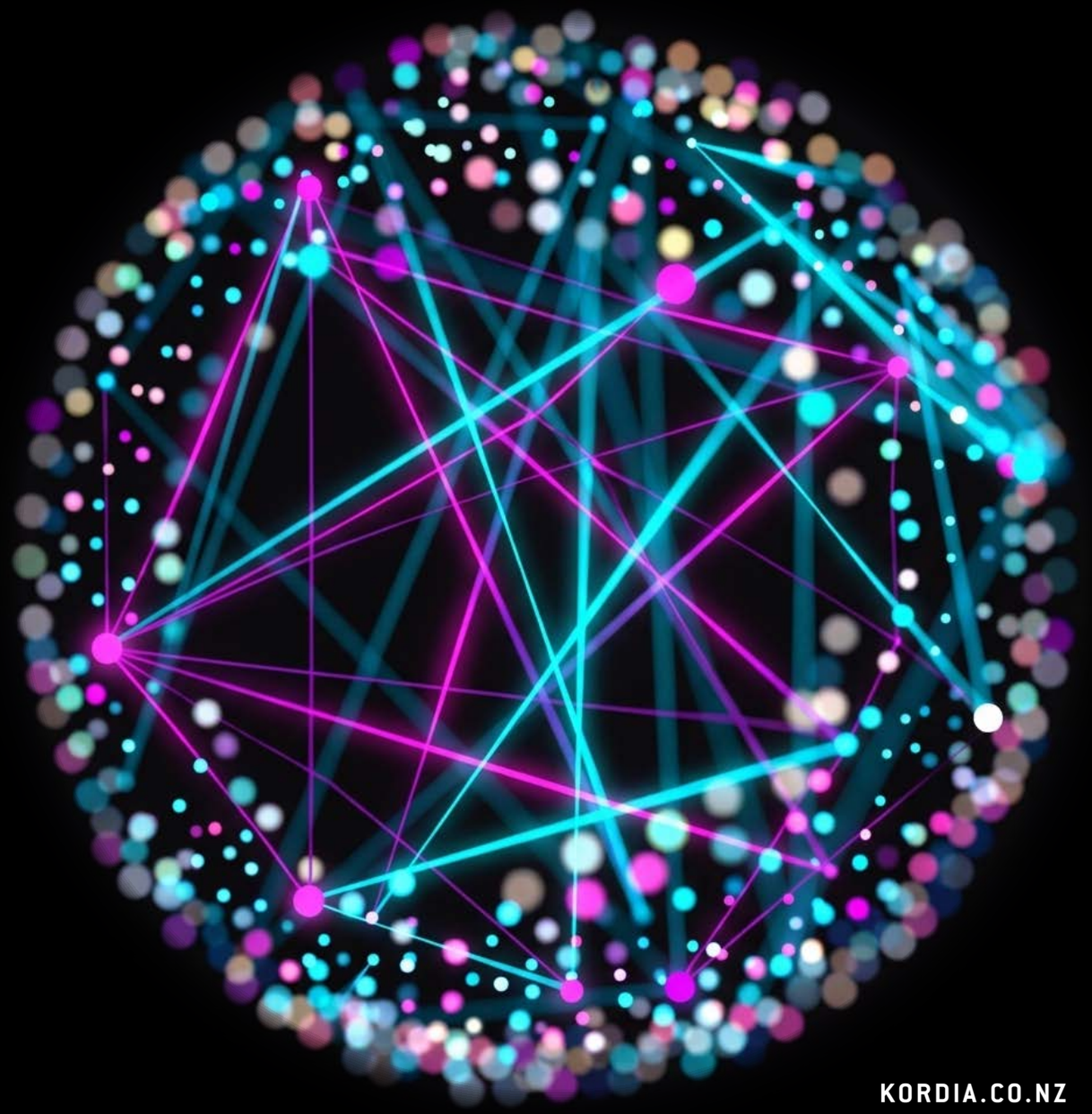
AI Usage Policy Checklist

Autumn 2026 update



kordia®

KORDIA.CO.NZ

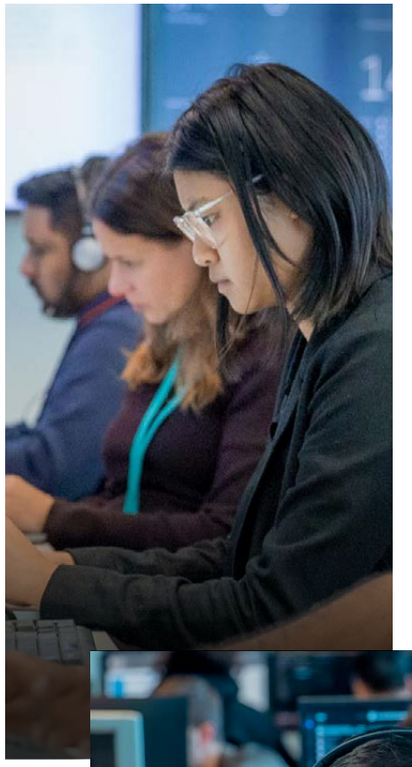
Introduction

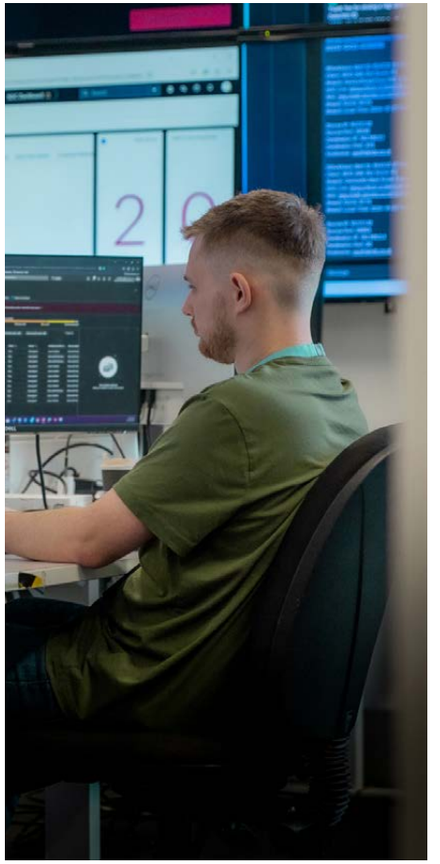
Generative AI (GenAI) tools are no longer experimental. AI features are being added into versions of everyday software and cloud services, not just obvious GenAI chatbots. Misuse can lead to data loss, privacy breaches, copyright breaches, and biased or misleading outputs, plus sophisticated AI-driven attacks can be harder to spot.

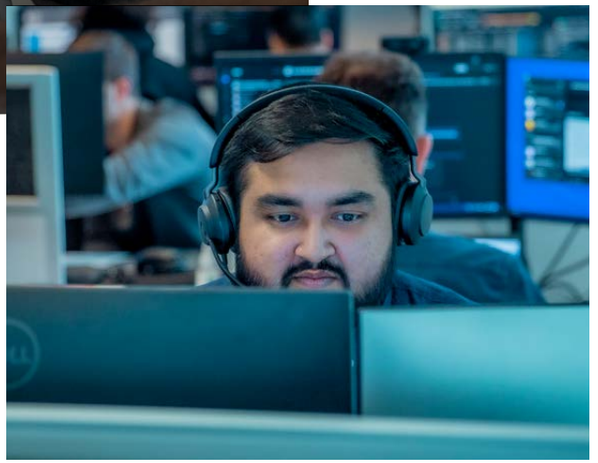
In 2025 almost half of large organisations in New Zealand suffered a cyber incident, with 45 percent of attacks involving email phishing, and a further 6 percent using voice or video deepfakes to trick staff. Almost 1 in 6 incidents involved an AI vulnerability or misuse, and 24 percent of business leaders now rate improper use of AI within their organisation as a top challenge to improving cyber security. So, socialising a clear AI Usage Policy is an important step in safeguarding your organisation, your staff and your customers from emerging risks.

