed levels of service to the Board • Monitor asset management risks as an element of AT's risk profile

Role	Responsibility
	• Approve Long Term Financial Plans and provide appropriate resources for asset management activities.
Director of Infrastructure & Place	• Governance oversight of asset management. • Continually promote asset management to the organisation, the Board, external stakeholders, and the community. • Develop a long-term financial plan that reflect the state of the assets and recognises asset consumption. • Endorse Asset Management Plans and monitor their outcomes. • Integrate asset management, service planning and financial planning within AT. • Ensure asset management policies, strategies and plans are integrated into the corporate governance framework. • Foster and support cross functional collaboration within the organisation. • Adopt a cross-functional view, resolve differences between business units when necessary, and provide asset management leadership and support to achieve the benefits sought by AT. • Promote continual improvement. • Ensure accurate and reliable asset information is presented to the Board for decision-making. • Ensure adequate resources are available for meeting the asset management objectives and principles.
Intangible and Other Asset Owners	• Governance oversight of asset management for intangible or other assets within their directorates. • Develop plans to manage the intangible or other assets, including financial plans, and monitor their outcomes. • Ensure plans are integrated into the corporate governance framework. • Foster and support cross functional collaboration within the organisation. • Adopt a cross-functional view, resolve differences between business units when necessary, and provide leadership and support to achieve the benefits sought by AT. • Promote continual improvement. • Ensure accurate and reliable intangible or other asset

Role	Responsibility
	information is, when required, presented to the Board for decision-making. • Ensure adequate resources are available for meeting the intangible or other asset management objectives. • Promote awareness of intangible or other assets and their value to AT.
Chief Engineer (Policy Owner)	• Overall responsibility for the implementation of this policy for road network and public transport assets • Provide a coordinated and collaborative approach to asset management and asset management improvement across AT. • Regularly report to the R+R PSG / ELT on asset management performance and improvement actions. • Ensure staff are appropriately trained and skilled to perform the required asset management functions. • Ensure adequate resources are available for meeting the asset management objectives and principles.
AT Board (Policy Approver)	• Approve asset management policy and strategy • Act as custodians of AT's assets
Strategic Asset Manager	• Develop and implement Asset Management Plans for individual asset classes of road network and public transport assets using principles of lifecycle analysis. • Develop and implement improvement plans for individual asset classes. • Develop renewal capital and capital works programmes in accordance with Asset Management Plans and the annual budget for delivery by RAMR or IPD teams. • Consult with stakeholders and deliver levels of service to agreed risk and cost standards. • Manage infrastructure assets in consideration of long-term sustainability.

6. Supporting Information

Legislative compliance	This Policy supports Auckland Transport's compliance with the following legislation, including but not limited to: • Local Government (Auckland Council) Act 2009 • Land Transport Management Act 2008 • Utilities Access Act 2010 • Resource Management Act 1991 • Public Records Act 2005
Supporting documents	• Auckland Transport Statement of Intent • Asset Management Strategy • Asset Management Procedures • Asset Management Plans • Regional Land Transport Plan (RLTP) • ISO 55000 Series International Asset Management Standard • Auckland Transport Seismic Management Procedures
Related documents	• Auckland Transport Risk Management Framework

7. Non-Compliance

Asset management supports the compliance to multiple governance, legal, regulatory, government and shareholder requirements. Non-compliance perceived or otherwise, with those requirements can lead to loss of public reputation, increased stakeholder scrutiny, investigations and reviews, penalties and in extreme circumstances prosecution and/or fines.

Non-compliance may also lead to poor management of AT's infrastructure assets, which may result in unexpected and extended infrastructure asset outages, significant unbudgeted increases in costs and increased staff and public safety risks.

8. Approval & Review

Policy Owner: Director of Infrastructure & Place	**Policy Contact:** Chief Engineer
Endorsed by:	**Approved by:**
[Add signature] **Chief Executive**	[Add signature] **Auckland Transport Board**
Approval date: [DD/MM/YYYY]	
Effective date: [DD/MM/YYYY]	**Next review date:** [DD/MM/YYYY]

AT reserves the right to review, amend or add to this policy at any time upon reasonable notice to employees and representatives.

Information Security Policy

1. What is this policy about?

1.1. This policy defines the principles, objectives and responsibilities necessary for the secure operation of Auckland Transport's (AT's) **technology systems**, and **information assets**. It helps to ensure the **information security** practices of AT are reasonable, appropriate, and efficient.

1.2. By maintaining the **confidentiality**, **integrity**, and **availability** of AT's technology systems and information assets, we help to build trust and confidence through:

- Continued, uninterrupted operations across AT.
- Reduced exposure to liability.
- A safe environment for both staff and the public.
- **Compliance** with our legal and contractual obligations.

1.3. This policy is not a 'standalone' document. It is important to know that there are other AT policies, **security standards** and procedures that need to be followed, to ensure our security principles are met. These include AT's:

- Acceptable Use Policy
- Security standards
- Procedures that support security.

