26 September 2025

VEDGE New Zealand Limited
Insurance Resources Limited New Zealand

Technology, Artificial Intelligence, and Data Governance Policy V1.2

Purpose

- This policy establishes a comprehensive framework for the responsible use, management, and governance of technology, artificial intelligence (AI), and data at VEDGE New Zealand Limited (VNZ) & Insurance Resources Limited (IRL) New Zealand.
- It ensures alignment with international standards including ISO/IEC 42001 for AI management systems, NIST AI Risk Management Framework (RMF), GDPR for data protection, the EU AI Act for AI regulation, and ISO 27001 & SOC 2 for system and organization controls, to mitigate risks, protect stakeholder interests, and maintain compliance in the rollout of software such as ObliX for insurance brokers.
- The policy addresses the critical intersection of AI governance and insurance coverage, emphasizing that AI mistakes are not covered without documented proof of human oversight, risk management, and ethical deployment.

Scope

- Applies to all employees, contractors, and third-party vendors involved in the development, deployment, use, or oversight of technology, AI systems, and data processing at IRL, including but not limited to insurance brokerage workflows, client data handling, and decision-support tools.
- Covers all AI-enabled technologies, such as ObliX, used for tasks like data analysis, risk scoring, policy drafting, or client interactions, where errors could lead to financial, legal, or reputational harm.
- Excludes non-AI technologies unless they interface with AI systems or involve sensitive data governed by this policy.

Definitions

- **Artificial Intelligence (AI)**: Systems that perform tasks requiring human-like intelligence, including machine learning, predictive analytics, and automated decision-making, as defined under the EU AI Act.
- **Data Governance**: The processes for ensuring data quality, security, privacy, and compliance, incorporating GDPR principles of lawfulness, fairness, and transparency.
- **High-Risk AI Systems**: AI applications with potential for significant harm, such as those affecting financial decisions or client outcomes, requiring enhanced controls per NIST AI RMF and EU AI Act.
- **Human Oversight**: Mandatory review by qualified personnel to validate AI outputs, preventing negligent delegation as highlighted in insurance coverage considerations.

Governance Structure

- **Chief Technology and Data Officer (CTDO) Responsibilities**: Rick Lim, as CTDO, oversees policy implementation, appoints an AI Governance Committee, and ensures annual reviews for alignment with evolving standards like ISO 42001 and SOC 2.
- **AI Governance Committee**: Comprising representatives from IT, legal, compliance, and operations, responsible for risk assessments, impact evaluations, and approval of AI deployments.

- **Independent Audits**: Annual bias and fairness audits by external auditors, testing for disparate impact using tools like SHAP and LIME, with results publicly disclosed on the IRL website, including tool distribution dates.

Key Principles

- **Risk Management**: Adopt a structured approach per NIST AI RMF to identify, assess, mitigate, and monitor AI risks across the lifecycle, including mapping potential harms, measuring performance, and managing model drift.
- **Ethical AI Use**: Align with ISO 42001 by establishing boundaries for AI as a supportive tool, not a replacement for human judgment, emphasizing responsibility, transparency, and avoidance of prohibited practices under the EU AI Act (e.g., manipulative or exploitative AI).

- **Data Protection and Privacy**: Comply with GDPR by ensuring lawful data processing, minimizing collection, implementing pseudonymization where feasible, and conducting Data Protection Impact Assessments (DPIAs) for AI systems handling personal data.
- **Security and Controls**: Meet ISO 27001 & SOC 2 criteria for security, availability, processing integrity, confidentiality, and privacy through role-based access controls (RBAC), multi-factor authentication (MFA), and adversarial protection measures like Counterfit.
- **Transparency and Explainability**: Require public disclosure of AI involvement in workflows, including when AI influences judgments, touches client data, alters costs, or poses bias risks, to safeguard trust, compliance, and insurance coverage.
- **Human-Centric Approach**: Mandate human oversight for all high-risk AI outputs, with documentation proving reviewer accountability, as insurers prioritize evidence of governance over vendor assurances.

AI Use and Management

- **AI Use Policy**: AI tools, including ObliX, are permitted only for preliminary tasks such as drafting summaries or calculating initial scores; they are explicitly prohibited for final decisions, legal advice, or client-facing outputs without licensed review.
- **Review Log**: Maintain a digital AI Review & Oversight Log with columns for Date, AI Tool, Task, Reviewer, and Final Action Taken; entries are required for any decision with legal, financial, or client impact, ensuring proof of oversight for insurance claims.
- **Red Flag Rule**: Immediately halt AI use and escalate for licensed review if outputs exhibit missing data, low confidence, biases, or conflicts; this rule must be posted, initialed by staff, and integrated into onboarding.
- **Deployment Requirements**: Prior to rollout, conduct impact assessments per ISO 42001, ensure data quality and governance under EU AI Act, and verify compliance with NIST functions (Govern, Map, Measure, Manage).
- **Incident Response**: Establish protocols for post-deployment monitoring, including model performance tracking and rapid response to biases or errors, with reporting to the AI Governance Committee.

