

AI Lifecycle Management Standard

1. Purpose

Artificial Intelligence (AI) presents opportunities to improve how Contact operates through enhanced insight to support decision-making, efficiency, automation, and innovation. To realise these benefits safely and responsibly, AI solutions must be governed throughout their lifecycle.

This AI Lifecycle Management Standard defines the minimum requirements for the design, development, acquisition, deployment, operation, monitoring, and retirement of AI systems used at Contact. It establishes a consistent approach to managing AI-related risks, assigning accountability, maintaining transparency, and ensuring compliance with legal, regulatory, security, privacy, and ethical obligations.

This standard supports the Responsible AI Usage Policy by embedding responsible AI practices across the AI lifecycle and ensuring that AI systems are implemented in a way that is safe, trustworthy, and aligned with Contact's values.

2. Scope

This standard applies to Artificial Intelligence (AI) systems and AI-enabled solutions that are developed, configured, procured, integrated, deployed, operated, or used by or on behalf of Contact.

For the purposes of this standard, AI includes technologies that use data-driven algorithms or models to generate predictions, recommendations, decisions, content, insights, or actions. This includes, but is not limited to:

- Machine learning and predictive models
- Generative AI and large language models (LLMs)
- Agentic AI and autonomous AI systems
- Computer vision and image recognition
- Natural language processing (NLP)
- AI-enabled automation and workflow orchestration
- Other emerging AI capabilities and technologies

3. Application of this Standard

This standard applies to all new and existing AI solutions used beyond personal productivity regardless of whether the AI capability is developed internally or provided by a third party. Personal productivity use is governed by Contact's Responsible AI Usage Policy and approved technology

controls. AI solutions used for internal business purposes, shared across teams or business units, integrated into business processes, relied on by others, used by customers or partners, or producing outputs shared outside Contact must follow this standard.

Use type	Audience	Description	Standard applies
Personal productivity	Myself	AI solutions used by an individual to support their own productivity which are not shared, published, integrated into business processes, or relied on by others.	No
Internal business use	Internal	AI solutions shared with teams, departments, or business units, or across Contact to support internal business processes, decisions, operations, or employees.	Yes
External use	External	AI solutions used by customers, partners or external stakeholders, or where AI-generated outputs are provided outside of Contact.	Yes

4. Definitions

Artificial Intelligence (AI) refers to systems designed to perform tasks that typically require human intelligence, such as learning, reasoning, problem-solving, perception, and language understanding. These systems use data-driven algorithms and models to make predictions, generate insights, or take actions, and may improve their performance over time through adaptive learning.

Artificial Intelligence (AI) is an umbrella term that encompasses a wide range of technologies and capabilities designed to perform tasks that typically require human intelligence. The following table provides definitions and examples of several key areas within AI, helping to clarify the breadth and depth of what AI can achieve in practical settings.

Type	Description	Examples / Use Cases
Machine Learning (ML)	A subset of AI that enables systems to learn patterns from data and improve performance without explicit programming. Most ML algorithms follow deterministic mathematical procedures given the same data and parameters, they produce the same model and predictions. However, the learning process itself is adaptive: the system adjusts its internal parameters based on observed data rather than fixed rules.	Learns from historical data to improve predictions or recommendations as new data arrives. Used in predictive analytics, anomaly detection, and recommendation systems.
Computer Vision	A field of AI that enables systems to interpret, analyse, and understand visual information from images, video, cameras, sensors, or other visual inputs. It commonly uses machine learning and deep learning to recognise objects, detect patterns, read text, track movement, and derive insights from visual data.	Used for visual inspection, asset condition monitoring, defect detection, image classification, object detection, optical character recognition, safety monitoring, and analysis of imagery from drones, cameras, or operational systems.