If you are not sure what security documents apply to you and your role, you can use AT ASSIST's Request a Security Resource - Auckland Transport or email Cyber Security to request a discussion.

2. Who does it apply to?

2.1 This policy applies to all AT employees and AT representatives (such as contractors, consultants, agency temps, external staff on secondment and volunteers) who use AT's information and systems.

2.2 This policy also applies to:

- All AT **data/information**, whether created, modified, processed, received, or stored.
- All **Information & Communications Technology (ICT)** and **Operational Technology (OT)** systems creating, storing, transmitting, or processing AT's information, whether owned by AT or owned by a third party (such as a cloud-based system, or leased).
- All AT locations, and any technology systems used by anyone to access AT information, wherever located.

2.3 Where reference is made to **Information Technology (IT)** equipment or an ICT system within AT's policy documents, it includes both IT and OT equipment and systems.

2.4 Where this policy uses pronouns like "you", "your", "we", or "us", it is referring to anyone listed above, who this policy applies to.

3. Principles

Each table in this document covers a key area of information security and management. For each one, you'll find guiding principles to help shape our approach, a short explanation of why they matter, and clear policy statements that show how we put them into practice. We've also included roles and responsibilities so everyone knows what's expected of them, depending on their role.

These principles help ensure AT technology systems and information assets are used securely and responsibly. The policy statements are backed by detailed standards, which lay out additional information such as specifications, requirements, actions, and configurations.

Senior Leadership needs to ensure that the adequate resources (both technology and personnel) are in place to support the implementation and operation of our systems, networks, and associated controls measures; to ensure that our information security risks are within AT's risk appetite. If external vendor support is needed, continuity of that support must be actively managed to prevent any lapse.

Security area	Principle
Access Control	We must protect our information and technology systems from unauthorised, use, disclosure, or modification.
Assurance and Governance	We will have timely and accurate reporting on information security matters.
Availability, recovery, and continuity	Systems and information must be available when we need them.
Business integration	We integrate information security into all our business operations.
Change control	We make sure that changes to our systems don't impact the confidentiality, integrity, or availability of our information systems.
Compliance	We will ensure that AT complies with its legal, contractual, and regulatory obligations associated with information and technology.
Incident and problem management	We proactively anticipate potential threats, and manage security incidents, breaches, and problems effectively.
Personnel security	We only provide access to our information and technologies to trusted people and hold people accountable for serious or intentional breaches.
Physical security	We will physically protect our data/information and information assets from compromise.

Security area	Principle
Risk management	We take a risk-based approach to information security, to ensure that information security risks are treated in a consistent and effective manner.
Security awareness, education, and capability	We must have the knowledge, skills, and training we need to help keep our systems and information safe.
Security by design	Security is most effective when embedded throughout the design, implementation, and maintenance of technology systems and processes. Before acquiring or implementing systems, security requirements must be clearly defined and met.
Third party risk management	We evaluate and manage the information security risks posed by our third parties.

3.1 Access Control

Core principles	**We must protect our information and technology systems from unauthorised, use, disclosure, or modification.** This means we must ensure the integrity, accuracy and consistency of the information and **data** we hold, and we keep information entrusted to us secure.
Rationale	Inappropriate access to systems and information can result in a number of issues such as fraud, theft, privacy breaches, disruption to operations, reputational ham, and even physical harm (if certain operational technologies are compromised).
Policy statements	Access to AT's systems (and the data/information they contain), needs to be managed and restricted, so that only the appropriate people have access. This should be done through physical, logical, and operational controls, and Role Based Access Control (RBAC). System access also needs to ensure that incompatible functions are kept separate and that segregation controls are working as intended. This includes (but is not limited to) segregation of routine user access from administrator access, and separation of developer, tester and production access. Controls must be applied to ensure access is appropriate, including:

- Restricting connections to authorised devices.
- Restricting the use of equipment media on AT devices.
- Classifying AT information (or designating information as unclassified) and applying appropriate operational controls based on the classification.
- Detection and prevention controls to limit the intentional or accidental disclosure of sensitive information to unauthorised people.

It is the responsibility of system and application administrators to ensure that access restrictions and controls are in place. However, all users of AT's systems are expected to adhere to the restrictions and controls (i.e. don't try to 'work around' them), and to flag any **access control** gaps or issues identified.

You may have access to information related to AT and its **stakeholders** which is not known to the public or others within AT. As outlined in our Code of Conduct, all AT staff AT representatives are required to maintain the confidentiality of AT's non-public data and information, both during their engagement with AT and after their employment or contract ends.