It is also important to recognise that AI laws and expectations differ across jurisdictions such as the United States, China and Europe, with varying approaches to surveillance, data access and intellectual property. New Zealand organisations must understand which regimes apply to their AI suppliers and data.

This Checklist is a practical place to start. It is not a full AI management system, but it reflects current good practice in AI governance and security, and it is consistent with recent frameworks such as ISO/IEC 42001 and the OWASP AI Maturity Assessment model. You can use it to shape your own AI Usage Policy, set expectations for staff, and begin building a safe, ethical and resilient approach to AI across your organisation.







Structuring your AI policy

Scope & objectives

The first step is to understand how and why AI might be used in your organisation – and by who. Employees may want to use AI for a range of different tasks, from drafting emails and transcribing meeting minutes, through to generating code, analysing data and summarising documents. It may be sensible to keep your policy confined to the business cases where AI provides value, and to restrict other AI usage until the risks are understood and managed.

Ensure you cover off:

- Defined business cases where the organisation sees value in using AI
- General employee use of public or third-party AI tools
- AI features in SaaS, cloud and security tools used by IT and business teams
- Use by technical teams and developers, for coding assistance, testing, automation, etc.
- What types of AI systems and providers are approved for use, and at what level of data sensitivity
- Any AI uses that are explicitly prohibited; for example, certain high-risk decisions or data types

Definition example

Artificial Intelligence (AI): A computer system that can use a neural network to analyse data and come up with reasoned responses to queries based on provided data.

Machine Learning (ML): A subset of AI that concentrates on the use of algorithms that improve through iterative use.

Deep Learning (DL): A subset of ML in which artificial neural networks that mimic the human brain are used to do unsupervised complex tasks.

For a more extensive list of terms visit our AI glossary

AI TERMS EXPLAINED

Structuring your AI policy cont.

Responsibilities & expectations

Set some guidelines on how your employees should approach AI. For example:

- Set out clear rules on how your employees should approach AI, and who is accountable for decisions about AI use.
- All employees are to have a defined business case and appropriate management signoffs before using an AI system in their work.
- Before using any public or third-party AI tool, its T&Cs and privacy policy should be checked to understand who can access your data, how it may be stored or reused, and whether your data, prompts or outputs may be used to train the supplier's models.
- The IT and data teams must first understand and assess how any tools or services they bring into the business use AI, how the AI components were trained, and what data they can access. This usually involves a security and risk assessment.
- If an individual or team decides to create or configure their own AI system, they must ensure training data is appropriately governed and documented, and that datasets are selected to minimise unfair bias and reflect the organisation's customers and users, including Māori and other under-represented groups.
- Users of AI tools should be aware that the way they phrase prompts can introduce bias and should therefore avoid wording that steers the system towards a desired conclusion.
- The CIO is to make the final decision on the usage or purchase of significant AI systems and tools, especially high-risk AI that processes personal, sensitive or regulated data.

Employee usage

This section should clearly state the rules that employees need to follow when interacting with an AI system. For example:

Do not's

- Paste or copy any company, partner or customer source code or configurations into an AI tool.
- Paste any confidential, sensitive or personal data, including internal email trails and credentials, into an AI tool.
- Paste strategic documents, business processes or internal workflows into public or unapproved AI tools.
- Rely on AI-generated responses and content without first sanity-checking or peer-reviewing them for reasonableness and accuracy.
- Give an AI tool access to data that has not been explicitly put in scope for the specific project or business case.
- Trust unexpected messages, emails or calls at face value: AI is increasingly being used to create convincing phishing emails and voice or video deepfakes.

