Artificial Intelligence Governance and Responsible Use Policy

Organisation	Suppeco Limited
Document Owner	Chief Executive Officer
Operational Owners	Technology, Information Security and Product Leadership
Version	1.0
Classification	Internal / Customer Assurance
Approval Status	Approved
Review Frequency	At least annually and following material regulatory, technological or business change

1. PURPOSE

1.1 Suppeco Limited ("Suppeco") recognises that Artificial Intelligence ("AI") can create significant operational, analytical and commercial value when it is developed and used responsibly.

1.2 This Policy establishes Suppeco's governance framework for the responsible development, procurement, deployment and use of AI.

1.3 Its purpose is to ensure that AI is used:

(a) for a defined and legitimate business purpose;

(b) with appropriate human accountability and oversight;

(c) securely and in accordance with Suppeco's information security requirements;

(d) in compliance with applicable law, regulation and contractual obligations;

(e) with appropriate consideration of privacy, fairness, transparency and potential harm;

(f) using proportionate risk assessment and approval processes;

(g) with appropriate monitoring throughout the AI lifecycle; and

(h) in a manner that allows users, customers and other affected stakeholders to raise concerns or provide feedback.

1.4 AI must support human decision-making and business outcomes without undermining accountability, security, confidentiality or trust.

2. SCOPE

2.1 This Policy applies to all Suppeco directors, employees, contractors, consultants and other personnel using AI on behalf of Suppeco.

2.2 It applies to:

(a) AI developed by or on behalf of Suppeco;

(b) AI capabilities incorporated within Suppeco products and services, including SuppEQ;

(c) third-party AI services, models, platforms or components used by Suppeco;

(d) AI used internally for business operations;

(e) machine learning, predictive analytics, natural-language processing and related intelligent technologies;

(f) AI functionality embedded within third-party software;

(g) AI-assisted development, analysis, research, content generation or decision support; and

(h) material changes to an existing AI capability or its intended use.

2.3 This Policy applies across the complete AI lifecycle, from initial business case and design through procurement, development, testing, deployment, operation, monitoring, modification and retirement.

3. POLICY PRINCIPLES

3.1 Suppeco applies the following principles to AI.

3.2 Human accountability

3.2.1 Accountability for an AI-enabled process always remains with an identifiable person or business owner.

3.2.2 Responsibility must not be delegated to an algorithm, model or automated system.

3.2.3 Where AI materially informs commercial, contractual, supplier, employment, security, legal or other significant decisions, appropriate human review must be retained.

3.3 Purpose and proportionality

3.3.1 AI must have a clearly defined business purpose.

3.3.2 Its anticipated benefit must be proportionate to its associated risks, complexity and potential impact.

3.3.3 AI should not be introduced solely because the technology is available where an established lower-risk approach would reasonably achieve the required outcome.

3.4 Security and confidentiality

3.4.1 AI must be used in accordance with Suppeco's information security framework.

3.4.2 Confidential, commercially sensitive, security-classified, personal or customer information must not be entered into an unauthorised AI service.

3.5 Privacy and data protection

3.5.1 Personal data used within AI systems must be processed lawfully, fairly and transparently, with appropriate consideration given to:

(a) purpose limitation;

(b) data minimisation;

(c) accuracy;

(d) retention;

(e) security;

(f) data subject rights;

(g) international data transfer requirements; and

(h) risks to the rights and freedoms of individuals.

3.5.2 Where required, a Data Protection Impact Assessment ("DPIA") or equivalent assessment must be completed before deployment.

3.6 Fairness

3.6.1 AI must not knowingly be designed or deployed in a manner that unlawfully discriminates against individuals or groups.

3.6.2 Potential bias must be considered when relevant to the use case, data, outputs and affected population.

3.7 Transparency and explainability

3.7.1 Suppeco will provide an appropriate level of transparency regarding the use of AI, proportionate to the nature and impact of the use case.

3.7.2 Where AI materially contributes to a recommendation, assessment or decision, users should be able to understand the purpose of the AI and the appropriate limitations of its output.

