SYSTEMS

GGTI Artificial Intelligence (AI) Policy: Responsible and Secure Use

Effective Date: 13/10/26

Version: 1

Reviewed By: DB

Approved By: DB

Uncontrolled document if printed or viewed outside Global GreenTag International's network
© Global GreenTag International 2026

Contents

1 Purpose 3
2 Scope 3
3 Acceptable Use 3
4 Information and Data Governance 4
5 Human Oversight 4
6 Risk Management and Compliance 4
7 Security Measures: Cyber Security and Incident Reporting 6
8 Training and Awareness 6
9 Review 6
10 References 7

Uncontrolled document if printed or viewed outside Global GreenTag International's network
© Global GreenTag International 2026

GGTI Artificial Intelligence (AI) Policy: Responsible and Secure Use

1 Purpose

The purpose of this policy is to establish the requirements for safe, responsible and secure use of Artificial Intelligence (AI) by Global GreenTag International (GGTI).

GGTI supports appropriate use of AI where it provides business benefit, whilst protecting client Information, company information, confidentiality, security, confidence and the integrity of our certification activities.

The policy is designed to ensure adherence to Australian and global legal standards, manage risks, and provide clear guidelines for employees regarding the use of AI systems.

This policy reinforces Global GreenTag's commitment to safe, responsible, ethical and secure use of AI, whilst protecting information, maintaining confidentiality and impartiality, meeting applicable regulatory and legal requirements, ensuring human review and oversight of all AI assisted work, and preserving the integrity and confidence of GGTI's certification activities.

2 Scope

This AI Policy applies to all employees, interns, contractors and other persons using AI on behalf of GGTI, including AI features built into software.

Objectives

- Ensure AI technologies are used ethically and securely.
- Comply with applicable Australian and international regulations.
- Define clear guidelines on data input and usage.
- Protect company data and systems from cybersecurity threats.

3 Acceptable Use

AI may only be used for business purposes and with tools approved by GGTI.
Examples of acceptable use:

- Drafting or improving non confidential business content
- Summarising or analysing information – when approved by CEO
- Research, brainstorming and administrative assistance (where no confidential data is entered)
- Improving productivity and internal processes
- Marketing Content and Social Media Management and Posting
- Sales Prospecting, Lead Management, Contact IDs
- Other uses as recorded in the AI Register

The AI Governance Register is in Microsoft Teams under:

Uncontrolled document if printed or viewed outside Global GreenTag International's network
© Global GreenTag International 2026

TEAM: **“Systems and Operations”**
CHANNEL: **“AI Governance Register”**
This Register outlines the tool; approved; approved by; business use; key risks; required controls; risk rating, date added; requested by; Department; status; version type Comments and review date

4 Information and Data Governance

Employees must not enter confidential, sensitive, personal, client or certification information into an AI Tool unless the tool and information have been specifically approved in writing by CEO.
AI must not be used to bypass the company’s privacy, confidential, information security, contractual or records management requirements.
When (approved) personal information is involved, applicable Australian and Internation privacy requirements must be met.
Governance effectiveness equation
Important to capture return on investment

5 Human Oversight

AI generated information must be reviewed by a competent person before it is relied on, issued externally (example: marketing materials) or used to make a business decision.
The responsible employee remains accountable for accuracy and appropriateness of AI assisted work.

6 Risk Management and Compliance

Each approved AI tool/ use case must be recorded in the AI Governance Register, including tool; approved; approved by; business use; key risks; required controls; risk rating, date added; requested by; Department; status; version type Comments and review date.
Microsoft Teams
TEAM: “Systems and Operations”
CHANNEL: “AI Governance Register”

The risk rating and controls must be appropriate to the intended use. Higher risk uses require written approval from CEO.
3 risk stacks

- Technical model failure, bias drift
- Operational risk – misuse, unapproved ai tools
- Regulatory and reputational – noncompliance

