

TestMu

Responsible AI Use and in Practice

Document ID: TMU-GRC-GDL-003

Version Number: 1.4

Statement of Confidentiality

This document contains confidential and proprietary information of TestMu Inc., d/b/a TestMu ("**TestMu/Company**"). Unauthorized use or disclosure of this information in any media is prohibited. The document represents the Intellectual Property of TestMu. No part of this document, in whole or in part, may be reproduced, stored in a retrieval system, or transmitted in any form or any means electronic or mechanical, including photocopying and recording for any purpose other than as agreed or permitted by TestMu. The information contained in this document is subject to change without notice.

Copyright © 2026 TestMu All Rights Reserved

Registered Office:

TestMu Inc. d/b/a TestMu
1390 Market Street
Suite 200 San Francisco
CA 94102.

Website: [TestMu](#)

Document Revision History

Ver #	Ver. Date	Description	Prepared By	Approved By
0.1	May 24,2025	First Draft	GRC Team	
0.2	Jun 08, 2025	Final Draft	GRC Team	
1.0	Aug 15, 2025	First Released	GRC Team	CEO
1.1	July 25,2026	2026 review & update		
1.2	Aug 28, 2026	2026 Released	GRC Team	CCO & Co-Founder
1.3	Sep 03,2026	Comprehensive enhancement of responsible AI practices, ethical use, stakeholder accountability, human oversight, data protection and risk management for public release and classification.	GRC Team	
1.4	Sep 26, 2026	2026 Revised Released	GRC Team	CCO & Co-Founder

Document Reviewers

Name	Role
[REDACTED]	Chief Executive Officer & Co- Founder
[REDACTED]	Chief Customer Officer & Co- Founder
[REDACTED]	Head of Product & Co-Founder
[REDACTED]	Chief Operating Officer
[REDACTED]	Chief Financial Officer
[REDACTED]	Group Senior Vice President, Engineering
[REDACTED]	Vice President, Human Resources
[REDACTED]	Chief Ecosystem Officer (CECO)
[REDACTED]	VP -DevOps & DevSecOps
[REDACTED]	VP of Product Management, Product
[REDACTED]	Senior Vice President, Engineering
[REDACTED]	Senior Vice President -InfoSec, Compliance & AI Governance & AIRO

Document Approvers

Name	Role	Signature	Date of sign off
[REDACTED]	Chief Customer Officer		Sep,26,2026

Table of Contents

1. OVERVIEW & INTRODUCTORY STATEMENT	5
2. PURPOSE & OBJECTIVES	5
3. SCOPE & APPLICABILITY	6
4. RESPONSIBLE AI PRINCIPLES AT TESTMU	6
5. RESPONSIBILITIES OF TESTMU & INTERESTED PARTIES	7
5.1 ROLES & RESPONSIBILITIES	7
5.2 SHARED ACCOUNTABILITY & HUMAN OVERSIGHT	9
6. ETHICAL USE & ACCEPTABLE AI PRACTICES	9
7. RESPONSIBLE AI USE BY EMPLOYEES & CONTRACTORS	9
8. CUSTOMER DATA PROTECTION & AI MODEL PROCESSING	10
9. HUMAN OVERSIGHT & AI OUTPUT VALIDATION	11
10. TESTMU-SPECIFIC RESPONSIBLE AI PRACTICES	11
11. AI SECURITY, AGENTS & THIRD-PARTY INTEGRATION	13
12. AI RISK, IMPACT & COMPLIANCE MANAGEMENT	14
13. TRANSPARENCY, ACCESSIBILITY & CUSTOMER TRUST	14
14. SHARED RESPONSIBILITIES & CUSTOMER JOURNEY	15
15. AI INCIDENT REPORTING, REMEDIATION & ASSURANCE	16
16. TRAINING, GOVERNANCE, ENFORCEMENT & CONTINUAL IMPROVEMENT	16
17. REFERENCE DOCUMENTS & PUBLIC RESOURCES	17
18. GLOSSARY OF TERMS	18

1. Overview & Introductory Statement

TestMu is committed to the **responsible, ethical, secure, transparent and accountable development, provision and use of artificial intelligence** across its Agentic AI-native Quality Engineering Platform and associated AI-enabled products and services.