Refer to:

- Data Loss Protection Security Standard
- Identity and Access Management Security Standard
- Fax Machines, MFDs, Network Printers Security Standard
- Mobile Device & BYOD Security Standard
- Network Security Standard

3.2 Assurance and governance

Core principles	**We will have timely and accurate reporting on information security matters.**
Rationale	Useful and timely assurance information provides management and those responsible for governance with an up-to-date picture of the risks posed to the organisation, to inform better decision making.
Policy statements	In order to do this: • An information security strategy will be developed, and maintained, to provide a framework for information security activities. • An information security plan will support the information security strategy. The plan must be flexible to account for changing risks and threats, and performance and progress against the plan will be monitored. • We will measure and check that our information security controls are operating effectively, and complying with relevant laws, contracts, or other standards. The results will be reported to management and information security governance bodies in a timely manner. • We will log and audit information security-related events as part of an incident management and system monitoring process. The Technology Security team are responsible for developing the relevant information security strategies and plans, as well as measuring controls (with the support of Risk and Assurance where relevant) and tracking information security events. It is your responsibility to support the Technology Security team in relation to any of the above, and to abide by the additional requirements in our strategy, plans, controls, standards, or other documents. Refer to AT's Security Assurance Security Standard for further information.

3.3 Availability, recovery, and continuity

Core principles	**Systems and information must be available when we need them.**
Rationale	If our technology systems aren't operating efficiently and effectively, then AT isn't either.
Policy statements	System Owners (Business) need to define the maximum downtime allowable for a system, and the maximum amount of information/data loss that is acceptable. System Owners (Technical) will create and implement disaster recovery, backup, capacity plans, and data restoration plans and controls, to ensure that the availability requirements of users are met. Disaster recovery plans must sufficiently consider the dependencies of systems on other systems, information, and people, to ensure effective recovery. These backups, plans and controls need to be periodically tested for effectiveness. Refer to AT's Backup and Recovery Security Standard and Capacity Management Security Standard for more information. Those responsible for technology processes and controls must create and periodically test operational business continuity plans to ensure their security and operational controls can continue or resume within the expected time following a disaster or other interruption. Refer to AT's Business Continuity Management Security Standard for more information. Use of any external tools or resources (including diagnostic tools) must not compromise existing security controls.

3.4 Business integration

Core principles	**We integrate information security into all our business operations.**
Rationale	Information security needs to work both ways – it protects AT and its operations, but it also helps to ensure the business meets its objectives and achieves its goals securely. As such, to the maximum extent possible, security controls should not impede business objectives.
Policy statements	The Business Owners and System Owners, need to consider its business needs as well as security requirements, so that both elements are aligned and working as needed. Those involved in developing, designing, procuring or managing business processes and systems will consider information security in the functional and non-functional requirements of their processes and systems.

3.5 Change control

Core principles	**We make sure that changes to our systems don't impact the confidentiality, integrity, or availability of our information systems.**
Rationale	Effective change management helps ensure our systems and information security are not compromised. It also drives greater benefit realisation and achievement of outcomes.
Policy statements	Any change to systems, data, system configuration, or processes must be authorised and controlled through appropriate change management processes to ensure security, functionality, and capability is maintained. Any team or individual responsible for system configurations must ensure that all configurations are thoroughly documented and independently verified. Any changes to configurations must be recorded to support future reference and accountability. Technology system changes are to be implemented through the AT ASSIST / ServiceNow platform, while changes to data or business processes must follow the established procedural requirements of the team responsible. Owners or people responsible for AT's systems and technology assets (including physical, software and virtual assets) need to

	ensure that an accurate inventory is kept of those **assets** and systems. For more information on **change control,** check out the following standards: - Change Control Security Standard - Technology Asset Management Security Standard

3.6 Compliance

Core principles	**We will ensure that AT complies with its legal, contractual, and regulatory obligations associated with information and technology.**
Rationale	Other people and stakeholders rely on AT to protect their personal and confidential information safe, and information security plays a critical role in this. By complying with the relevant legal and contractual obligations we protect confidential information, protect AT from fines and lawsuits, and help maintain trust and confidence in AT.
Policy statements	Each team at AT is responsible for understanding how they handle and manage technology and information, and in turn which laws, policies, contracts, and regulations apply to them. All compliance requirements relating to information and technology must be identified, communicated, and adhered to (e.g., laws, regulations, directives, policies and standards, contracts, memoranda of understanding). Compliance will be continually measured and reported as part of the assurance process. Contact Compliance Support for further information. In addition, systems containing **personal information** must undergo Privacy Impact Assessments with the assistance of AT's Privacy Officer. Controls must be applied to ensure that AT's privacy principles are adhered to. Refer to our Privacy Policy and Customer Privacy Policy for more information. For any systems storing, processing, or transmitting cardholder data, the cardholder data protection requirements of Payment Card Industry Data Security Standard (PCI DSS) must be met. It's important to note that if AT loses its PCI DSS **accreditation**, transacting with payment cards on our system may not be possible. No payment card data is to be stored with AT's systems (test data is permissible).

	When IT equipment is no longer intended for use, it must be sanitised or destroyed based on the sensitivity of the information it contains. It is the Technology Security team's responsibility to develop a robust and technically sound approach to sanitisation, destruction, and disposal. It is your responsibility to follow that approach and return IT equipment to the right place. Refer to AT's Data Destruction Security Standard for more information.