Physical AI	A field of AI that enables systems to perceive, reason about, and act within the physical world. Physical AI combines software intelligence with sensors, actuators, robotics, control systems, and operational technology so that AI can interact with real-world environments, assets, equipment, or infrastructure.	Used in robotics, autonomous systems, drones, smart devices, industrial automation, asset inspection, field operations, safety monitoring, and optimisation of physical processes or equipment.
Generative AI	Generative AI is a branch of Artificial Intelligence focused on creating new, original content such as text, images, audio, or video based on patterns learned from existing data. It is non-deterministic, meaning outputs can vary even with the same prompt because models use probabilistic sampling. Generative AI is trained on large data sets and generative AI models synthesize entirely new outputs that resemble the training data but are not exact copies.	Generative AI creates entirely new content such as articles, images, designs, or music rather than duplicating existing data.
Large Language Models (LLMs)	A Large Language Model (LLM) is an advanced AI system designed to understand and generate human language. It is trained on massive text datasets using deep learning to learn patterns such as grammar, meaning, and context. This enables LLMs to produce coherent, contextually relevant language outputs without explicit programming.	LLMs power tools that write reports, summarise documents, answer questions, generate code, and support chatbots. Some also handle images and audio.
Small Language Models (SLMs)	Lightweight versions of large language models, optimized for efficiency and resource-constrained environments such as mobile devices or edge computing.	Ideal for tasks requiring heightened privacy or tailored to specific domains, as well as deployment on mobile devices or at the network edge where resources are limited.
AI Assistant	AI Assistants are AI-powered systems that simulate human conversation, either through text or voice interactions. They use natural language processing (NLP) to understand user queries and respond appropriately. AI Assistants may be rule-based, using predefined scripts, or use machine learning and language models to engage in more dynamic, context-aware dialogue. Advanced AI Assistants continuously learn from interactions to improve their responses over time.	Some examples include handling customer service requests automatically, delivering technical support, helping users navigate procedures, assisting with reservations, and supplying information via websites, messaging platforms, or voice-activated assistants.
Agentic AI	Agentic AI refers to artificial intelligence systems that can operate independently to achieve a goal. These systems don't just respond to prompts, they can plan tasks, make decisions, and take actions without constant human input. Agentic AI can adapt based on feedback or changing conditions.	Agentic AI is used in scenarios where tasks need to be completed end-to-end without constant human input. For example, it can autonomously research and compile information, generate and format reports, or manage

		workflows by retrieving data, analysing it, and sending updates.
--	--	--

5. AI lifecycle

All eligible AI solutions must follow Contact's AI lifecycle management process from initial concept through to retirement. The lifecycle provides a consistent approach to governance, risk management, accountability, and oversight.

5.1 Intake and risk assessment

Identify the business problem, desired outcomes, and success measures. Assess whether AI is the appropriate solution and complete the AI assessment process to determine the AI type and risk level. Assign business and technical owners.

5.2 Design and solution architecture

Define the proposed solution architecture, leveraging approved architecture patterns where available. Design the data and DataOps approach, system integrations, security, privacy, human oversight, and control mechanisms required to meet the solution's risk, compliance, and operational requirements. Establish acceptance criteria and document the proposed architecture for implementation.

5.2.1 Location of data processing and geo-location

AI solutions must be deployed only within approved geographic locations and hosting environments that meet Contact's information security, privacy, legal, and regulatory requirements. The geographic location(s) in which AI models are hosted, executed, and process data must be identified and documented as part of the solution design and approval process.

The Business AI Steward and Technology AI Steward must document:

- The geographic location(s) where AI models are hosted and executed.
- The geographic location(s) where data, prompts, inputs, outputs, and supporting services are stored or processed.
- Any cross-border data processing, storage, replication, backup, or transfer arrangements associated with the solution.

Where an AI solution involves processing or storing data across multiple geographic regions, the proposed approach must be reviewed and approved by Information Security and any other relevant stakeholders.

As a standard practice, Contact's AI solutions are typically deployed within approved Australia, New Zealand, or Singapore data centre regions. Alternative geographic locations may be used where approved through the applicable security, privacy, and risk assessment processes.

Material changes to model hosting locations, data processing locations, or cross-border data flows must be reviewed, documented, and reflected in the AI Model Management Registry prior to implementation.

5.2.2 AI transparency and disclosure

Where appropriate, AI solutions must provide clear and meaningful disclosure when users are interacting with an AI system, receiving AI-generated content, or consuming outcomes that have

been materially influenced by AI. The disclosure mechanism must be proportionate to the intended audience, use case, and level of impact.

5.3 Data considerations

Good quality data is essential for achieving reliable, safe, and fit-for-purpose outcomes from AI solutions. AI solutions must use trusted, authorised, and appropriate data sources and be designed so that data can be understood, governed, and managed throughout the solution lifecycle.

During design, the Business AI Steward and Technology AI Steward must identify and document the data sources, intended use of data, sensitivity classification, ownership, access requirements, and key data flows associated with the solution. This documentation must support appropriate governance, security, monitoring, and auditability.

AI solutions must comply with Contact's data management, information security, privacy, and retention requirements. Access to data must be limited to what is necessary for the approved use case, and solutions must use approved data access and integration mechanisms.

Where personal or privacy-sensitive information is processed, a Privacy Impact Assessment must be completed to determine the appropriate treatment, controls, approvals, and ongoing monitoring requirements. Material changes to data sources, data flows, access permissions, or data usage must be reviewed and reflected in solution documentation and the AI Model Management Registry where applicable.

5.4 Development and configuration

Develop, configure, procure, or integrate the AI solution and supporting components, including model selection and configuration where applicable. Ensure appropriate documentation, version control, and traceability are maintained throughout development.

5.5 Testing and validation

Validate the AI solution against defined requirements and benchmarks to demonstrate that it is fit for purpose and meets functional, performance, security, privacy, safety, and compliance requirements before deployment.

