



FTD-CMPL-004

Artificial Intelligence (AI) Usage Requirements for External Parties

Prepared for:
Prepared by:

External Parties Contracting with Fortude
Compliance Department

CONTENTS

1. INTRODUCTION.....	6
1.1 Purpose.....	6
1.2 Scope.....	6
2. POLICY.....	6
2.1 General AI principles.....	6
2.2 Approved AI usage.....	7
2.3 Prohibited use	7
3. DATA PROTECTION AND CONFIDENTIALITY	8
4. HUMAN OVERSIGHT FOR HIGH-IMPACT DECISIONS.....	8
5. SECURE DEVELOPMENT.....	8
6. AI RISK MANAGEMENT	9
7. INCIDENT MANAGEMENT	9
8. INTELLECTUAL PROPERTY (IP)	9
9. AUDIT RIGHTS	10
10. SUBCONTRACTORS	10
11. COMPLIANCE & GOVERNANCE.....	10
11.1 Compliance.....	10
11.2 Governance.....	10
12. CONTACT.....	11

DOCUMENT VERSION CONTROL

DOCUMENT CONTROL				
Document Reference Number		FTD-CMPL-004		
Effective Date		1 st JULY 2026		
Document Classification		[External]		
DOCUMENT APPROVAL				
Version	Prepared by	Reviewed by	Approved By	Date Approved
1	Neluni Kulasuriya	Shiromali Nagahawatte Surangana Sarathchandra	Shiromali Nagahawatte Arjuna Sirinanda	1 st August 2026
REVISION HISTORY				
Version	Change Description	Change Author	Change Approver	Revision Date

DEFINITIONS, ACRONYMS, AND ABBREVIATIONS

Term	Definition
Artificial Intelligence (AI)	Machine-based systems that can generate predictions, recommendations, decisions, content, or other outputs that influence physical or virtual environments, including machine learning models, Generative AI, and autonomous AI systems.
AI System	Any software or service that uses Artificial Intelligence techniques to generate outputs, make recommendations, automate tasks, analyze information, or support decision-making.
Generative AI	AI capable of creating or generating content such as text, images, audio, video, software code or other digital content based on user prompts or inputs.
AI Output	Any text, image, software code, audio, video, recommendation, analysis, or other content generated wholly or partly by an AI system.
Public AI Tool	An AI service that is publicly accessible or consumer-based and where submitted data may be retained, processed, or used to improve the service or train AI models.
Enterprise AI Tool	An AI solution provided under an enterprise agreement that includes contractual commitments regarding security, privacy, confidentiality, and data handling.
External Party	Any vendor, supplier, contractor, consultant, service provider, outsourcing partner, temporary worker, subcontractor or other third party engaged by Fortude.
Confidential Information	Any non-public information belonging to or entrusted to Fortude, whether oral, written, electronic, or otherwise, that is identified as confidential or would reasonably be understood to be confidential—including business information, Intellectual Property, source code, financial data, operational data, and Customer Information (as defined below)
Customer Information	Any information provided by, or relating to, Fortude's customers, including personal data, confidential business information, and other data processed on behalf of customers. Customer Information is a subset of Confidential Information and is subject to the same protections, in addition to any further obligations set out in the applicable customer contract.
Personal Data	Any information relating to an identified or identifiable natural person, as defined under applicable data protection laws.
Sensitive Personal Data / Special Categories of Personal Data	Personal data requiring additional protection under Applicable Law, such as health information, biometric data, genetic data, racial or ethnic origin, political opinions, religious beliefs, trade union membership, or other categories prescribed by applicable legislation.

Data Processing Agreement (DPA)	An agreement governing the processing of Personal data between Fortude and an External Party in accordance with applicable data protection laws.
High-Risk AI System	An AI system that could materially affect individuals, business operations, legal obligations, financial outcomes, cybersecurity, or regulatory compliance and therefore requires enhanced governance and oversight.
Human Oversight	Meaningful review and decision-making by an appropriately qualified individual who remains accountable for decisions supported by AI.
Intellectual Property (IP)	Patents, copyrights, trademarks, trade secrets, software, source code, databases, designs, documentation, know-how and other proprietary rights recognized under Applicable Law.
Applicable Law	All laws, regulations, standards and regulatory guidance applicable to the services provided under the relevant agreement, including those relating to privacy, cybersecurity, Intellectual Property and AI .
Security Incident	Any actual or suspected event that compromises the confidentiality, integrity or availability of Customer/Confidential Information, systems or services, including incidents involving AI systems.