This Responsible AI Use & in Practice document translates TestMu's AI Policy into practical guidance for the design, development, deployment, operation and use of AI systems.

It describes the expected conduct and responsibilities of **customers, authorized users, employees, contractors, suppliers, AI model providers, technology partners and other relevant interested parties.**

TestMu recognizes that AI can improve software testing, quality engineering, automation and business productivity. However, AI-generated outputs may be inaccurate, incomplete, biased or inappropriate for particular uses. **Responsible AI requires appropriate human judgment, data protection, security safeguards, risk management and accountability throughout the AI lifecycle.**

This document complements the [TestMu AI Terms](#), [Acceptable Use Policy](#), [Terms of Service](#) and applicable customer agreements. The AI Terms and AUP establish the relevant contractual responsibilities and restrictions for customer use.

This document provides public guidance and does not replace applicable laws or binding contractual requirements.

2. Purpose & Objectives

The purpose of this document is to establish **practical responsible AI requirements** for TestMu's AI-enabled products, services, internal operations and relevant third-party integrations.

Its objectives are to:

- **Promote ethical, lawful and authorized AI use** across TestMu's operations and customer environments.
- **Protect customer data**, personal information, intellectual property and confidential information.
- Ensure AI-generated outputs receive **appropriate human review and validation** before consequential use.
- Establish practical safeguards against AI-specific security threats, misuse and unauthorized autonomous actions.
- Promote transparency, fairness, accessibility, reliability and accountability.
- Define the responsibilities of TestMu personnel, customers, suppliers and technology partners.
- Support AI risk management, incident reporting, training, monitoring and continual improvement.

AI is intended to augment human capabilities, not replace appropriate professional judgment or organizational accountability.

3. Scope & Applicability

This document applies to the responsible development, provision, integration, operation, maintenance, testing, evaluation and use of AI systems within TestMu's established AIMS scope.

It covers relevant AI-powered products and services, including **KaneAI, Kane CLI, Test Manager, Test Intelligence, HyperExecute, SmartUI/Visual AI, accessibility-related AI capabilities, Real Device Cloud and associated AI-enabled testing, analytics, APIs and integrations**, where applicable.

It also covers approved internal AI tools used for software development, documentation, analysis, security operations, customer support and other authorized business activities.

The document applies, according to each party's role, to TestMu employees, contractors, consultants, customers, authorized users, suppliers, AI model providers, integration partners and other relevant interested parties.

TestMu acts primarily as an **AI Provider** and, where applicable, as an **AI Producer, AI Partner and AI User**. Responsibilities depend on the specific AI system, deployment arrangement, operational boundaries and applicable agreement.

Traditional automation or deterministic functionality is not automatically classified as AI. Responsible AI controls apply according to the relevant system's capabilities, intended purpose and assessed risks.

4. Responsible AI Principles at TestMu

TestMu's responsible AI practices are guided by the following principles.

4.1 Transparency & Explainability

TestMu provides appropriate information about AI-enabled functionality, intended uses, capabilities, material limitations and relevant customer responsibilities.

Where technically feasible and appropriate, documentation, logs and traceability support understanding and review of AI-generated outputs.

AI-generated content must not be represented as independently verified when it has not undergone appropriate validation.

4.2 Accountability & Governance

Responsible AI governance is maintained through **Executive Management, the AI Governance Committee, designated AI governance and risk leadership, accountable AI System Owners and relevant control functions**.

Responsibilities for AI development, use, evaluation, monitoring, incident handling and material decisions are assigned according to the AI system and applicable risk.

4.3 Fairness & Non-Discrimination

TestMu considers foreseeable discriminatory outcomes and differential impacts where relevant to an AI system's intended purpose.

Appropriate testing, monitoring and corrective measures are applied according to risk.

AI must not be used to facilitate unlawful discrimination, harassment or other prohibited treatment.