3.8 Reliability and accuracy

3.8.1 AI output must not automatically be assumed to be factually correct.

3.8.2 Appropriate validation, testing and human review must be applied according to the consequences of an inaccurate, incomplete or misleading output.

3.9 Contestability and feedback

3.9.1 AI-enabled processes must provide an appropriate mechanism for users or affected parties to:

(a) question an AI-supported outcome;

(b) report suspected errors;

(c) identify potential bias;

(d) raise concerns about inappropriate behaviour;

(e) report security or privacy concerns; and

(f) provide positive, negative or unanticipated feedback.

3.9.2 Feedback will form part of Suppeco's ongoing monitoring and continuous improvement process.

4. AI GOVERNANCE

4.1 Executive accountability

4.1.1 The Chief Executive Officer retains executive accountability for Suppeco's organisational approach to AI.

4.1.2 The CEO is responsible for ensuring that:

(a) appropriate AI governance arrangements exist;

(b) material AI risks are understood;

(c) appropriate resources are assigned;

(d) unacceptable AI risks are not knowingly accepted without executive review; and

(e) this Policy remains appropriate to Suppeco's business and regulatory environment.

4.2 AI Governance Lead

4.2.1 Suppeco shall nominate an AI Governance Lead responsible for coordinating implementation of this Policy.

4.2.2 Responsibilities include:

(a) maintaining the AI Systems Register;

(b) coordinating AI use-case assessments;

(c) assigning or confirming AI risk classifications;

(d) ensuring required reviews and approvals occur;

(e) maintaining AI governance documentation;

(f) monitoring relevant AI regulatory and standards developments;

(g) coordinating periodic reviews of deployed AI;

(h) receiving and coordinating investigation of AI-related feedback or concerns; and

(i) escalating material AI risks to executive management.

4.2.3 The AI Governance Lead may delegate individual activities but retains responsibility for governance coordination.

4.3 Technology and Product

4.3.1 Technology and Product owners are responsible for:

(a) establishing the technical design of AI capabilities;

(b) documenting intended system behaviour;

(c) evaluating model and technology dependencies;

(d) establishing testing and acceptance criteria;

(e) ensuring appropriate access controls and technical safeguards;

(f) defining human oversight requirements;

(g) implementing monitoring;

(h) managing material changes; and

(i) maintaining appropriate technical documentation.

4.4 Information Security

4.4.1 Information Security responsibilities include:

(a) security assessment of material AI implementations;

(b) assessment of data handling and access;

(c) supplier security due diligence where appropriate;

(d) credential and identity management;

(e) vulnerability and threat assessment;

(f) monitoring security implications of AI use; and

(g) coordinating AI-related security incidents through Suppeco's established incident-management processes.

4.5 Business or Use-Case Owner

4.5.1 Every material AI use case must have a named owner.

4.5.2 The owner is accountable for:

(a) defining the business objective;

(b) demonstrating the need for the proposed use;

(c) identifying affected stakeholders;

(d) identifying intended and foreseeable unintended uses;

(e) defining acceptable output quality;

(f) ensuring appropriate human oversight;

(g) understanding operational consequences;

(h) monitoring the AI following implementation; and

(i) escalating material issues.

4.6 Users

4.6.1 All users of AI must:

(a) use only authorised AI services for Suppeco business;

(b) comply with information classification requirements;

(c) understand that AI output may contain errors;

(d) exercise appropriate professional judgement;

(e) validate material outputs before reliance;

(f) avoid misrepresenting AI-generated information as independently verified fact; and

(g) report suspected inappropriate AI behaviour, data exposure, bias, security incidents or material inaccuracies.

5. AI SYSTEMS REGISTER

5.1 Suppeco shall maintain a proportionate register of material AI technologies used, developed or deployed by the organisation.

5.2 The register should contain, where applicable:

(a) AI system or service name;

(b) description and intended purpose;

(c) business owner;

(d) technical owner;

(e) provider;

(f) data types processed;

(g) customer-data involvement;

(h) affected stakeholders;

(i) internal risk classification;

(j) applicable legal or regulatory considerations;

(k) human oversight arrangements;

(l) approval status;

(m) approval date;

(n) significant dependencies;

(o) material restrictions;

(p) review date; and

(q) retirement date where relevant.