1. INTRODUCTION

1.1 Purpose

This document establishes the mandatory minimum requirements governing the development, deployment and use of Artificial Intelligence (AI) by external parties engaged by Fortude. These requirements are intended to ensure that AI is used responsibly, securely, ethically and in compliance with Applicable Laws while protecting Fortude's Confidential Information, Intellectual Property (IP), customers, employees and business operations.

This policy will be reviewed at least quarterly to reflect evolving AI technologies and regulatory requirements.

1.2 Scope

These requirements form part of the contractual obligations applicable to External Parties unless otherwise agreed in writing. These requirements apply only to AI use in connection with services, deliverables or engagements performed for Fortude or Fortude's customers, including consulting and advisory engagements, and do not extend to an External Party's AI use outside the scope of its engagement with Fortude.

It applies whenever an External Party:

- Accesses Fortude systems
- Processes Fortude or Customer Information
- Develop software for Fortude
- Delivers managed services
- Uses AI to perform services for Fortude, including consulting, advisory or professional services engagements

2. POLICY

2.1 General AI principles

External Parties must ensure AI is used:

- a. Ethically
- b. Lawfully
- c. Transparently
- d. Securely
- e. Bringing in appropriate human oversight
- f. Consistent with applicable privacy laws
- g. Consistent with contractual obligations
- h. In a manner consistent with responsible and ethical AI use, including fairness, non-discrimination, and respect for human rights

The External Party remains fully responsible for all work produced using AI and the use of AI does not transfer accountability.

2.2 Approved AI usage

External Parties must not rely solely upon AI-generated outputs. All deliverables submitted to Fortude remain the responsibility of the External Party.

External Parties may only use AI:

- For activities permitted under their agreement with Fortude
- Where appropriate security controls exist
- Where confidentiality obligations are maintained
- Where outputs are reviewed by qualified personnel

External Parties shall promptly disclose to Fortude where AI has materially contributed to:

- Software code
- Architecture
- Customer deliverables
- Recommendations affecting Fortude
- Processing Customer/Confidential Information

The notification should include:

- AI tool used
- Purpose
- Nature of AI assistance
- Human review performed
- Limitations identified

Such disclosure shall be made in writing to the designated Fortude contact or project manager, at or before submission of the relevant deliverable, and shall identify the AI tool(s) used and the nature of AI involvement.

Failure to make a required disclosure shall be treated as a breach of this Policy and may result in the consequences set out in Section 11.

2.3 Prohibited use

External Parties shall not;

- Upload Fortude confidential information into Public AI Tools
- Upload Customer Information into consumer AI platforms
- Use AI tools that retain submitted data for training unless expressly approved
- Use AI to create misleading or deceptive content
- Use AI to impersonate Fortude personnel
- Generate deepfakes involving Fortude
- Use AI for autonomous decisions affecting Fortude without approval

- Use AI to bypass security controls
- Reverse engineer Fortude IP using AI

3. DATA PROTECTION AND CONFIDENTIALITY

External Parties must:

- Comply with all applicable privacy and data protection laws and regulations, including those applicable in the jurisdiction(s) in which the External Party operates and those governing the processing of Fortude or Customer Personal Data.
- Comply with all contractual privacy, confidentiality and information security obligations, including any applicable Data Processing Agreement (DPA), Non-Disclosure Agreement (NDA) or other contractual requirements.
- Implement technical and organizational security controls.
- Prevent unauthorized disclosure of Customer / Confidential Information.
- Process Personal Data only for documented and authorized purposes.

Fortude's Customer Information, Confidential Information and Personal Data must not be entered into:

- Public AI chatbots
- Free AI tools
- Consumer AI applications
- Any other AI service that has not been reviewed and approved by Fortude

Approved Enterprise AI solutions must, where applicable:

- Provide contractual privacy and confidentiality protection
- Support Zero Data Retention (ZDR), no-training, or equivalent controls to prevent submitted data from being used to train AI models
- Enforce appropriate identity and access management controls
- Encrypt data in transit and at rest
- Meet Fortude's applicable information security and privacy requirements

4. HUMAN OVERSIGHT FOR HIGH-IMPACT DECISIONS

AI must not be the sole basis for decisions that produce legal or similarly significant effects on an individual. A qualified human must review AI outputs, exercise independent judgment, and make the final decision. The reviewer must have the authority to override the AI recommendation, and the role of AI in the decision-making process must be explainable.