4.4 Human Oversight

AI-generated recommendations, test cases, scripts, summaries and autonomous actions require **human oversight proportionate to their intended use and potential consequences.**

Human reviewers remain responsible for validating material outputs and approving consequential decisions or actions.

4.5 Privacy & Data Protection by Design

AI systems and workflows must apply **data minimization, purpose limitation, appropriate access controls and applicable privacy safeguards.**

Personal and sensitive information may be processed only where authorized by the relevant service, agreement and applicable law.

4.6 Security & Robustness

TestMu applies risk-based safeguards against relevant AI security threats, including **prompt injection, sensitive-information disclosure, insecure output handling, unauthorized tool execution, model or retrieval poisoning and excessive agent autonomy.**

4.7 Sustainability & Ethics

TestMu considers responsible resource use, accessibility and relevant environmental and societal impacts in AI design, procurement and operation, consistent with its ESG commitments.

5. Responsibilities of TestMu & Interested Parties

Responsible AI is a **shared responsibility across TestMu's business, technology, governance and support functions**, as well as customers, employees, suppliers, AI providers, partners and other relevant interested parties. Responsibilities are assigned according to each party's role, intended AI use, operational control and applicable legal or contractual obligations.

5.1 Roles & Responsibilities

Function / Interested Party	Responsible AI Responsibilities
-----------------------------	---------------------------------

Executive Management & AI Governance Committee	Establish AI governance, approve policies and objectives, provide resources, and oversee AI risks, performance and accountability.
Product Management, Engineering & QA	Define AI systems' intended purposes, maintain ownership, integrate responsible AI by design, and conduct risk assessments, impact assessments, testing and validation.
DevOps, DevSecOps, Cloud & SRE	Implement secure AI deployment, infrastructure protection, access controls, monitoring, resilience and incident response.
Information Security, Privacy, AI Governance, & GRC	Maintain AIMS governance, oversee AI risks, security, privacy, regulatory compliance, supplier assurance, audits and incident management.
Legal	Assess applicable AI laws and regulatory obligations; review AI-related contracts, intellectual-property rights, liability, data protection provisions and third-party agreements; advise on legal risks and regulatory reporting requirements
IT	Manage approved AI tools, internal integrations, user access, information classification and secure AI use.
HR & Administration	Promote AI literacy and training, protect employee information, and ensure fairness and human oversight in AI-assisted HR activities.
Finance & Procurement	Validate AI-assisted financial outputs, protect sensitive information, and conduct appropriate AI supplier due diligence.
Sales, Marketing & Business Development	Ensure accurate AI-related representations, responsible AI-generated content, customer transparency and protection of prospect information.
Customer Success, Support & Professional Services	Guide customers on intended AI use, communicate capabilities and limitations, address feedback, and escalate AI-related incidents.
Employees, Contractors & Consultants	Use approved AI tools, protect confidential information, validate AI-generated outputs and promptly report suspected misuse or incidents.
Customers & Authorized End Users	Ensure lawful and authorized AI use, appropriate input data, access controls and human review of consequential outputs, subject to applicable agreements.
Suppliers, Third-Party AI Providers & Partners	Fulfil applicable security, privacy, confidentiality, responsible AI and contractual obligations, including agreed shared responsibilities.
Regulators, Auditors, Certification Bodies & Other Interested Parties	TestMu considers applicable regulatory requirements, independent assurance obligations and relevant stakeholder expectations.

5.2 Shared Accountability & Human Oversight

All relevant functions and interested parties must apply **responsible AI principles, appropriate human oversight, data protection, security and risk management** within their respective responsibilities throughout the AI lifecycle.

TestMu retains accountability for AI systems and controls within its organizational and technical boundaries. **Customer-managed models, infrastructure, data and integrations are governed through documented shared-responsibility arrangements**, as applicable.

Customer and third-party obligations remain subject to the applicable [AI Terms](#), [Acceptable Use Policy](#), contractual agreements and relevant laws.

6. Ethical Use & Acceptable AI Practices

AI must be used only for an **authorized purpose**, using approved accounts, permitted data and appropriate system configurations.