5.3 Experimental or proof-of-concept AI that processes no sensitive, confidential, personal or customer data may initially be recorded using a proportionate simplified process.

5.4 It must undergo full assessment before production or material business use where required under this Policy.

6. AI USE-CASE ASSESSMENT AND APPROVAL

6.1 No material AI use case may progress into production or business-critical use without appropriate assessment and approval.

6.2 The assessment must be proportionate to risk and consider the following.

6.3 Business purpose

6.3.1 The proposed use must identify:

(a) the problem being addressed;

(b) expected benefit;

(c) intended users;

(d) expected outputs;

(e) why AI is appropriate;

(f) expected operational dependencies; and

(g) criteria for determining whether the use case is successful.

6.4 Stakeholder impact

6.4.1 The assessment must consider:

(a) who may be affected;

(b) whether the AI influences decisions affecting an individual or organisation;

(c) the severity of an incorrect output;

(d) whether an affected person can reasonably challenge the outcome;

(e) potential negative or unintended consequences; and

(f) whether appropriate human intervention is available.

6.5 Data

6.5.1 The assessment must establish:

(a) what information will be processed;

(b) its source;

(c) ownership and permitted use;

(d) whether personal data is involved;

(e) whether customer confidential information is involved;

(f) whether commercially sensitive information is involved;

(g) data quality requirements;

(h) retention arrangements;

(i) whether information may leave Suppeco-controlled environments; and

(j) whether the AI provider may retain, reuse or learn from submitted information.

6.6 Accuracy and performance

6.6.1 The owner must define an appropriate approach for evaluating:

(a) accuracy;

(b) relevance;

(c) reliability;

(d) reproducibility where required;

(e) false positives or false negatives;

(f) potentially fabricated or misleading output;

(g) performance against the intended use case; and

(h) known limitations.

6.7 Fairness and bias

6.7.1 Where the use case could materially affect people, suppliers or other stakeholders, the assessment must consider whether characteristics of the data, model or process could produce systematically unfair outcomes.

6.8 Transparency

6.8.1 The assessment must determine whether users or affected parties should be informed that AI is being used and what level of explanation is appropriate.

6.9 Human oversight

6.9.1 The assessment must define:

(a) who reviews AI output;

(b) when review is mandatory;

(c) when AI recommendations may be rejected or overridden;

(d) how exceptions are handled; and

(e) who remains accountable for the resulting action or decision.

6.10 Security

6.10.1 The assessment must consider:

(a) access controls;

(b) data leakage;

(c) model or prompt manipulation;

(d) inappropriate disclosure;

(e) malicious input;

(f) external connectivity;

(g) third-party dependencies;

(h) logging;

(i) security monitoring; and

(j) relevant threat scenarios.

6.11 Supplier and technology dependency

6.11.1 For externally supplied AI, Suppeco shall consider where relevant:

(a) provider security;

(b) privacy;

(c) contractual protections;

(d) data use;

(e) data residency;

(f) availability;

(g) business continuity;

(h) model/service changes;

(i) intellectual property considerations;

(j) subcontractors;

(k) termination arrangements; and

(l) vendor concentration or dependency risk.

7. INTERNAL AI RISK CLASSIFICATION

7.1 Suppeco uses a proportionate internal classification to determine governance requirements.

7.2 These classifications are an **internal management mechanism** and do not automatically determine the legal classification of an AI system under the EU AI Act or other regulation.

7.3 Tier 1 — Low Risk

7.3.1 Examples include AI used for:

(a) brainstorming;

(b) non-sensitive drafting;

(c) summarisation of non-sensitive information;

(d) internal productivity support; or

(e) low-impact analytical assistance.

7.3.2 Approval may be provided by the Business Owner subject to compliance with approved-use requirements.

7.4 Tier 2 — Moderate Risk

7.4.1 Includes use cases involving:

(a) confidential business information;

(b) meaningful operational recommendations;

(c) customer-facing AI functionality;

(d) analysis that may materially influence business action;

(e) automated processing of significant operational datasets; or

(f) third-party AI integration into Suppeco products or services.