Data Governance

- **Data Sovereignty and Integrity**: Implement stringent measures to secure data storage, access, and transfer, ensuring privacy and integrity in line with GDPR and ISO 27001 & SOC 2 privacy criteria.
- **Data Minimization and Quality**: Collect only necessary data for AI training/validation, apply governance practices to prevent biases, and use high-quality datasets as required by EU AI Act for high-risk systems.
- **Access Controls**: Enforce RBAC and MFA for all data-handling systems, with regular audits to detect unauthorized access or breaches.
- **Compliance Reporting**: Document and report data usage in AI contexts, including to insurers upon request, to confirm coverage for AI-related incidents.

Compliance and Auditing

- **Standards Alignment**: Integrate ISO 42001 for AI management, NIST AI RMF for risk handling, GDPR for data rights (e.g., right to explanation for automated decisions), EU AI Act for risk classification, and ISO 27001 & SOC 2for operational controls.
- **Annual Reviews**: Conduct internal audits and external certifications, with public disclosure of results to demonstrate ongoing compliance.
- **Insurer Communication**: Proactively query insurers on AI coverage, documentation needs, and tool reporting, attaching policy artifacts for record.
- **Training and Enforcement**: Provide mandatory training on this policy, with violations subject to disciplinary action to ensure adherence.

Best Practices

- Establish a dedicated AI Governance Binder or digital folder containing the policy, logs, and insurer correspondence for quick access during audits or claims.
- Use explainability tools (e.g., IBM AI Fairness 360) routinely to audit for biases and ensure fairness in insurance applications.
- Foster a culture of disclosure by training staff to respond affirmatively to queries on AI use, reinforcing that transparency protects trust and coverage.
- Integrate AI governance into vendor contracts for tools like ObliX, requiring ISO 27001 & SOC 2compliance and shared risk assessments.
- Monitor regulatory updates to standards like the EU AI Act and NIST AI RMF, updating the policy within 90 days of changes.
- Conduct quarterly simulations of AI incidents to test response plans, enhancing preparedness for real-world errors.
- Collaborate with external experts for independent audits, ensuring objectivity in bias testing and disparate impact analysis.
- Prioritize human oversight in all AI workflows, documenting decisions to avoid "negligent delegation" claims from insurers.
- Leverage data governance platforms to automate compliance tracking, reducing administrative burden while maintaining ISO 27001 & SOC 2and GDPR alignment.
- Encourage ethical innovation by rewarding staff contributions to AI improvements that enhance fairness and reliability.

Key Best Practices for Data Management in Insurance Brokerage

- **Establish a Strong Data Governance Framework**: Implement structured policies for data quality, stewardship, and compliance, aligning with standards like GDPR or local regulations to simplify audits and reduce penalties. This includes defining roles for data owners and conducting regular governance reviews to address issues like data silos or inconsistencies.
- **Adopt Master Data Management (MDM)**: Centralize client, policy, and risk data into a single, accurate source of truth to ensure consistency across systems. This strategic imperative helps brokers avoid errors in underwriting or claims processing and supports scalable growth.
- **Leverage Data Analytics and AI Tools**: Use analytics platforms to derive insights from client data for personalized recommendations, risk scoring, and trend forecasting. Start with simple implementations like dashboards for policy renewals, ensuring human oversight to maintain ethical standards and avoid biases.
- **Automate Data Processes**: Integrate AI-driven automation for tasks like data entry, validation, and reporting to streamline workflows, reduce manual errors, and improve efficiency. Focus on tools that handle high-volume data from quotes to claims while maintaining audit trails.
- **Prioritize Data Security and Ethical Practices**: Enforce encryption, access controls, and incident response plans to protect sensitive client information. Build on four ethical pillars—transparency, fairness, privacy, and accountability—to foster trust and comply with regulations, including regular employee training on data handling.
- **Mitigate Risks Through Continuous Monitoring**: Regularly assess data for quality and biases, using tools for risk management that combine technology with traditional methods. This includes monitoring for operational risks and ensuring data-driven decisions are documented for insurance coverage purposes.

By focusing on these practices, insurance brokers can transform data from a mere asset into a competitive advantage, ultimately leading to better client outcomes and business resilience.

Signed

VEDGE NZ Limited – Chief Technology and Data Officer, CTDO

INSURANCE RESOURCES Limited – Managing Director