5. SECURE DEVELOPMENT

Where an External Party develops software, they shall ensure AI-generated code is:

- Reviewed by a qualified human

- Tested
- Security scanned
- Licensed appropriately
- Free from known vulnerabilities
- Free from known third-party IP infringement

AI-generated code shall not be deployed directly into production without first completing the review, testing and security scanning requirements set out above, including sign-off by a qualified human reviewer.

6. AI RISK MANAGEMENT

External Parties shall:

- Identify and assess AI-related risks arising from their use of AI in connection with the services that may affect Fortude, its customers or individuals
- Assess impact
- Maintain appropriate controls
- Document significant AI use
- Cooperate with Fortude assessments

Fortude may request evidence of:

- AI governance
- Risk assessments
- Security testing
- Privacy assessments

7. INCIDENT MANAGEMENT

External Parties must notify the Fortude Information Security Team (riskandsecurity@fortude.co) within 24 hours of becoming aware of any of the following incidents, or within the required timeframe under the applicable agreement.

- Unauthorized or unapproved use of AI tools.
- Exposure, leakage or unauthorized disclosure of Fortude, Customer or Confidential Information through AI.
- Security incidents involving AI systems, including AI model compromise or AI supply chain compromise.
- Prompt injection or other attempts to manipulate AI behavior.
- AI outputs that are materially inaccurate, misleading or hallucinated where they result in customer, legal, regulatory, financial, or operational impact.

8. INTELLECTUAL PROPERTY (IP)

External Parties shall ensure:

- They possess rights to AI-generated deliverables
- Outputs do not knowingly infringe third-party IP
- Fortude IP is not used to train external AI models
- Prompts containing Fortude's Customer / Confidential Information are protected

9. AUDIT RIGHTS

Upon request, vendors shall provide reasonable evidence demonstrating compliance, including:

- AI governance policies
- Approved AI tools
- Security certifications
- AI risk assessments
- Audit reports where available

Fortude reserves the right to assess compliance as permitted under the applicable contract.

10. SUBCONTRACTORS

Where subcontractors of an External Party use AI, the External Party shall ensure such subcontractors comply with requirements equivalent to this policy. The primary External Party remains fully responsible.

11. COMPLIANCE & GOVERNANCE

11.1 Compliance

External Parties shall ensure that any AI systems or AI-enabled services used in connection with services provided to Fortude are deployed, developed, used responsibly, ethically, and in compliance with all Applicable Laws and regulations, including those relating to AI, data protection, privacy, cybersecurity, IP, and anti-discrimination, as applicable in the jurisdictions in which they operate and, where applicable, the jurisdictions in which Fortude's customers are located.

11.2 Governance

External Parties shall maintain appropriate governance arrangements for use of AI, including:

- Designated ownership
- Documented approval process
- Periodic review

- Incident response
- Employee awareness
- Compliance / adherence to this policy

Fortude may request evidence of these governance arrangements in accordance with Section 9 (Audit Rights).

Failure to establish appropriate governance arrangements for AI, or otherwise to comply with this Policy may result in:

- Corrective action
- Suspension / removal of systems access
- Contractual remedies
- Termination of the agreement where appropriate
- The right to suspend AI-related services pending remediation

12. CONTACT

Questions regarding AI usage should be directed to:

- Fortude Information Security Team at riskandsecurity@fortude.co
- Fortude Compliance Team at FTD-Compliance@fortude.co

Protection of Confidential Information

This document has been prepared by Fortude and is not to be distributed, copied or reproduced without permission. The information contained in this document describes confidential information concerning Fortude services and methodology. Receipt of this document constitutes acknowledgment that this information is proprietary to Fortude recipients of this document will protect and not disclose the contents herein (and any copies thereof); including said confidential information, using the same procedures and requirements by which they protect their own proprietary and confidential information. Recipients will not, in whole or in part, disclose any of the proprietary or confidential information to any person, firm, corporation, association or other entity for any reasons or purpose whatsoever, nor shall they make use of any proprietary or confidential information for their own purposes or benefit except to the extent of Recipient's compliance with applicable open records laws.