7.4.2 Approval requires the Business Owner and appropriate Technology, Security, Privacy or AI Governance review.

7.5 Tier 3 — Elevated Risk

7.5.1 Includes use cases capable of materially affecting:

(a) individuals;

(b) employment;

(c) contractual rights;

(d) material commercial decisions;

(e) regulatory compliance;

(f) security;

(g) significant customer outcomes;

(h) supplier sanctions or corrective actions; or

(i) other areas where incorrect or biased output could cause significant harm.

7.5.2 Tier 3 use cases require a documented assessment and executive approval, together with specialist security, privacy, legal or technical review where applicable.

7.5.3 Additional impact assessments may be required.

7.6 Tier 4 — Prohibited

7.6.1 AI use is prohibited where it:

(a) is unlawful;

(b) deliberately facilitates unlawful discrimination;

(c) intentionally deceives individuals in a materially harmful manner;

(d) circumvents required human accountability;

(e) processes information contrary to contractual or confidentiality obligations;

(f) uses customer information for unauthorised purposes;

(g) introduces an unacceptable security, privacy or legal risk; or

(h) falls within a category of prohibited AI use under legislation applicable to Suppeco.

7.6.2 Such uses may not be approved through an exception to this Policy where the activity would be unlawful.

8. PRODUCT AI AND SUPPEQ

8.1 AI functionality incorporated within Suppeco products, including SuppEQ, is subject to the same governance principles described in this Policy.

8.2 Suppeco's product AI is intended to assist users in interpreting operational information and identifying relevant patterns, insights, risks, recommendations, improvements, mitigations and other decision-support information.

8.3 AI-generated insights must be treated according to their context and materiality.

8.4 Suppeco shall maintain appropriate controls to ensure that:

(a) authorised customer data is used only for legitimate agreed purposes;

(b) access to customer information is appropriately controlled;

(c) customer data is appropriately segregated;

(d) AI output does not remove customer responsibility for business decisions;

(e) material AI functionality is tested prior to production release;

(f) material changes are governed through appropriate development and release processes;

(g) known limitations are considered in product design;

(h) feedback can be captured and investigated; and

(i) inappropriate or materially unreliable behaviour can be corrected, restricted or disabled.

8.5 Customer data must not be used to train or fine-tune a model for the benefit of unrelated third parties unless such use has been expressly authorised, is contractually permitted and is lawful.

8.6 Where third-party AI infrastructure or models form part of the service architecture, Suppeco shall apply appropriate supplier, security, contractual and technical controls proportionate to risk.

9. USE OF EXTERNAL AI TOOLS

9.1 Personnel may only use AI tools for Suppeco business in accordance with approved-use requirements.

9.2 Unless specifically approved, users must not submit the following to publicly accessible or unapproved AI services:

(a) customer confidential information;

(b) supplier confidential information;

(c) commercially sensitive information;

(d) personal data;

(e) authentication credentials;

(f) security configurations;

(g) source code;

(h) intellectual property not authorised for disclosure;

(i) controlled or security-classified information; or

(j) information subject to contractual restrictions.

9.3 Users remain responsible for any content they create, modify or distribute with AI assistance.

10. HUMAN OVERSIGHT

10.1 Human oversight must be proportionate to the impact of the AI system.

10.2 AI must not become the unreviewed sole authority for a material decision where meaningful human judgement is required.

10.3 Human reviewers must, where relevant:

(a) understand the context in which the AI output was produced;

(b) have sufficient information to challenge the result;

(c) understand relevant limitations;

(d) be able to override the AI output;

(e) be alert to automation bias; and

(f) remain accountable for decisions made.

10.4 Human review must be genuine rather than a procedural approval of an AI recommendation.

11. TESTING AND VALIDATION

11.1 Material AI functionality must undergo proportionate testing before production use.

11.2 Testing may include:

(a) functional testing;

(b) output quality assessment;

(c) accuracy evaluation;

(d) security testing;

(e) privacy assessment;

(f) misuse or abuse-case testing;

(g) bias or fairness testing where relevant;

(h) adversarial testing where appropriate;

(i) performance testing;

(j) user acceptance testing; and

(k) evaluation against predefined acceptance criteria.