Do's

- Review any Licence Agreement or Terms of Use before using any public or unapproved AI system and only use systems in a way that abides by these agreements.
- Get advice from your manager – or from information security, data, privacy, legal or other domain owners – if you aren't sure about the risks involved in using AI systems at work.
- Treat AI-generated predictions (such as financial forecast data or behavioural risk scores) with scepticism – they're indicative, not fact, and should support your best judgement.
- Report any suspected AI-related security or privacy issue (such as a deepfake video, unusual AI behaviour, or an apparent AI data leak) through your regular incident reporting channels.

Organisational usage

This section should set out the rules that the organisation and employees need to follow when purchasing or developing an AI/ML system. For example:

Do not's

- Accept marketing material about AI as accurate – always verify claims, take up references, and check how the system actually works in your environment.
- Use AI systems that store or process sensitive, personal or Māori data in jurisdictions where you do not understand the legal and sovereignty implications, including whether foreign governments can compel access to your data.
- Integrate an AI system with company systems without express signoffs from the data owners, information security and privacy, and without completing any required supplier and security risk assessments and Privacy Impact Assessments (PIAs).
- Start a company-wide AI project without clear objectives, expected Return on Investment (ROI), and simple metrics for success and safety (for example, accuracy, error rates, bias, and incident reporting).
- Tie yourself into a single AI model or provider without considering portability and exit options. This is such a rapidly evolving area that a tool you build your processes around can quickly become obsolete, change terms, or become too expensive.

Organisational usage cont.

This section should outline suggested guidelines that the organisation and employees should follow when purchasing or developing an AI/ML system. For example:

Do's

- Follow standard business case criteria for AI initiatives and ensure signoffs from data governance, information security, privacy, and relevant business owners.
- Understand the cost model – including data transfer, storage and inference costs – so you can manage AI spend over time.
- Start small, measure outcomes and risks, learn from successes and failures, but scale only when there is evidence that the AI system can safely and reliably deliver value.
- Consider data location, jurisdiction and data sovereignty when selecting AI suppliers; understand where data will be stored and processed, what foreign laws may apply (for example, US CLOUD Act–style access), and whether NZ-based or NZ-governed options are more appropriate for sensitive or Māori data.
- Be aware that AI suppliers operate under different legal and cultural regimes (for example, US, EU and Chinese approaches to surveillance, IP and data access), and factor this into procurement, data sovereignty and IP risk decisions.
- Conduct a Privacy Impact Assessment (PIA) and appropriate supplier and security risk assessments for any AI system that will process personal, sensitive or regulated data.
- Select systems that let your organisation retain ownership and control of its data and intellectual property, and that provide clear documentation about how models are trained and used.
- When developing or training AI systems, anonymise sensitive data where possible, use representative datasets, and check for unfair bias in training data and outputs.
- Rigorously test AI systems before and during implementation, so you can understand their accuracy, limitations and biases, and put countermeasures in place before making commercially significant changes.
- Verify the terms of any copyright or third-party intellectual property before including such content in training data or prompts.
- Provide onboarding and training to staff using AI systems – be sure to cover appropriate use, security and privacy obligations, and when to escalate concerns.
- Ensure any client or staff member interacting with an AI system is aware of that fact and can easily reach a human, if needed.
- Plan for regular updates, retraining and software patching of AI platforms, and assess all changes (to the AI engine, rules, syntax or underlying components) for security, privacy and business impact before deployment. Specialised development and testing skills may be required for this.
- Monitor developments in legislation, regulation and industry codes of practice, and be prepared to adjust or withdraw AI systems, if required.

Measurement & evaulation

It is worthwhile putting some measurements in place to gauge the effectiveness of your AI usage and policy. Consider implementing the following metrics:

- Number of hours saved by AI doing an existing task previously done by a human
- Number of tasks the AI can undertake that no one could have done previously
- Number of AI systems recorded in the organisation's internal AI register or inventory
- Number of tools using AI that are reviewed and approved by <X> before use, each month
- Number of times a month a staff member is found to be using an unsanctioned AI tool (Shadow AI).