3.7 Incident and problem management

Core principles	We proactively anticipate potential threats, and manage security incidents, breaches, and problems effectively.
Rationale	Effective management helps to maintain a resilient and secure environment by minimising the impact of security incidents and addressing known errors.
Policy statements	AT's Technology Security team will design, implement, and continually improve a security incident and problem management process, to effectively respond to unexpected events. It will include: • Planning for common incidents and incidents that can be expected to occur – such as risk/threat assessments. • Ongoing threat intelligence and communications with external security professionals (for staff with threat identification responsibilities). • Testing of AT's incident response capability. • Security tools and technical controls to detect and alert to threats and security events within AT's technology systems. • Regular, ongoing identification of vulnerabilities in technology systems, and timely mitigation of them (e.g. through patching). • Consideration (and monitoring) of insider threats. Refer to the Security Incident Management Security Standard. Information security-related events must be appropriately logged, protected, and audited to ensure accountability and support incident management, forensic investigations, and system monitoring. Event logs must be retained for a duration

	sufficient to meet the objectives of the controls they support. For detailed requirements and guidance, refer to the Event Logging Security Standard. To support vulnerability management, System Owners (Technical) must ensure patches, firmware updates, and alternative mitigation timelines are followed and standards aligned with. Refer to AT's Vulnerability Management Security Standard. To minimise security incidents, staff and onboarded AT representatives across AT must complete all security incident training assigned to them (see below). It's also important that you report security breaches or incidents as soon as possible (serious breaches should be reported immediately), so that they can be investigated and managed promptly. For more information on what constitutes a security breach, refer to ClickAware Hub. For more information on ways to Speak Up, check out our Speak Up Hub, or contact the AT Service Desk (0800 AT ASSIST).

3.8 Personnel security

Core principles	**We only provide access to our information and technologies to trusted people and hold people accountable for serious or intentional breaches.**
Rationale	Human beings are often one of the weakest links in information security. Robust personnel security ensures that our staff and other people that access our information and systems are appropriate, trained, and trusted to access them. Together with clearly defined consequences for breaching security requirements, they help to manage our information security risks.
Policy statements	Anyone wishing to have access to our technology systems must be screened and vetted, and completed access agreements, before access is granted. • People & Performance's (P&P) standard processes must be followed when onboarding AT employees or representatives, and P&P's processes must comply with AT's Personnel Security Standard. • Contractor and consultant responsibilities for information security will be included in contractual agreements, and

	access agreements must be in place before any access is granted. This is one of the reasons why it is important to use AT's standard contracts when engaging contractors.

3.9 Physical security

Core principles	**We will physically protect our data/information and information assets from compromise.**
Rationale	Physical security provides a key line of defence for sensitive information and technology equipment.
Policy statements	Appropriate physical security controls will be applied to restrict access to systems and information. Anyone responsible for AT's technology equipment needs to ensure that: • Physical security controls are in place to ensure the continuity and resilience of systems (for example, power supply, temperature, fire suppression, and flood protection). • The physical locations meet AT's minimum physical security standards. Refer to AT's Physical Security of Technology Systems Security Standard for more information.

3.10 Risk management

Core principles	**We take a risk-based approach to information security, to ensure that information security risks are treated in a consistent and effective manner.**
Rationale	Good security **risk management** ensures that controls and resources are most efficiently applied proportionate to risk.
Policy statements	System Owners assist with identifying, analysing, evaluating, treating, and monitoring security risks. They also ensure appropriate controls and mitigations are applied so AT's net or residual security risks are within AT's risk appetite, or at a level deemed acceptable by AT's Head of Technology Security. System Owners must ensure that AT's Proactive Security Manager or Head of Security is notified of identified security risks. AT's Proactive Security Manager will log these into the

	Security Risk Management Plan (SRMP), and corporate risk register. If you identify an information security risk or issue, you need to report it to the Technology Security team via AT ASSIST. For example, if you [believe you or someone else's account has been compromised, or if you find you can access information you don't think you should be able to see. If any net or residual information security risks exceeds AT's risk appetite, they must be formally escalated to Head of Technology Security, with documented details of the risks' possible impacts. The Head of Technology Security or delegate is responsible for determining AT's agreed approach to such risks. Risks owners must re-evaluate information security risks regularly, and whenever conditions change that may impact the risk. Refer to the Security Risk Management Security Standard.

3.11 Security awareness, education, and capability

Core principles	**We must have the knowledge, skills, and training we need to help keep our systems and information safe.**
Rationale	The successful control of information security risks requires everyone to know how to stay safe and secure. AT also needs enough staff with the right skills and knowledge to apply security controls.
Policy statements	Security education will be delivered through a structured programme managed by the Technology Security team, that is continually improved through regular monitoring of awareness. Everyone who accesses AT's information systems needs to: - complete the information security training that has been assigned to you via ThinkTank and Security Education platform; - read the policies, (in particular Acceptable Use Policy); standards (such as those referenced within this document), other information security documents, or sites (such as Click Aware and Viva); and

	- complete and abide by all related agreements and access requirements, such as the Remote Access Agreement (for third parties). AT must have enough staff with the right skills and experience to apply and manage AT's security controls. External resources should be used where AT's internal capacity and competencies are not sufficient. Those with particular security responsibilities for a system (such as System Owners) will be advised of and trained on their responsibilities. If you are not sure what training requirements may apply to you, reach out to the Technology Security team. Refer to AT's Security Awareness Security Standard for more information.