11.3 The extent of testing shall reflect the potential impact of failure.

11.4 Significant test findings must be addressed or formally accepted by an authorised risk owner before deployment.

12. CHANGE MANAGEMENT

12.1 AI technology can change independently of the software in which it is embedded.

12.2 Material changes to:

(a) model;

(b) provider;

(c) architecture;

(d) data sources;

(e) training or configuration;

(f) system instructions;

(g) intended purpose;

(h) autonomy;

(i) integration;

(j) access to information; or

(k) decision-making significance

must be assessed to determine whether the original risk assessment and approval remain valid.

12.3 A material change may require reassessment and reapproval.

13. TRANSPARENCY

13.1 Suppeco will provide proportionate information about the use of AI where appropriate.

13.2 Depending upon context this may include:

(a) identification that an AI capability is being used;

(b) its intended purpose;

(c) the nature of its output;

(d) appropriate limitations;

(e) the role of human oversight; and

(f) a route for obtaining further information or raising concerns.

13.3 Transparency requirements will consider applicable regulatory, contractual and customer requirements.

14. MONITORING

14.1 AI risk management does not end at implementation.

14.2 Material AI systems must be monitored proportionately throughout their operational life.

14.3 Monitoring may include:

(a) output quality;

(b) accuracy;

(c) inappropriate responses;

(d) unusual system behaviour;

(e) security events;

(f) user feedback;

(g) customer feedback;

(h) complaints;

(i) model or provider changes;

(j) performance drift;

(k) emerging regulatory requirements; and

(l) evidence that the intended business benefit continues to be achieved.

14.4 Where monitoring identifies a material deterioration or new risk, Suppeco may:

(a) modify the system;

(b) increase human oversight;

(c) restrict functionality;

(d) suspend the use case;

(e) change the provider or model;

(f) undertake additional assessment; or

(g) withdraw the AI capability.

15. FEEDBACK, CHALLENGE AND UNANTICIPATED IMPACTS

15.1 Suppeco encourages the reporting of both positive and negative AI outcomes.

15.2 Employees, customers, suppliers and other relevant stakeholders should be able to raise concerns regarding:

(a) inaccurate AI output;

(b) misleading recommendations;

(c) suspected bias;

(d) unexpected behaviour;

(e) inappropriate content;

(f) privacy concerns;

(g) security concerns;

(h) adverse operational consequences;

(i) potential misuse; or

(j) other unintended impacts.

15.3 AI-related concerns may be raised through the appropriate Suppeco support, security, management or customer relationship channel.

15.4 Material concerns shall be recorded and assessed.

15.5 The AI Governance Lead or appropriate delegate will determine whether the issue requires:

(a) investigation;

(b) escalation;

(c) corrective action;

(d) customer notification;

(e) security incident handling;

(f) privacy incident handling;

(g) temporary suspension;

(h) risk reassessment;

(i) product change; or

(j) regulatory or legal review.

15.6 Lessons arising from incidents and feedback shall be considered as part of continual improvement.

15.7 No employee will be disadvantaged for raising a genuine concern regarding the responsible or safe use of AI.

16. AI INCIDENTS

16.1 An AI incident includes an event where an AI capability causes or materially contributes to:

(a) unauthorised disclosure;

(b) significant inaccurate or misleading output;

(c) inappropriate automated action;

(d) security compromise;

(e) privacy breach;

(f) unlawful discrimination;

(g) significant customer impact;

(h) breach of contractual obligation;

(i) loss of system control; or

(j) another material adverse consequence.

16.2 AI incidents shall be managed through Suppeco's applicable incident-management processes.

16.3 Where appropriate, the relevant AI system may be suspended or restricted while the incident is investigated.

16.4 Root cause, corrective action and lessons learned shall be documented for material incidents.

17. RECORDS AND AUDITABILITY

17.1 Suppeco shall retain records proportionate to the risk and materiality of AI use.

17.2 Records may include:

(a) AI Systems Register entries;

(b) business cases;

(c) risk assessments;

(d) DPIAs;

(e) approvals;

(f) test results;

(g) technical documentation;

(h) supplier assessments;

(i) change records;

(j) significant monitoring results;

(k) incidents;

(l) complaints;

(m) corrective actions; and

(n) periodic reviews.

