Standards for Supplier Use of AI in the Delivery of Products and Services to SITA

Global Privacy Office

Mark Keddie, Chief Privacy & Data Protection Officer

1st September 2025

1. Introduction

Informed and responsible use of AI offers SITA the opportunity to increase efficiency, improve decision making and foster innovation. However, the benefits of AI must be carefully managed against potential risks, including data protection incidents, breaches of copyright, the misuse of confidential information, ethical considerations and compliance with wider legal obligations.

This policy applies to all suppliers, contractors and sub-contractors who use AI to support their own operations or delivery of products and services to SITA.

2.Purpose

The objectives of this policy are to:

- Ensure that the use of AI in the delivery, on-going provision and support of products and services to SITA is consistent with SITA's values and standards.
- Protect the use of SITA Data as it may be accessed, processed and stored by suppliers in the context of AI.
- Provide the mechanisms and procedures for the robust monitoring, evaluation, and reporting of the use of AI by suppliers, including timely notifications

3. Responsible AI Requirements

Suppliers are expected to follow SITA's approach to the responsible use of AI, including 'Generative AI' being AI that enables creation of new content such as text, images, audio, video and code, based on learned patterns from existing data. SITA has defined the responsible use of AI and requires:

Ethical

- You treat individuals fairly and with respect.
- You monitor your AI to ensure any outcomes are fair and free of bias.
- You take steps to identify and manage bias in AI tools and systems.
- You understand the risk of bias and take steps to mitigate it.

Purposeful

- AI will always be introduced to address a defined business challenge or opportunity.
- AI will be designed and used to empower individuals and improve their lives.
- AI should unlock value for SITA, our customers and society.
- AI will be built in such a way that it can be harnessed for good, its use and power can be controlled and can be monitored.

Honest

- You take responsibility for your actions and protect individuals, SITA and our customers against the misuse of AI.
- You ensure an appropriately trained individual has overall responsibility over the AI.
- You take steps to ensure AI training data and data sets are trustworthy and of good quality.
- You test your AI and document your findings.

Customer centric

- You are transparent about your actions as they relate to AI design and use.
- You listen to your stakeholders and customers and are transparent about how you design, develop and use AI.
- You take steps to explain how the AI you design/use works and what factors impact its output.
- You embed both security and privacy, including privacy-by-design into AI initiatives, products and services.

4. General Requirements

Suppliers who use or have AI in the provision of products or services to SITA must:

- Conduct an **impact/ and risk assessment** of their use of AI prior to its deployment or use, and periodically thereafter, to identify and address the potential risks and impacts of such systems on SITA, its customer and people.
- Ensure AI is used in a manner that **respects and protects the interests** of SITA, its customers and employees. This includes but is not limited to, rights and interests related to privacy, data protection, intellectual property, diversity and inclusion.

- Ensure use of AI is **transparent, explainable, and understandable**, and that they provide clear and accurate information and communication to SITA about their use of AI, such as its purpose, functionality, capabilities, limitations, performance, and outcomes.
- Provide clear and explainable **instructions for use** including, AI logic, training data, and decision-making processes
- Ensure that their personnel, including employees and third-party contractors, are appropriately **trained in its use of AI.**
- Have effective and accessible **mechanisms and procedures** for the oversight, review, audit, feedback, complaint, redress, and remedy of their use of AI.
- Have adequate and **appropriate measures and safeguards** to prevent, detect, and respond to any unauthorised, unlawful, or malicious access, use, modification, interference, disruption, or damage of their AI software, or the data associated with it.
- Adhere to **manufacturer's acceptable use policies** and all applicable terms and conditions in their use of AI.
- In the context of the relationship with SITA use of AI must **only be for the purposes** for which they have been designed and as necessary to provide products and services to SITA under the applicable contractual arrangements.
- Retain **records of the use** of AI and AI system performance in the provision of the product or service and make these available to SITA as required.
- Appropriate **insurance policies** in place covering their use of AI.
- Provide **termination and exit services** governing the use of SITA Data in AI systems.

5. Training Data

Suppliers must adhere to the following requirements regarding training of the AI model and the use of training data, Suppliers must:

- Provide assurances that they have secured the necessary permissions to train the relevant Large Language Model (LLM), where using third party systems.

- Warrant that the confidentiality of SITA Data is protected, and that ownership of the training data is established before any training takes place.

- Provide all information to allow SITA to make an assessment that the training data has been checked for bias, and that it is accurate and representative.

- Provide assurances that they have obtained the necessary permissions and licenses for any data used to train the AI system.

- Suppliers must provide assurances for any personal data in the training data, including that it is being processed lawfully in accordance with applicable data protection legislation, including any data processing agreement in place between the Supplier and SITA and SITAs security standards.

6. Input Data and Output Data

Suppliers must adhere to the following requirements regarding the use of input data and output data:

- Ensure that they have policies and safeguards in place governing the use of any of the following as input data, and that such policies will be made available to SITA on request:
    - SITA Data (including that of our customers)
    - Data subject to intellectual property rights
    - Data subject to additional protections or contractual restrictions
    - Any SITA Group or third-party software content, such as code or data

- Output data content, code, software or products must never be accepted, published or shared without human validation.

- Provide an intellectual property rights indemnity to cover SITA's use of any AI output, including in relation to the use of Generative AI.

7. Compliance

SITA reserves the right to monitor, evaluate, and audit the compliance of suppliers with this policy, and to request any information, data, or evidence from the suppliers to verify their compliance with this policy.

Suppliers must cooperate and collaborate with SITA in the implementation and enforcement of this policy, and must report any incidents, issues, or concerns related to the use of AI by the suppliers, or by their subcontractors, partners, or affiliates, to SITA immediately.

Suppliers must also comply with any other policies, guidelines, standards, or codes of conduct that SITA may issue or adopt in relation to the ethical and legal use of AI, as well as with any applicable laws and regulations that govern the use of AI in the relevant jurisdiction

8. Updates

From time to time this Policy may be updated and communicated to reflect external legal and regulatory requirements and/ or internal organisational changes. Suppliers must check this Policy regularly for any changes. By continuing to use AI, Suppliers agree to be bound by the updated or revised policy.

The most recent version of this Policy is 18th August 2025

If you have any questions, comments, or feedback about this policy, please contact privacy@sita.aero