3.12 Security by design

Core principles	**Security is most effective when embedded throughout the design, implementation, and maintenance of technology systems and processes. Before acquiring or implementing systems, we must ensure AT's security requirements are clearly defined and met.**
Rationale	Embedding security from the earliest stages of design avoids delays, re-work, and potential breaches later on.
Policy statements	A robust security certification and **accreditation** process needs to be in place across all AT's technology systems, to assess the risks and ensure effective controls are applied. System Owners must ensure that systems: - Have a System Security Plan that defines the context, boundaries, security requirements, and controls of the system. - Use secure development methods with appropriate tools and testing when developing – to minimise coding errors and prevent security vulnerabilities. - Create, and make available (to the appropriate people) system documentation and architecture. - Consider what controls are required for each system. For example:

    - physical **access controls**, environmental controls, redundancy and resilience requirements are needed (for systems that involve equipment)
    - security controls for website and web-based applications.
- Design and implement network architecture in a manner that:
    - limits the risk of a cyber security-related incident.
    - has a minimum **baseline** security configuration which has been defined, applied, and tested (for any system with configurable security options).
- Define minimum security requirements and acceptance criteria prior to selecting a technology system or service.
- Integrate information security requirements and checkpoints into the project management process and software development lifecycle.
- **Harden** standard operating environments to minimise attacks and compromise. Standard Operating Environment Security Standard.
- Store, process, or transmit AT information using only software or cloud services that are approved as referenced in the Information and Records Repository Standard, or via the Technology Security team.
- Are designed to allow for the identification and deletion or disposal of information after it is no longer needed (to support privacy and record-keeping requirements).
- Are certified and accredited prior to being operated.
- Are re-certified and re-accredited periodically or whenever the system (or risks or the systems) significantly changes

Refer to:

- Certification and Accreditation Security Standard
- Cloud Computing Security Standard
- Data Encryption Security Standard
- Email Security Standard

	- Radio Frequency and Infrared Devices Security Standard - Removable Media Security Standard - Security Token Management Standard - Systems Development Life Cycle Security Standard - Virtualisation Security Standard

3.13 Third party risk management

Core principles	**We evaluate and manage the information security risks posed by our third parties.**
Rationale	Third parties often have access to AT's systems or data. If they are compromised, AT could be exposed to cyberattacks, data leaks, and regulatory violations.
Policy statements	All contracts that involve access to AT's information or technology systems must include minimum information security requirements. Any modifications to AT's standard security clauses, or the use of non-AT contract templates, must be reviewed and approved by the Proactive Security Manager. The Technology Security team must obtain assurance that any security controls applied by a third party relating to Auckland Transport's information or technology systems, meet or exceed the equivalent controls Auckland Transport requires for its internal systems and processes. System Owners (Business) must require that staff and third parties have undergone appropriate vetting checks prior to the users' being granted access to systems. Refer to the Supply Chain Risk Management Security Standard.

4. Key terms

Term	Definition
Access control	At a high level, access control is a selective restriction of access to data or systems. It consists of two main components: authentication and authorisation. It is a method of guaranteeing that users are who they say they are and that they have the appropriate access.

Term	Definition
Accreditation	Accreditation is the formal authority for a system to operate. Accreditation requires risk identification and assessment, selection and implementation of baseline and other appropriate controls and the recognition and acceptance of residual risks relating to the operation of a system.
Assurance	The confidence that a system meets its security requirements and is resilient against security vulnerabilities and failures. Represents the level of trust we give to a system that is safe to use.
Asset	A person, structure, facility, information, and records, information technology system and resources (hardware, software), process, relationships, or reputation that has value. Examples of IT assets are printers and multi-functional devices, mobile devices such as smart phones and tablets, payment devices such as credit card readers and EFTPOS terminals, CCTV cameras and related equipment such as video walls, traffic light circuits and management equipment, off the shelf software including software as a service (SaaS), customised and purpose-built software developed as part of the delivery of an information technology system or service.
Availability	Being accessible and usable upon demand. Ensuring that authorised users have timely and reliable access to information.
Baseline	A baseline is a type of standard that sets the minimum expectation for how a specific system or device must be configured to ensure security. An AT standard also may require that a specific external baseline be applied (for example, CIS hardening standards are followed for Azure).
Business integration	Aligns the business to security and vice-versa. It is the technology, controls, tactical solutions employed day-to-day to defend against cyber threats combined with the blueprint, framework, strategic plan, road map, governance and policies designed to influence and protect the company.
Capability	The means to accomplish a mission, function, or objective.