Users must not:

- Use AI to perform unlawful activities, harassment, exploitation or unlawful discrimination.
- Attempt unauthorized access, surveillance, data extraction or circumvention of security safeguards.
- Submit data without the necessary rights, permissions or contractual authorization.
- Use AI-generated outputs to mislead others about material facts or completed verification.
- Use autonomous agents to perform unauthorized or harmful actions.
- Rely solely on AI outputs where qualified human review is required.

High-impact or legally sensitive use cases require additional assessment and controls and may be unsupported or restricted under the applicable service terms.

Customer-facing restrictions are governed by the [TestMu Acceptable Use Policy](#).

7. Responsible AI Use by Employees & Contractors

7.1 Approved AI tools

Personnel must use **only enterprise or other AI tools approved by TestMu** for the relevant business purpose.

Approval of a tool does not automatically authorize the processing of every category of company or customer information.

7.2 Information classification

Confidential or restricted information may be processed only in approved AI environments and where the applicable **information classification, privacy, security and contractual controls** permit it.

Customer confidential information, credentials, secrets and restricted data must not be uploaded to unapproved consumer AI accounts.

7.3 Output validation

Personnel remain accountable for work performed with AI assistance.

AI-generated code, documentation, analysis, customer communications and other material outputs must be reviewed for **accuracy, security, confidentiality, intellectual-property concerns and suitability for the intended purpose.**

7.4 Consequential decisions

AI must not independently make consequential employment, legal, financial, security or other high-impact decisions where human review and authorization are required.

Established approval and escalation procedures remain applicable when AI is used to assist these workflows.

7.5 Reporting

Personnel must promptly report suspected AI misuse, unsafe outputs, unauthorized actions, privacy concerns or security incidents through established internal channels.

8. Customer Data Protection & AI Model Processing

8.1 Customer data and model training

TestMu does not use Customer Data, including test execution data, Inputs, Outputs or Usage Data, to train, retrain or fine-tune AI models made available to other customers, in accordance with its published [AI Terms](#).

Any supported customer-specific model customization is governed by the applicable contractual and authorized processing arrangements.

8.2 Data minimization

Users should submit **only the information necessary for the authorized AI task.**

Synthetic or appropriately masked test data should be used where practicable to reduce unnecessary exposure of personal, confidential or production information.

8.3 Restricted information

Passwords, API tokens, payment-card information, protected health information, classified information and other restricted data must not be submitted to AI tools unless the relevant service, agreement and organizational controls expressly permit the processing.

8.4 Third-party model processing

Certain TestMu AI features may incorporate third-party AI models, APIs or supporting services.

Model-provider processing, data-use restrictions, locations, retention and safeguards may differ by product and deployment. Relevant arrangements must be evaluated against the applicable agreement, product documentation and [Subprocessor List](#).

8.5 Prompts, outputs & generated artifacts

Prompts, retrieved content, AI-generated code, screenshots, logs, transcripts and outputs may contain sensitive information.

They must be handled according to applicable **access-control, secure-storage, retention, deletion, confidentiality and intellectual-property requirements.**

9. Human Oversight & AI Output Validation

Human oversight is a fundamental requirement for responsible AI use at TestMu.

AI-generated outputs may contain hallucinations, inaccurate assumptions, incomplete test coverage, insecure code, misleading explanations or inappropriate recommendations.

Users must apply appropriate validation before accepting or acting on material outputs.

9.1 Validation requirements

Depending on the use case, validation should address:

- **Accuracy and consistency** with relevant requirements and source evidence.
- Test coverage, reproducibility and reliability.
- Security vulnerabilities, sensitive-information disclosure and unsafe actions.
- Fairness, accessibility and potential adverse impacts where relevant.
- Intellectual-property, licensing and applicable contractual requirements.

9.2 High-impact activities

Production-impacting changes, regulated data processing, material security configurations and other consequential activities require the applicable established approvals.

Model confidence scores or fluent explanations are not substitutes for verified evidence.