17.3 Records must be maintained in accordance with applicable Suppeco retention requirements.

18. AI LITERACY AND TRAINING

18.1 Personnel using or governing AI must have an appropriate level of awareness relevant to their responsibilities.

18.2 Training and guidance may include:

(a) appropriate use of AI;

(b) limitations of AI-generated output;

(c) information security;

(d) confidentiality;

(e) privacy;

(f) recognising inaccurate or fabricated information;

(g) responsible prompt and data handling;

(h) human oversight;

(i) bias and fairness;

(j) incident reporting; and

(k) applicable regulatory requirements.

18.3 Higher-risk responsibilities may require additional role-specific competency.

19. THIRD-PARTY AI

19.1 Suppeco remains responsible for assessing material risks associated with AI supplied by third parties.

19.2 The fact that an AI capability is provided by a recognised technology provider does not remove Suppeco's obligation to consider its suitability.

19.3 Due diligence shall be proportionate to the use case and may consider:

(a) supplier maturity;

(b) security;

(c) privacy;

(d) data-processing arrangements;

(e) use of submitted information;

(f) model governance;

(g) transparency;

(h) contractual protections;

(i) availability;

(j) resilience;

(k) regulatory considerations;

(l) geographic processing;

(m) intellectual property;

(n) change notification; and

(o) exit arrangements.

19.4 Material third-party AI services must be approved before use.

20. INTELLECTUAL PROPERTY

20.1 AI users must respect copyright, licensing, confidentiality and other intellectual-property rights.

20.2 Personnel must not intentionally use AI to reproduce, disclose or misappropriate protected information where Suppeco does not have an appropriate right to do so.

20.3 Where AI-generated material is intended for material external or commercial use, appropriate review should consider:

(a) provenance;

(b) originality;

(c) confidential information;

(d) third-party intellectual property; and

(e) contractual requirements.

21. RESPONSIBLE AI FRAMEWORK ALIGNMENT

21.1 Suppeco's AI governance approach is informed by recognised international AI governance and risk-management principles, including:

21.2 ISO/IEC 42001

21.2.1 Suppeco considers principles contained within **ISO/IEC 42001:2023 — Artificial Intelligence Management Systems**, including:

(a) leadership and accountability;

(b) AI policy;

(c) risk and opportunity management;

(d) defined roles;

(e) impact assessment;

(f) lifecycle controls;

(g) monitoring;

(h) documented information; and

(i) continual improvement.

21.2.2 Unless separately and explicitly confirmed, this Policy does **not** represent a claim that Suppeco is certified to ISO/IEC 42001.

21.3 NIST AI Risk Management Framework

21.3.1 Suppeco's approach is informed by the **NIST AI Risk Management Framework (AI RMF)** and its four principal risk-management functions:

(a) **Govern**

(b) **Map**

(c) **Measure**

(d) **Manage**

21.3.2 These principles are reflected within Suppeco's approach to ownership, impact assessment, testing, monitoring and risk treatment.

21.4 EU Artificial Intelligence Act

21.4.1 Where applicable to Suppeco's activities, products or customers, Suppeco considers the **risk-based approach of the EU Artificial Intelligence Act**, including relevant requirements relating to:

(a) prohibited AI practices;

(b) risk classification;

(c) transparency;

(d) human oversight;

(e) AI literacy;

(f) governance;

(g) record keeping; and

(h) monitoring.

21.4.2 Legal classification under the EU AI Act must be assessed separately from Suppeco's internal AI risk classification.

21.5 Data Protection and ICO Guidance

21.5.1 Where AI involves personal data, Suppeco applies applicable UK data-protection requirements and considers relevant guidance issued by the UK Information Commissioner's Office concerning AI, data protection, fairness, transparency and individual rights.

21.6 Information Security

21.6.1 AI governance operates alongside Suppeco's established information-security management arrangements.

21.6.2 Information security, privacy, access control, supplier management, incident management, risk management and business continuity controls remain applicable where AI is introduced.