Term	Definition
Certification	Certification is the process to confirm that a system complies with minimum security standards. It is based on evaluation of the security and may include such activities as reviewing security documentation and test results. Certification is a prerequisite for accreditation.
Change control	A systematic approach to managing all changes made to a product or system. The purpose is to ensure that no unnecessary changes are made which can disrupt service or cause future implications.
Compliance	Ensuring AT is complying to the minimum of the security-related requirements. Compliance studies security processes and details the security at a single moment in time and compares it to a specific set of regulatory requirements. These requirements come in the form of legislation, industry regulations, or standards created from best practices.
Confidentiality	Ensuring that only authorised users can access information.
Continuity	The capability of an organisation to continue the delivery of services at pre-defined acceptable levels following a disruptive incident.
Control	A risk treatment implemented to reduce the likelihood and/or impact of a risk.
Data / Information	Includes written information, information in audio and/or visual format, documented records, structured data, spatial data, analytical data, data science models, and may include personal information.
Governance	The process of establishing and maintaining a framework to provide assurance that information security strategies are aligned with and support business objectives, are consistent with applicable laws and regulations through adherence to policies and internal controls, and provide assignment of responsibility, to manage risk.

Term	Definition
Harden	Hardening means tightening a system's settings and removing unnecessary features to reduce vulnerabilities and make it harder for attackers to break in. As an example, Technology and Technology Security teams may use CIS Benchmarks as a hardening guide or standard or refer to vendor's hardening recommendations.
Incident management	The process of managing IT service disruptions and restoring services within agreed service level agreements.
Information asset	A group of organised information that is organised and managed as a single entity e.g., AT's financial records.
Information & Communications Technology (ICT)	Refers to the systems and services used to manage and support business operations through computing technologies, including the communication layer.
Information Technology (IT)	Systems used to store, process and transmit information. Examples include servers, laptops, cloud infrastructure and mobile devices.
Information security	The practice of protecting information against unauthorised access or disclosure (confidentiality), protecting against unauthorised or improper modification (integrity), and ensuring information can be accessed when required (availability).
Integrity	Ensuring the accuracy and completeness of information and information processing methods.
Operational Technology (OT)	Systems that control or monitor physical devices, process and events. Examples include industrial control systems (ICS), sensors and human-machine interfaces.
Personal Information	Information about an identifiable individual. This includes any data that can reasonably be used to identify a living person, even if it doesn't explicitly name them. Examples include: • Name, address, email, phone number • Date of birth, photos, geolocation data • Financial and medical records • IP addresses, number plates, biometric data

Term	Definition
Personnel security	The purpose of personnel security is to establish controls on the hiring, training, and termination of all personnel (e.g., employees, contractors) to enforce compliance with the information security program. This gives a reasonable degree of confidence in the trustworthiness, integrity, and reliability of individuals, who, while performing their duties, have access to sensitive, critical, or valuable information, staff, and information processing facilities.
Physical security	Physical security is the protection of personnel, hardware, software, networks and data from physical actions and events that could cause serious loss or damage. This includes protection from fire, flood, natural disasters, burglary, theft, vandalism, and terrorism. The purpose of physical security documentation is to establish the rules for granting, control, monitoring, and removal of physical access to office premises; to identify sensitive areas within the organisation; and to define and restrict access to the same.
Problem management	Managing the lifecycle of all problems that happen or could happen in an IT service. The primary objectives are to prevent problems and resulting incidents from happening, to eliminate recurring incidents, and to minimise the impact of incidents that cannot be prevented.
Recovery	Disaster recovery's primary objective is to provide business continuity after disruption from manufactured or natural causes. Security recovery protects data assets after a data breach.
Risk management	The ongoing process of identifying security risks and implementing plans to address them. Risk is determined by considering the likelihood that known threats will exploit vulnerabilities and the impact they have on valuable assets.
Security awareness	The knowledge and attitude individuals possess regarding the protection of physical, and informational assets achieved through security awareness training. This is a formal process for increasing people's security awareness, eliciting secure behaviours in practice and developing a culture of security.

Term	Definition
Security by design	Refers to thinking about security at the start of the project. Security is built into a product, system, or service by design, instead of being added later. This concept can be approached through measures such as continuous testing, authentication safeguards and adherence to best programming practices.
Security standard	Standards define the minimum expectations to be applied within AT, regardless of the specific systems and processes in place. Standards specify operational criteria for products, services, and systems to ensure that they are safe, reliable, and consistently perform the way that they are intended to. Compliance with Standards is mandatory.
Stakeholder	A person or organisation that can affect, be affected by, or perceive themselves to be affected by a risk eventuating.
Technology system	The collective term applied to the different systems that transform, store, transport, or control data for particular purposes. This includes: Information Technology (IT) systems used to store, process, or transmit data and/or information. Operational Technology (OT) systems that control or monitor physical devices, processes, and events. Industrial Control Systems (ICS), being a subset of Operational Technology systems used to monitor and control industrial processes. IoT (Internet of Things), being physical objects that feature an IP address for internet connectivity, and the communication that occurs between these objects and other Internet-enabled devices and systems. These can be related to Information Technology or Operational Technology.
Third party risk management	The process of analysing and controlling risks associated with outsourcing to third-party vendors or service providers. This could include access to intellectual property, data, operations, finances, customer information or other sensitive information.