Where relevant, assess the consistency, reliability, and variability of AI outputs and confirm that performance remains within defined acceptance thresholds.

For AI solutions using LLMs, agents, or other generative AI capabilities, establish benchmark test cases and automated regression testing where practical.

If relevant for probabilistic outputs, perform uncertainty quantification and confirm that observed variability is within requirement specification.

Testing should be repeated following material changes, including updates to prompts, configurations, workflows, data sources, underlying models, or model versions, to confirm the solution continues to meet its requirements.

5.6 Deployment and release

Deploy the AI solution using approved release management processes. Prior to deployment, confirm that testing, validation, risk assessments, and required approvals have been completed.

Maintain an auditable record of deployment decisions, versions, prompts, model configurations, approvals, release notes, and supporting documentation.

Register the deployed solution in the AI Model Management Registry and update the register whenever there are material changes to the solution, including changes to models, prompts, integrations, configurations, or intended use.

5.7 Operation and monitoring

Monitor the AI solution throughout its operational lifecycle to ensure it continues to perform as intended and remains fit for purpose. Appropriate monitoring, logging, and audit mechanisms must be established and maintained to support oversight, accountability, incident investigation, and compliance activities. Performance, usage, risks, incidents, security, privacy, and compliance requirements must be reviewed on an ongoing basis.

Where relevant, monitor for data drift, concept drift, changes in user behaviour, **cost drift** and degradation in model or solution performance. Establish thresholds and alerting mechanisms to identify significant departures from expected outcomes, accuracy, reliability, or service levels.

Define and maintain appropriate mitigation measures, including human oversight, fallback processes, retraining, revalidation, rollback, or solution suspension where monitoring identifies unacceptable risks or performance issues.

Material incidents, performance issues, changes to risk profiles, and significant updates to the solution must be documented and reflected in the AI Model Management Registry.

5.8 Change management and continuous improvement

Changes to models, prompts, training data, configurations, integrations, workflows, or controls must be managed through approved change management processes. Proposed changes should be assessed for their potential impact on performance, risk, security, privacy, safety, compliance, and business outcomes.

Material changes must undergo appropriate testing and validation, including regression testing where practical, before release. Changes should only be implemented where there is evidence that the solution continues to meet defined requirements and delivers the intended outcomes.

The Business AI Steward and Technology AI Steward must jointly review and approve material releases. All changes, approvals, and supporting documentation must be maintained as part of the solution's lifecycle records and reflected in the AI Model Management Registry where applicable.

5.9 Retirement and decommissioning

AI solutions that are no longer required, supported, or fit for purpose must be retired in a controlled manner, including removal of access, management of retained information in alignment with the Information and Data Disposal Standard, and updating the AI Model Management Registry.

6. AI lifecycle management

AI Lifecycle Management is the process of governing AI solutions throughout their lifecycle to ensure they are designed, developed, deployed, operated, monitored, and retired in a safe, effective, and responsible manner.

Consistent with the principles of **NZS ISO/IEC 42001:2025**, Contact applies a lifecycle-based approach to AI governance that integrates risk management, accountability, human oversight,

transparency, security, privacy, and continuous improvement throughout the operation of AI solutions.

6.1 AI model management registry

The AI Model Management Registry is the authoritative record of AI solutions used, developed, configured, or deployed across the organisation.

All AI solutions within the scope of this standard must be recorded in the registry and maintained throughout their lifecycle. The registry must support governance, risk management, compliance, operational oversight, and audit requirements, and must be version controlled to maintain a history of material changes.

At a minimum, the registry must include:

- Solution name and description
- Business AI Steward and Technology AI Steward
- Intended use and business outcomes
- AI pattern(s) utilised (for example, chatbot, agent, retrieval-augmented generation, prediction, classification, optimisation, computer vision)
- Risk classification and approval status
- Operational status (for example, proposed, development, testing, production, retired)
- Key models, data sources, integrations, and dependencies
- Version history and material changes
- Links to relevant lifecycle artefacts, including assessments, approvals, testing records, monitoring evidence, and supporting documentation

6.2 AI assessments

The AI Assessment is used to determine the governance requirements that apply to an AI solution. It forms part of the Intake and Risk Assessment stage and is used to identify the solution's governance zone, risk profile, required controls, ownership, and lifecycle obligations.

The results of the AI Assessment must be considered throughout the lifecycle of the AI solution and reviewed when material changes occur.

6.3 Technology Asset Registration

AI solutions classified as having business impact or criticality to Contact operations must be registered within the Technology Asset Management (TAM) system and managed in accordance with Contact's technology asset management requirements. Registration must include identification of the service owner, support arrangements, service criticality, target service levels (SLAs), and incident recovery expectations (MTTR) appropriate to the business impact of the solution. AI solutions used solely for individual productivity and not relied upon by others are not required to be registered in TAM.