22. EXCEPTIONS

22.1 Exceptions to this Policy must:

(a) have a documented business justification;

(b) identify the associated risk;

(c) identify compensating controls;

(d) be time limited where appropriate; and

(e) receive approval from an appropriately authorised risk owner.

22.2 An exception cannot authorise activity that would be unlawful.

23. NON-COMPLIANCE

23.1 Failure to comply with this Policy may result in:

(a) removal of access to AI services;

(b) suspension of an AI use case;

(c) corrective action;

(d) disciplinary action where applicable;

(e) supplier remediation;

(f) contractual action; or

(g) other measures proportionate to the circumstances.

23.2 Material breaches must be escalated to appropriate management.

24. REVIEW AND CONTINUOUS IMPROVEMENT

24.1 This Policy will be reviewed at least annually.

24.2 An earlier review will be undertaken where warranted by:

(a) significant changes to Suppeco's AI capabilities;

(b) significant changes to SuppEQ;

(c) material AI incidents;

(d) changes in applicable law or regulation;

(e) significant updates to recognised standards or guidance;

(f) significant changes to third-party AI dependencies;

(g) audit findings; or

(h) material stakeholder feedback.

24.3 Suppeco will continually develop its AI governance arrangements as technology, regulation, business use and recognised good practice evolve.

APPENDIX A — AI USE-CASE APPROVAL RECORD

A.1 Each material AI use case should record, as applicable:

Ref	Assessment	Required Information
A.1.1	**Use case**	What is AI being used to achieve?
A.1.2	**Business owner**	Who is accountable?
A.1.3	**Users**	Who will use the capability?
A.1.4	**Affected parties**	Who could be affected by the output?
A.1.5	**AI technology**	What model/service/system is involved?
A.1.6	**Provider**	Internal or third-party provider
A.1.7	**Data**	What data will be processed?
A.1.8	**Personal data**	Yes / No
A.1.9	**Customer data**	Yes / No
A.1.10	**Confidential data**	Yes / No
A.1.11	**Decision impact**	What decisions or actions may the AI influence?
A.1.12	**Potential harm**	What could reasonably go wrong?
A.1.13	**Human oversight**	Who reviews or can override the output?
A.1.14	**Accuracy**	How will output quality be assessed?
A.1.15	**Bias/fairness**	Is fairness assessment relevant?
A.1.16	**Transparency**	Must users/affected parties be informed?
A.1.17	**Security**	Have security risks been assessed?
A.1.18	**Privacy**	Is a DPIA or privacy review required?
A.1.19	**Legal/regulatory**	Are specific legal requirements applicable?
A.1.20	**Third-party risk**	Has the provider been assessed?
A.1.21	**Monitoring**	How will performance and adverse impacts be monitored?
A.1.22	**Feedback**	How can concerns or errors be reported?
A.1.23	**Exit/rollback**	Can the AI be disabled or replaced if required?
A.1.24	**Internal risk tier**	Tier 1 / 2 / 3 / 4
A.1.25	**Approval**	Approved / Approved with Conditions / Rejected
A.1.26	**Approver**	Name and role
A.1.27	**Review date**	Scheduled review

APPENDIX B — AI APPROVAL DECISION

B.1 An AI use case may only be approved when the approving authority is satisfied that:

(a) there is a clear and legitimate business purpose;

(b) AI is an appropriate and proportionate means of achieving that purpose;

(c) relevant risks have been identified;

(d) the data proposed for use is authorised and appropriate;

(e) security and privacy requirements have been addressed;

(f) potential adverse impacts have been considered;

(g) appropriate human accountability exists;

(h) output quality can be evaluated;

(i) appropriate controls can be implemented;

(j) monitoring and feedback mechanisms exist;

(k) material third-party dependencies have been considered;

(l) the use complies with applicable legal, regulatory, contractual and policy requirements; and

(m) residual risk is acceptable to the authorised risk owner.

B.2 Where these criteria cannot be met, the AI use case must not be approved.

APPENDIX C — POLICY APPROVAL

Approved by	S Mydat
Role	CEO
Date	31/08/2026
Policy Owner	CTO - Operational
Next Review Date	Annually or on material change