5. Roles and Responsibilities

Role	Responsibility
All employees, contractors, and consultants working for or on behalf of AT	• Maintain awareness and compliance of information security policies, standards, and processes. • Request, receive, and within allocated timeframes complete adequate and relevant information security awareness and training, necessary to undertake your role. • Be security aware and inform if breach of policy, standards or procedures are found; or any suspicious activity, to the Service Desk or whistle-blower process.
AT Board (Policy approver)	• Approve the Information Security Policy.
Auditor	• Provide independent feedback on the effectiveness of controls.
Chief Executive and Executive Leadership Team	• Clearly articulate roles and responsibilities. • Provide a positive tone from the top to communicate the importance of effective information security and risk management at AT.
Chief Technology Officer (CTO) (Policy owner)	• Ensure the security strategy aligns with the overall technology and business strategy. This includes integrating security into product development, infrastructure, and IT operations. • Work closely with the Head of Technology Security and other stakeholders to define security goals, priorities, and initiatives. • Ensure that technical teams understand and implement these strategies. • Manage, monitor, and report upwards on ongoing compliance efforts and the completion of risk management activities; and • Review and endorse the Information Security Policy.
Contracts Manager	• Ensure contractor responsibilities for information security are identified in contractual agreements. • Ensure minimum information security requirements are defined in all contracts that involve access to or provision of AT information or technology systems.
Head of Technology Security	• Assist AT management in interpreting the Information Security Policy. • Maintain and review the Information Security Policy. • Inform stakeholders of significant changes to the Information Security Policy. • Approve or reject security risks. • Annually review all accepted risks and revalue where appropriate.
Information Management & Data Governance Teams	• Provide a framework and processes for classifying information, storing, and handling information, and protectively marking information in accordance with its classification. • Responsible for providing strategic direction and focus to the activities of data and information management across AT. The scope includes data quality.

Role	Responsibility
	• Approve the deletion of data/information on AT's assets.
Management / People Leaders	• Ensure that AT employees and contractors comply with the information security policies, security standards, and procedures. • Promote security awareness to staff. • With the support of P&P, instigate investigation and/or disciplinary proceedings (where appropriate) against employees who breach the information security policies, the security standards and/or security procedures. • Ensure that any data/information, which by definition are AT records, is stored in the respective repository as prescribed by AT's Records Repository Standard. • Integrate information security into AT's project management and change management processes to identify and address information security risks. Ensure projects are implemented in compliance with the Information Security Policy, security standards, and security procedures.
People & Performance Team	• Screen personnel prior to them being granted access to systems. • Ensure access agreements are in place. • Enforce disciplinary and dismissal processes. • Ensure staff are adequately trained.
Privacy Officer	• Ensure that security is sufficiently considered as part of privacy activities, to guarantee that privacy principles are applied, and compliance requirements are met.
Proactive Security Manager	• Implement and assist system owners to obtain and maintain certification and accreditation of their systems. • Assist system owners in the developing, maintaining, updating, and implementing Security Plans and monitor progress. • Issue instructions on security and ensure that the instructions are followed. • Arrange for routine security assessments. • Responsible for helping the business to identify and apply security controls that support compliance. This includes overall accountability for: ○ Information Security ○ Policy ○ Acceptable use ○ Awareness ○ Incident response • Check the implementation and effectiveness of information security controls, and compliance and report these to management. • Log security risks on ARM.

Role	Responsibility
Project Managers	- Work with system owners to identify the policies, standards, processes, and guidelines applicable to the systems they are developing, and ensure that systems meet all technical and operational security requirements prior to project delivery. - Work with system owners (technical) to design Security Risk Management Plans, System Security Plans and Standard Operating Procedures for systems within their projects. - Ensure that the system certification and accreditation process is followed regarding their projects.
Reactive Security Manager	- Ensure security logs are incorporated into the Security Information and Event Management (SIEM) system and archived appropriately for auditing. - Investigate breaches of security and Security Incident response.
Risk & Compliance Manager	- Ongoing role to support, advise and co-ordinate the consistent approach to risk management and reporting. - Guide risk assessment and governance responsibilities. - Audit information security program, i.e., ensure all aspects of this document are updated as appropriate and completed. - Provide independent feedback on the effectiveness of controls. - Ensure all compliance requirements are identified, communicated, adhered to, continually measured, and reported as part of the assurance process.
Senior Leadership Team	- Lead and foster a culture that values, protects, and uses information for the success of AT. - Approve and communicate the Information Security Policy. - Define AT information security risk appetite in the context of the prevailing legal, political, socio-economic, and technological environment and external standards. - Ensure that a fit for purpose and adequately resourced information security framework is in place, including this policy as the top-level reference document. - Oversee the security related activities of the Leadership Team.
System Owners (Business)	- Obtain and maintain security accreditation of the systems under their business ownership. - Ensure sufficient personnel and technology resources are available. - Specify, authorise, and periodically review user access rights to their systems. - Define the requirements of their systems, including functionality, security, classification, and availability. - Ensure availability of vendor support cannot be allowed to lapse. - Accept residual business risk relating to their systems. - Ensure all security related audit issues are resolved.

