

Supplier Policy
Artificial Intelligence (AI) Security

C1 Public

SCOPE

These policy requirements apply to all suppliers that provide AI-enabled products or services to One NZ, including:

- Generative AI and Large Language Model (LLM) services
- AI-enabled Software-as-a-Service (SaaS) platforms
- AI-powered development and productivity tools
- Machine learning solutions and analytics platforms
- AI agents, automation services, and intelligent assistants
- Any solution that uses AI to generate content, recommendations, predictions, decisions, or automated actions

1 POLICY

1.1 Introduction

One New Zealand (One NZ) is committed to the secure, responsible, and ethical use of Artificial Intelligence (AI). These Supplier AI Security Requirements define the minimum expectations for suppliers that provide, develop, host, support, or operate AI-enabled products, services, platforms, or capabilities on behalf of One NZ.

The purpose of these requirements is to ensure AI solutions are implemented and operated in a manner that protects One NZ, its customers, employees, partners, and information assets, while supporting compliance with applicable legal, regulatory, privacy, and contractual obligations.

2 SUPPLIER REQUIREMENTS

2.1 Governance and Accountability

Suppliers must maintain appropriate governance arrangements for the development, deployment, operation, and monitoring of AI capabilities. Clear accountability must exist for the management of AI-related risks, security controls, and regulatory compliance obligations.
Suppliers must be able to demonstrate that AI capabilities are subject to documented oversight and risk management processes appropriate to the nature and impact of the service being provided.

2.2 Secure By Design

AI solutions provided to One NZ must be designed, implemented, and operated using recognised security practices. Security controls should be integrated throughout the lifecycle of the AI capability, including design, development, testing, deployment, operation, maintenance, and retirement.
Suppliers must take reasonable measures to identify, assess, and mitigate risks arising from AI functionality, system integrations, and the use of data.

2.3 Data Protection and Privacy

Suppliers must protect One NZ information and personal information throughout its lifecycle.
Data used by AI systems must be handled in accordance with applicable privacy laws, contractual obligations, and industry good practice. Suppliers must implement appropriate safeguards to prevent unauthorised access, disclosure, alteration, or loss of information.
Data provided by One NZ must not be used to train, improve, or develop AI models unless explicitly authorised in writing by One NZ.

C1 Public

2.4 Identity and Access Management

Access to AI systems, supporting infrastructure, and data must be restricted to authorised individuals, services, and processes.
Suppliers must implement access controls based on least privilege principles and maintain processes for the secure management of identities, credentials, and privileged access.

2.5 Monitoring and Incident Management

Suppliers must maintain appropriate monitoring and logging capabilities to support the detection, investigation, and response to security events affecting AI services.
Suppliers must promptly notify One NZ of any actual or suspected security incident, privacy breach, unauthorised access, or material issue that may affect the confidentiality, integrity, availability, or reliability of services provided to One NZ.
Suppliers must cooperate with One NZ during investigations and support remediation activities where required.

2.6 Responsible AI Practices

Suppliers are expected to develop and operate AI capabilities in a responsible manner that promotes fairness, transparency, accountability, and human oversight where appropriate.
Suppliers should be able to explain the intended purpose of AI capabilities and demonstrate reasonable controls to reduce the risk of harmful, unsafe, discriminatory, or unintended outcomes.

2.7 Regulatory and Contractual Compliance

Suppliers must comply with all applicable legal, regulatory, privacy, and contractual obligations relevant to the services provided to One NZ.
Where required by contract, suppliers must provide evidence of compliance with security, privacy, and risk management requirements and support reasonable assurance activities conducted by or on behalf of One NZ.

2.8 Continuous Improvement

Suppliers are expected to maintain an ongoing programme of security and risk management activities to address emerging threats, vulnerabilities, regulatory changes, and developments in AI technology.
Material changes to AI services that may affect risk, security, privacy, or compliance must be communicated to One NZ in accordance with contractual obligations.

2.9 Compliance

Compliance with these requirements may be assessed as part of supplier onboarding, contract management, risk assessment, or assurance activities undertaken by One NZ.
Failure to meet these requirements may result in remediation actions, additional controls, contractual review, or termination of services where appropriate.

C1 Public

3 DEFINITIONS AND INTERPRETATION

In this One NZ AI Security Policy, the following words and expressions shall have the meanings set out below:

"AI Solution"	A system, application, or service that incorporates one or more AI systems and supporting components (including data, models, algorithms, infrastructure, and processes) designed to perform tasks or provide outputs that influence decision-making or operations.
"AI Capability"	The ability of an AI system or AI solution to perform one or more AI functionalities to achieve intended outcomes within a defined context of use.
"AI System"	A machine-based system that, for explicit or implicit objectives, infers from input data how to generate outputs such as predictions, content, recommendations, or decisions that influence physical or virtual environments.
"AI Pipeline"	The AI Pipeline is a One NZ system used to govern AI capabilities across their lifecycle, acting as the system of record and enforcing required controls, approvals, and assurance processes.
"AI Principles"	The set of guiding values and requirements established by the organisation to ensure that AI systems are developed, deployed, and used in a responsible, ethical, and trustworthy manner.

C1 Public