9.3 Intervention & escalation

Where AI output or autonomous behavior is unsafe, materially misleading or outside its authorized scope, users should **stop relying on the output, pause or contain the activity where feasible, preserve relevant evidence and report the issue.**

10. TestMu-Specific Responsible AI Practices

TestMu applies **responsible AI principles, security, privacy, human oversight and risk-based controls** across its Agentic AI-native Quality Engineering Platform. The following requirements apply to each product according to its AI capabilities, intended purpose and deployment configuration.

10.1 AI Products, Intended Uses & Responsible AI Safeguards

AI product or capability	Intended use	Responsible-use requirement
KaneAI	End-to-end AI QA agent for test creation, execution and maintenance.	Validate generated tests, scripts, assertions and results; apply human oversight and approval for consequential actions.
Kane CLI	AI-assisted testing directly from the terminal.	Review generated commands and code; restrict credentials, repository access and potentially destructive operations.
Agent Assurance	End-to-end testing and assurance of AI agent behavior and actions.	Evaluate agent reliability, safety, authorized actions, tool usage and unintended behavior.
Chat, Voice & Video Agent Testing	Testing conversational and multimodal AI agents.	Validate responses, protect conversations and recordings, and assess privacy, accuracy and harmful behavior.
Test Manager & Test Intelligence	AI-assisted test planning, management and prioritization.	Verify generated test plans, coverage, priorities and recommendations against project requirements.
AI Test Insights	AI-assisted test analytics, failure analysis and quality insights.	Corroborate generated insights, defect explanations and recommendations with logs and reproducible evidence.
Accessibility Testing Agent	AI-assisted identification and testing of accessibility issues.	Validate findings through appropriate accessibility testing; do not rely solely on AI results to establish WCAG conformance.
SmartUI & Visual Testing	Visual comparison and identification of potential UI defects.	Review visual findings, baseline integrity, false positives and false negatives.
HyperExecute – AI Test Orchestration	AI-assisted test orchestration and execution optimization.	Apply approved execution permissions, environment isolation, monitoring and validation of AI-generated recommendations.
Real Device Cloud	Testing applications on real mobile devices.	Protect test data, enforce device and session isolation, and apply responsible AI controls where AI-enabled features are used.
Test Automation Platform	Automated software testing across supported environments.	Validate AI-generated automation, protect credentials and apply appropriate human oversight where AI capabilities are used..
Native App Automation Cloud	Automated testing of native mobile applications.	Protect application data, control device permissions and validate AI-assisted testing activities where applicable.

Browser Cloud for AI Agents	Browser-based environments for AI agent testing and execution.	Restrict agent permissions, isolate sessions, control external actions and monitor unexpected behavior.
Performance Testing	Application performance and scalability testing.	Validate AI-assisted analysis and recommendations against measured performance data, where AI capabilities are used.
TestMu AI MCP Server	Integration of AI agents with TestMu tools and testing capabilities	Enforce least-privilege tool access, authentication, input validation and approval of sensitive agent actions.
AI APIs & integrations	Integration of AI-enabled testing and analytics	Apply appropriate authentication, authorization, data protection, monitoring and customer-approved access boundaries.

10.2 Common Responsible AI Requirements

All applicable TestMu products and AI-enabled capabilities must incorporate safeguards proportionate to their intended purpose and assessed risks:

- **Human oversight:** Validate material AI-generated outputs and require appropriate approval for consequential actions.
- **Security and privacy:** Apply least-privilege access, data minimization, secure integrations and appropriate protection of customer information.
- **Transparency and reliability:** Communicate relevant AI capabilities and limitations, and validate outputs against appropriate evidence.
- **Agentic AI safeguards:** Restrict autonomous actions, tool permissions and access to sensitive environments.
- **Risk management:** Apply relevant AI risk and impact assessments, testing, monitoring and incident-management controls.

11. AI Security, Agents & Third-Party Integration

11.1 Untrusted inputs

Prompts, external webpages, repository files, logs, tickets, retrieved documents and tool responses must be treated as potentially untrusted.

Instructions embedded in untrusted content must not override organizational policies, configured system instructions, access controls or approved tasks.