You can also ask a small set of yes/no questions twice a year to assess your organisational maturity:

- Do we have a clear, communicated AI Usage Policy that staff understand?
- Do we train staff on safe and appropriate AI use, including AI-enabled phishing and deepfakes?
- Do we track our high-risk AI use cases, and complete AI-specific risk and privacy assessments for them?
- Do we have defined processes for monitoring AI systems and responding to AI-related incidents?

Next Steps

Kordia and our independent consultancy - Aura Information Security - have specialist capability to help you assess, plan and implement AI into your organisation in an ethical and secure manner.

Last updated: March 2026, by Aura Information Security, and based on findings in Kordia's New Zealand Business Cyber Security Report 2026.

Further reading & references

New Zealand guidance & standards

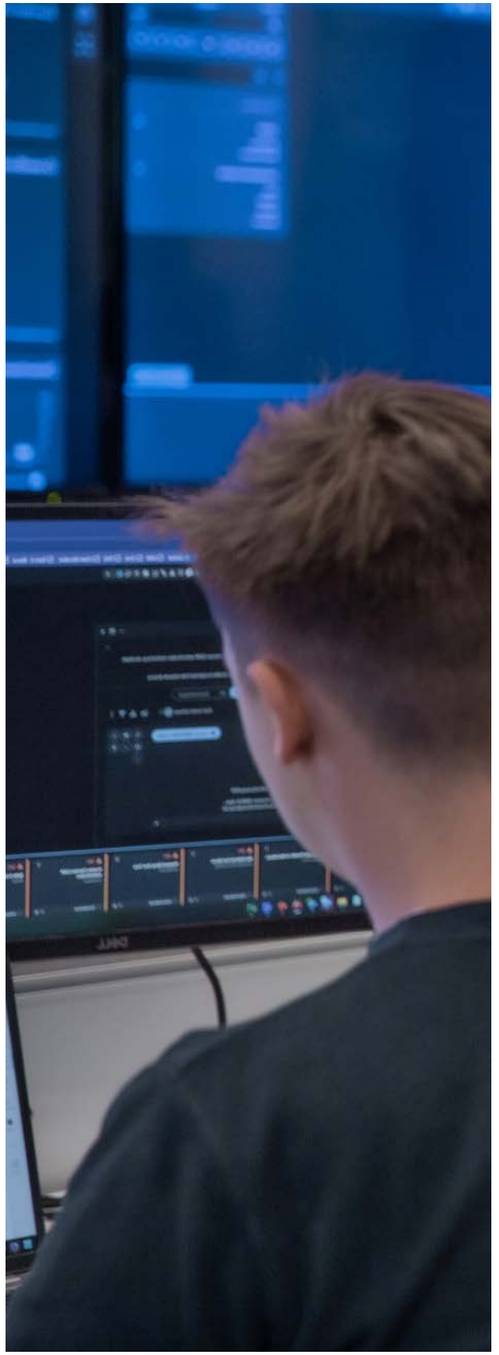
- Ministry of Business, Innovation & Employment (MBIE), Responsible AI Guidance for Businesses: Investing with Confidence, July 2025.
- New Zealand Government, New Zealand's AI Strategy and Guidance for Business.
- National Cyber Security Centre (NCSC NZ) and partners, Guidelines for Secure AI System Development and Deploying AI Systems Securely.
- Office of the Privacy Commissioner (NZ), Guidance on Artificial Intelligence and the Privacy Act 2020.
- Stats NZ, Algorithm Impact Assessment Toolkit.
- Kordia's New Zealand Business Cyber Security Report 2026.

International guidance & standards

- ISO/IEC 42001:2023, Artificial Intelligence – Management System.
- OWASP Foundation, OWASP AI Maturity Assessment (AIMA), Version 1.0, 2025.

AI governance material for boards

- Institute of Directors in New Zealand, A Director's Guide to AI Board Governance, July 2024.
- Institute of Directors in New Zealand, Governing in an AI world.
- Australian Institute of Company Directors & Human Technology Institute (UTS), A Director's Guide to AI Governance, 2024.




kordia®
KORDIA.CO.NZ