Role	Responsibility
	• Check privacy principles, and PCI DSS requirements are adhered to for the systems under their business ownership. • Obtain assurance that third party controls meet or exceed the equivalent controls AT requires.
System Owners (Technical)	• Design, configure, operate, maintain, test and document systems under their technical ownership and in accordance with policies and standards. • Ensure the development, maintenance and implementation of complete, accurate and up-to-date Security Risk Management Plans, System Security Plans and Standard Operating Procedures for systems under their ownership. • Apply physical, logical, and operational access controls. • Apply segregation of incompatible functions. • Adhere to change management processes for any change to systems, data, or system configuration. • Implement an accurate inventory of all systems and technology assets. • Sanitise or destroy IT equipment according to process. • Apply classification to unstructured information, align with retention and records policies.
Technical Security Team	• Responsible for safeguarding its technology infrastructure, data and personnel from internal and external threats. • Maintain the confidentiality, integrity and availability of information systems and ensuring compliance with AT's security standards. •
Third Parties	• Third-party service providers who have access to AT information must be able to demonstrate that their systems and controls are compliant. • Third-party service providers who hold/perform related responsibilities on behalf of AT must be able to demonstrate that the services they provide relevant to this standard are compliant. • Third Parties are required to provide evidence of business continuity, service continuity, incident management and emergency management capability as stated in supplier agreements.

6. Supporting Information

Legislative compliance	• Contract and Commercial Law Act • Electronic Transactions Act 2002 • General Data Protection Regulation 2016/679. • LGOIMA (Local Government Official Information and Meetings Act) – Local Government Official Information and Meetings Act 1987 • Privacy Act 2020 • Public Records Act 2005 & Amendment Act 2010
Supporting documents	Security standards: • Backup and Recovery Security Standard • Business Continuity Management Security Standard • Capacity Management Security Standard • CCTV Standards • Certification and Accreditation Security Standard • Change Control Security Standard • Classification and Protective Marking • Cloud Computing Security Standard • Data Destruction Security Standard • Data Encryption Security Standard • Data Loss Protection Security Standard • Email Security Standard • Event Logging Security Standard • Fax Machines, Multi-function Devices and Network Printers Security Standard • Identity and Access Management Security Standard • Mobile Devices & BYOD Security Standard • Network Security Standard • Operational Technology • Payment Card Industry Data Security Standard • Personnel Security • Physical Security of Technology Systems • Radio Frequency and Infrared Devices • Removable Media Security Standard • Security Assurance • Security Awareness Security Standard • Security Incident Management • Security Risk Management Security Standard • Security Token Management • Standard Operating Environment Security Standard • Supply Chain Risk Management Security Standard • Systems Development Life Cycle Security Standard • Technology Asset Management Security Standard

	• Virtualisation Security Standard • Vulnerability Management Security Standard Guidelines: • Acceptable Use Guidelines • Mobile Device Guidelines
Related documents	• CCTV Policy • Code of Conduct Policy • Fraud and Corruption Policy • Information Sharing Agreement • Information and Records Management Policy • Information and Records Repositories Standard • Privacy Policy • Records Disposal Schedule • Risk Management Policy This Policy supports AT's compliance with the following external frameworks and standards: • NIST Cybersecurity Framework • New Zealand Information Security Manual • PCI DSS (Payment Card Industry Data Security Standard) • Protective Security Requirements

7. Non-compliance

7.1 Consequences

Non-compliance with AT's information security policies, standards, or procedures may compromise technology systems and information assets, exposing the organisation and its stakeholders to unnecessary risk.

Serious and/or deliberate violations of the information security policies, standards or procedures will be subject to AT's disciplinary policy, which may include disciplinary action, up to and including dismissal or contract termination.

7.2 Exception process

Full compliance with AT's security standards and procedures is expected. However, it is acknowledged that this may not always be possible or practical.

Dispensation from any of the information security policy, standards, or procedures requires the express written approval of the Head of Technology Security and must be based on an assessment of the risk posed.

Any decisions to be non-compliant with security standards must be reviewed at least annually. The review process should be aligned with the Risk Management Framework.

8. Approval & Review

Policy Owner: Chief Technology Officer	**Policy Contact:** Proactive Security Manager

Endorsed by:
[Add signature]

[Add title of endorser]

Approved by:
[Add signature]

[Add title of approver]

Approval date: [DD/MM/YYYY]

Effective date: [DD/MM/YYYY]

Next review date: [DD/MM/YYYY]

AT reserves the right to review, amend or add to this policy at any time upon reasonable notice to employees and representatives.