7. Compliance

Contact requires all employees, contractors, consultants, secondees, subsidiaries, and third parties acting on behalf of Contact to comply with this standard where it applies. Compliance will be

monitored by Technology Innovation, with oversight from Data and AI governance and relevant risk, security, privacy, legal, and assurance processes.

On occasion, there may be sound business reasons why conformance to this AI Lifecycle Management Standard and related policies and standards may not be appropriate. Such exceptions must be raised with a manager, the relevant Leadership Team member, the Business AI Steward, or Technology AI Steward with approval based on a risk assessment and business justification.

Known or suspected non-compliance must be raised with a manager, the relevant Leadership Team member, the Business AI Steward, or Technology AI Steward. Employees may also raise concerns in accordance with Contact's *Protected Disclosures (Whistleblowing) Policy*.

8. Related Documents

List of related documents

8.1 Policies

- Responsible AI Usage Policy
- Information Security Policy
- Confidentiality and Privacy Policy
- Data and Information Management Policy
- Technology Acceptable Use Policy

8.2 Standards

- Information and Data Capture Standard
- Information and Data Disposal Standard
- Information and Data Sharing Standard
- Contact's Requirements for data retention Standard
- Data Retention and Destruction for Personal Information Standard
- Data Retention and Destruction for Corporate Information Standard

9. Document control

Version	1
Approved	July 2026
Document approver	Tighe Wall, Chief Technology Officer
Document owner	Kate Kolich, Head of Data and AI
Next review date	July 2027

10. Appendices

10.1 Glossary

The following terms that may be used have a specific meaning:

Term	Definition
Automation Bias	The tendency for people to favour decisions or suggestions made by automated systems, even when those systems may be incorrect.
Bias (in AI)	Systematic errors in AI outputs caused by flawed data, design or assumptions, which can lead to unfair or discriminatory outcomes.
Business AI Steward	The Business AI Steward is accountable for business outcomes, risk management, human oversight, and responsible use of the solution.
Context Binding	The process by which an AI system maintains awareness of relevant information across interactions, allowing it to respond appropriately based on prior inputs, user roles, or situational context.
EULA	End User License Agreement
Explainability	The extent to which the workings and decisions of an AI system can be understood and interpreted by humans.
Human-in-the-loop	Where human oversight is maintained in AI decision-making processes, especially for critical or high-risk tasks.
Machine Learning (ML)	A branch of AI that enables systems to learn from data and improve performance over time without being explicitly programmed for each task.
Model Drift	A decline in the accuracy or reliability of an AI model over time due to changes in the underlying data or environment.
Neural Network	A computational structure inspired by the human brain, used in machine learning to detect patterns and relationships in data.
Responsible AI	The practice of designing, developing and using AI in ways that are ethical, transparent and aligned with legal and organisational values.
Technology AI Steward	The Technology AI Steward is accountable for the technical design, implementation, operation, monitoring, security, and maintenance of the solution.

10.2 Relevant Legislation for AI use in New Zealand

MBIE's Responsible AI Guidance for Businesses (2025) highlights several key legislative areas that intersect with AI use which have been provided here for context as the minimum legislation that all companies in New Zealand using AI should be aware of and adhere to:

1. Commerce Act 1986

- **Relevance:** AI systems must not engage in anti-competitive behaviour or mislead consumers.
- **Examples:** Algorithmic pricing collusion, false reviews, or deceptive advertising practices.

2. Privacy Act 2020

- **Relevance:** AI systems must handle personal data in accordance with New Zealand's privacy principles.
- **Examples:** Ensuring lawful data collection, informed consent, data minimisation, and secure storage.

3. Human Rights Act 1993

- **Relevance:** AI must not discriminate or infringe on individual rights.
- **Examples:** Avoiding bias in recruitment algorithms or service delivery tools.

4. Consumer Law: Fair Trading Act 1986 and Consumer Guarantees Act 1993

- **Relevance:** AI-generated content or decisions must not mislead or deceive.
- **Examples:** Automated customer service or product recommendations must be accurate and fair.

5. Copyright Act 1994

- **Relevance:** AI systems must respect intellectual property rights, especially when training on third-party content.
- **Examples:** Using copyrighted datasets or generating derivative works.

6. Employment Relations Act 2000

- **Relevance:** AI tools used in HR or performance management must comply with employment law.
- **Examples:** Transparency in automated decision-making affecting staff.

7. Health and Safety at Work Act 2015

- **Relevance:** AI systems used in operational environments must not introduce safety risks.
- **Examples:** Autonomous systems in energy generation or field operations.

8. Companies Act 1993

- **Relevance:** Directors need to be across these to make sure that they are exercising due care and upholding their legal and ethical obligations.
- **Examples:** Duty of care.

9. Māori Data considerations.