© Global GreenTag International 2026

RISK	CONTROL
Data Security – Confidential, sensitive or company information may be disclosed to an AI system or unauthorised parties	Only approved AI tools may be used for GGTI business. Confidential, sensitive, personal or client information must not be entered unless the specific tool and use have been approved and access is managed through authorised company accounts.
Privacy – Personal information may be entered, processed or retained by an AI system inappropriately.	Personal information must only be used in approved AI tools and for legitimate business purposes when approved by CEO in writing. Users must comply with company privacy requirements and applicable Australian privacy obligations.
Hallucinations – AI may generate information that is false, fabricated or unsupported but appears credible.	AI-generated information must be reviewed and verified by a competent person before it is relied upon, issued externally. Important facts, references and conclusions must be checked against reliable sources.
Bias – AI outputs may contain inappropriate, unfair or discriminatory assumptions or recommendations.	Users must exercise professional judgement and review AI outputs for potential bias or inappropriate assumptions. AI must not be the sole basis for significant decisions.
Inaccurate Outputs – AI may provide incorrect, incomplete, outdated or misleading information.	AI is treated as an assistance tool rather than an authoritative source. Outputs must be reviewed by a competent person for accuracy, completeness and relevance before being used in business.
Human Oversight – Employees may rely on AI outputs without appropriate review, professional judgement or accountability.	A competent person remains responsible for reviewing and approving AI-assisted work. AI must not replace appropriate professional judgement.
Certification Integrity / Impartiality – AI use may influence certification, audit or assessment activities in a way that compromises impartiality, consistency or confidence in certification outcomes.	**AI is not at this stage used for certification, audit or assessment decisions; this is currently prohibited by GGTI.** Additionally, until further notice, AI-assisted outputs must be independently reviewed by appropriately competent personnel, with conflicts of interest and impartiality requirements maintained.
Legal / Regulatory / IP Compliance – AI use or AI-generated content may breach applicable laws, regulations, contractual requirements,	AI must be used in accordance with applicable legal, regulatory, contractual and certification requirements. Users must verify important content and avoid using AI-generated material where

Uncontrolled document if printed or viewed outside Global GreenTag International's network
© Global GreenTag International 2026

certification requirements or third-party intellectual property rights	ownership, licensing or third-party rights are uncertain.
Cybersecurity - AI tools, integrations or AI-generated content may introduce security vulnerabilities, malicious content, phishing, malware or unauthorised access.	Only approved and appropriately configured AI tools may be used. Users must not upload or execute unknown files, code, links or content generated by AI without appropriate checks. Normal company cybersecurity controls, access controls and incident reporting requirements apply such as firewalls, intrusion detection systems (Huntress), and regular updates. Cybersecurity training for employees.

7 Security Measures: Cyber Security and Incident Reporting

Only authorised accounts and approved AI services may be used for company business.
Suspected disclosure of confidential information, privacy incidents, inaccurate AI output causing harm, security issues or other significant AI-related incidents must be reported promptly through the company's normal Cyber incident reporting process. Urgent issues should be immediately reported to Infotrust 1300 007 001.
GGTI may suspend or withdraw approval for an AI tool where risks cannot be adequately controlled.

8 Training and Awareness

Relevant employees will be made aware of this policy and the requirements for using approved AI tools. Employees are responsible for understanding the limitations of AI, including the possibility of inaccurate, misleading, biased or inappropriate outputs.

Violations of this policy may result in disciplinary action, including termination of employment. Employees are responsible for understanding and adhering to this policy and for reporting any breaches or concerns.

9 Review

The (Teams) AI Register will be maintained as GGTI's central record of approved AI use.
This policy and the (Teams) AI Register will be reviewed at least annually, or earlier if there is a significant change to AI use, legislation, customer requirements, security risks or GGTI's certification activities.

This policy applies to all AI systems, tools, and technologies used within Global GreenTag International, including but not limited to machine learning models, natural language processing tools, and other AI applications.

Uncontrolled document if printed or viewed outside Global GreenTag International's network
© Global GreenTag International 2026

10 References

Privacy Act 1988: https://www.legislation.gov.au/C2004A03712/latest/text

Australian Cyber Security Centre (ACSC) Guidelines: https://www.cyber.gov.au/about-us/view-all-content/advice-guidance-publications

General Data Protection Regulation (GDPR): https://gdpr-info.eu/

ISO/IEC 27001: https://www.iso.org/standard/27001

EVS_EN_ISO_IEC_27001;2023+A1;2024_en_Information Systems located O:\GGTI\REFERENCE_DOCS\STANDARDS_ISO, AS, NZS,SABS\ISO

Additional Sources:

ESG

EU AI Act

ASEAN AI Governance Network active

NIST AI RMF and executive orders – USA: 4 functions – Govern, Map, Measure, Manage

Generative AI regulations – China

AI Safety Institute UK

ISO 9001/ 42001 requirements

Uncontrolled document if printed or viewed outside Global GreenTag International's network
© Global GreenTag International 2026

Revision Register

Document Number	**Version 1**
Document	GGTI Artificial Intelligence (AI) Policy: Responsible and Secure Use
Original Author	TL
Current Revision Author(s)	TL

Revision	Date	Author	Notes
DRAFT	14/8/26	TL	Created draft
V1	13/10/26	TL	Updates as per DB requests: Section 3.0. Approved usage – added: Sales Prospecting, Lead Management, Contact IDs; Marketing Content; Social Media Management and Posting Section 5. 'AI must not be the sole basis for any decisions 'updated Section 6. updated: “AI is not used for certification, audit or assessment decisions at all, this is “currently” prohibited by GGTI.”

© Global GreenTag International 2026