11.2 Agent permissions

AI agents and tool integrations should use **least-privilege access, scoped credentials, approved APIs, appropriate environment separation and risk-based action controls**.

Potentially destructive, irreversible or externally consequential actions require appropriate restrictions or human confirmation.

11.3 AI-specific security threats

Relevant assessments consider prompt injection, indirect prompt injection, insecure output handling, sensitive-information disclosure, model and retrieval poisoning, tool-call abuse, excessive agency and denial-of-service risks.

11.4 Third-party integrations

External models and AI integrations are assessed according to relevant security, privacy, licensing, data-use, resilience and contractual requirements.

Customer-managed integrations remain subject to documented shared responsibilities.

12. AI Risk, Impact & Compliance Management

TestMu applies risk-based governance throughout the AI lifecycle, aligned with its AI Policy and AIMS.

12.1 Risk identification & assessment

Relevant AI systems and use cases are assessed for foreseeable **security, privacy, reliability, fairness, accessibility, operational, legal and other applicable risks.**

The depth of assessment reflects intended purpose, affected parties, deployment configuration and potential consequences.

12.2 AI system impact assessment

AI system impact assessments consider potential consequences for individuals, groups, organizations and society where relevant.

Assessments are performed according to applicable legal requirements, risk and TestMu's internal governance criteria.

12.3 Risk treatment & testing

Relevant controls may include **bias evaluation, adversarial testing, vulnerability management, output validation, human oversight, monitoring and documented release approval.**

Material residual risks are escalated through established governance processes.

12.4 Compliance

TestMu evaluates relevant AI, privacy, cybersecurity, consumer protection, intellectual-property, employment, accessibility and sector-specific requirements according to its role, intended use and jurisdiction.

The AIMS draws on ISO/IEC 42001, NIST AI RMF, OECD AI Principles and other relevant guidance.

13. Transparency, Accessibility & Customer Trust

13.1 AI transparency

TestMu provides product-appropriate information about AI capabilities, intended purposes, material limitations and available customer controls.

AI features may have different maturity levels, including beta, preview or general availability, where designated in the relevant product documentation.

13.2 Explainability

Where technically feasible and appropriate, documentation, logs and traceability help users understand and review AI-generated outputs.

TestMu does not guarantee that every model output can be fully explained or independently reproduced.

13.3 Accessibility

AI-generated accessibility observations should be considered alongside manual testing and other appropriate evaluation methods.

An AI-generated result alone does not establish WCAG conformance.

13.4 Stakeholder feedback

Customers, partners and other relevant interested parties may raise concerns about AI-generated outputs, accessibility, security, privacy or suspected misuse through established support and reporting channels.

14. Shared Responsibilities & Customer Journey

Responsible AI requirements apply throughout customer evaluation, onboarding, configuration, operation and service exit.

14.1 Evaluation & onboarding

Customers should identify their intended testing purpose, deployment model, authorized users, data sensitivity, integrations and relevant regulatory or sector-specific constraints.

TestMu provides applicable product documentation and available assurance materials through established channels.

14.2 Configuration

Customers are responsible for configuring user permissions, permitted repositories, connected tools, test environments and relevant approval checkpoints according to the applicable service and agreement.

14.3 Operation

Users should validate generated tests, scripts, defect explanations, summaries and recommendations against source evidence, application behavior and relevant security requirements.

14.4 Customer-hosted & on-premises deployments

For customer-hosted or on-premises deployments using customer-selected models, **TestMu and the customer follow the agreed allocation of responsibilities.**

Unless otherwise agreed, customer-managed model training, infrastructure, encryption keys and infrastructure access remain within the customer's operational scope, while TestMu remains responsible for controls within its agreed application and service boundary.

14.5 Change & exit

Customers should review material integration and model changes, remove obsolete access and follow applicable export, retention and deletion arrangements.

15. AI Incident Reporting, Remediation & Assurance

15.1 Reporting

Suspected AI vulnerabilities, data exposure, unauthorized tool actions, harmful outputs, material inaccuracies or other incidents should be reported promptly through the relevant support, security or privacy channels.

Reports should include the **affected feature, relevant timestamps, reproducible steps and appropriate non-sensitive evidence.**

15.2 Incident response

TestMu investigates reported issues through its established incident and vulnerability-management processes.

Where warranted, TestMu applies containment, remediation, root-cause analysis and corrective action, with notification according to applicable law and contractual obligations.

15.3 Customer assurance

Customers may request appropriate assurance documentation through TestMu's established Trust Center, Compliance Center or account channels, subject to confidentiality and availability.

Internal risk registers, sensitive security architecture, detailed audit evidence and personal information are not automatically disclosed through this public document.

16. Training, Governance, Enforcement & Continual Improvement

16.1 AI literacy & awareness

Relevant personnel receive **role-appropriate responsible AI, security, privacy and AI literacy training.**

Specialized awareness is provided where necessary for personnel involved in AI development, deployment, monitoring and governance.

16.2 Governance & oversight

The AI Governance Committee oversees relevant responsible AI risks and governance matters, supported by designated AI System Owners and control functions.

Material issues are escalated through approved executive governance channels.

16.3 Enforcement

Violations by TestMu personnel may result in corrective action or disciplinary measures under applicable internal policies and law.

Customer, supplier and partner violations are addressed according to applicable contractual obligations, policies and legal requirements.

16.4 Continuous improvement

TestMu reviews responsible AI practices in response to regulatory developments, technological changes, customer feedback, AI incidents, audits and management reviews.

This document is reviewed at least annually and following material changes.

17. Reference Documents & Public Resources

The following documents and frameworks support the implementation of TestMu's Responsible AI Use & in Practice.

S. No.	Document or framework	Reference
1	TestMu AI Policy	TestMu AI Policy
2	TestMu AI Terms	AI Terms
3	TestMu Terms of Service	Terms of Service
4	TestMu Acceptable Use Policy	Acceptable Use Policy
5	TestMu Privacy Policy	Privacy Policy
6	TestMu Data Processing Addendum	DPA
7	TestMu Subprocessor List	Subprocessors
8	TestMu Information Security Policy	Information Security Policy
9	ISO/IEC 42001:2023	AI Management Systems
10	ISO/IEC 42005:2025	AI System Impact Assessment
11	NIST AI RMF	AI Risk Management Framework
12	OECD AI Principles	OECD AI Principles
13	EU AI Act	Regulation (EU) 2024/1689
14	OWASP LLM Security	OWASP LLM Top 10

18. Glossary of Terms

Term	Definition
Artificial Intelligence (AI)	Machine-based systems capable of generating outputs such as predictions, content, recommendations or decisions for defined objectives.
AIMS	Artificial Intelligence Management System governing AI-related responsibilities, risks, controls and continual improvement.
AI System	A machine-based system that infers from inputs how to generate outputs for explicit or implicit objectives, with varying levels of autonomy.
AI Provider	An organization providing an AI system or AI-enabled service, with responsibilities determined by its role and applicable law.
AI Producer/Developer	An organization or function involved in designing or developing an AI system or component.
AI Partner/Integrator	A party integrating or supporting AI systems, models or services within an agreed technical or commercial arrangement.
AI User	A person or organization using an AI system for an authorized purpose.
AI Lifecycle	Activities from system identification and design through development, deployment, operation, monitoring, change and retirement.
AI Risk Assessment	A structured process for identifying, analyzing and evaluating AI-related risks.
AI Impact Assessment	A structured evaluation of potential consequences of an AI system for relevant individuals, groups, organizations or society.
Human Oversight	Human review, intervention, approval or escalation proportionate to an AI system's intended use and risks.
Prompt Injection	An attempt to manipulate an AI system through malicious or unauthorized instructions in prompts or other content.
Model Drift	Changes in model performance or behavior over time, potentially affecting reliability or suitability.
TEVV	Testing, Evaluation, Verification and Validation of AI systems.
ToMs	Technical and Organizational Measures applied to protect systems, information and relevant processing activities.
Customer Data	Data provided, uploaded or processed by or on behalf of a customer within the relevant TestMu service, as defined by the applicable agreement.