

TestMu AI Policy

Document ID: TMU-GRC-POL-021

Version Number: 1.4

Statement of Confidentiality

This document contains confidential and proprietary information of LambdaTest 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:

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

Website: [TestMu](https://testmu.com)

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	Jun 12,2026	2026 yearly review & update		
1.2	Aug 28, 2026	2026Revised Released	GRC Team	CCO & Co-Founder
1.3	Sep 03,2026	Comprehensive enhancement of AI governance, risk management, responsible AI, security, privacy and global regulatory compliance 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 & Co- Founder		Sep ,26,2026

Table of Contents

1.INTRODUCTION & APPLICABILITY	5
2. OBJECTIVE.....	5
3. PURPOSE & COMMITMENT.....	6
4. SCOPE	6
5. AI GOVERNANCE & FRAMEWORK ALIGNMENTS	7
5.1 LEADERSHIP AND GOVERNANCE.....	8
5.2 AI INVENTORY AND ACCOUNTABILITY	8
5.3 RISK ESCALATION AND DECISION-MAKING.....	8
5.4 REPORTING AND ORGANIZATIONAL CULTURE.....	8
5.5 FRAMEWORK AND LEGAL ALIGNMENT	8
6. GUIDING AI PRINCIPLES	9
6.1 TRANSPARENCY AND EXPLAINABILITY.....	9
6.2 ACCOUNTABILITY AND GOVERNANCE.....	9
6.3 FAIRNESS AND NON-DISCRIMINATION	9
6.4 HUMAN OVERSIGHT	9
6.5 PRIVACY AND DATA PROTECTION BY DESIGN	10
6.6 SECURITY AND ROBUSTNESS.....	10
6.7 SUSTAINABILITY AND ETHICS	10
7. CORE AI POLICY DOMAINS	10
7.1 DATA PROTECTION AND PRIVACY	10
7.2 AI MODEL SECURITY	11
7.3 ACCESS CONTROL AND AUTHENTICATION.....	12
7.4 API SECURITY	12
7.5 MONITORING , LOGGING AND INCIDENT RESPONSE	12
7.6 ETHICAL AI AND RESPONSIBLE USE.....	12
7.7 THIRD-PARTY AND VENDOR MANAGEMENT.....	12
7.8 TRAINING AND AWARENESS.....	13
7.9 TESTMU CULTURE AND ESG ALIGNMENT	13
7.10 TECHNICAL AND ORGANIZATIONAL MEASURES (ToMs).....	13
7.11 AI RISK AND IMPACT ASSESSMENT	14
8. SPECIFIC AI PRODUCTS, FEATURES & INTENDED USE.....	14
9. AI LIFECYCLE MANAGEMENT , RISK & IMPACT ASSESSMENT	15
10. AGENTIC AI, MODEL SECURITY & THIRD PARTY AI GOVERNANCE	16
11. CUSTOMER DATA PROTECTION & SHARED RESPONSIBILITY.....	17
12. TRANSPARENCY, HUMAN OVERSIGHT & STAKEHOLDER ENGAGEMENT	18
13. AI INCIDENT MANAGEMENT , MONITORING & ASSURANCE	19
14. ENFORCEMENT & ACCOUNTABILITY	20
15. REVIEW & CONTINUOUS IMPROVEMENT	20
16. PUBLIC REFERENCES, CONTACT & CONCLUSION.....	21

1. Introduction & Applicability

LambdaTest Inc., d/b/a TestMu, and its applicable affiliates (collectively, “**TestMu**”) are committed to developing, providing, integrating, operating and using artificial intelligence responsibly, securely, transparently and in accordance with applicable legal, regulatory and contractual requirements.

As a global Agentic AI-native Quality Engineering Platform provider, TestMu recognizes that artificial intelligence can significantly improve software testing, automation, quality engineering and decision-making. TestMu also recognizes the importance of **identifying, assessing and managing the risks and potential impacts associated with AI systems throughout their lifecycle**.

This AI Policy establishes TestMu’s organizational commitments, governance principles, accountability arrangements and requirements for the responsible development, provision, deployment, operation and use of AI systems and AI-enabled products and services.

It is intended for **customers, authorized users, employees, contractors, consultants, suppliers, AI model and technology providers, business partners, investors, auditors, certification bodies, regulators, authorities and other interested parties**.

This Policy complements TestMu’s customer agreements, AI Terms, Acceptable Use Policy, Privacy Policy, Information Security Policy, Technical and Organizational Measures (ToMs), Responsible AI Use & Practices and internal Artificial Intelligence Management System (AIMS).

Applicable contractual and legal requirements govern where they differ from this Policy. TestMu addresses such differences through its established governance processes.

2. Objective

The objective of this Policy is to ensure that AI developed, provided, integrated, operated or used by TestMu is **governed consistently, supports responsible innovation and is subject to proportionate risk, impact, security, privacy, quality, transparency and human-oversight controls throughout its lifecycle**.

The Policy establishes requirements to:

- Define **organizational accountability and governance responsibilities** for AI systems.
- **Identify, assess, evaluate, treat and monitor** AI-related risks, opportunities and reasonably foreseeable impacts.
- Incorporate responsible AI principles, information security, privacy and data protection into AI system design, development and operation.
- Establish appropriate controls for generative AI, large language models, autonomous and semi-autonomous agents, AI-assisted testing and third-party AI systems.
- **Protect customer data and other information assets**.
- Establish appropriate human oversight, transparency and accountability arrangements.

- Support compliance with applicable international standards, AI regulations, privacy laws and contractual requirements.
- Establish measurable AI governance objectives and continual improvement mechanisms.

The **application of these requirements shall be proportionate** to each AI system's intended purpose, operating context, risk classification, potential impacts and applicable obligations.

3. Purpose & Commitment

TestMu establishes this Policy to communicate its public commitments and provide management direction for responsible AI.

TestMu commits to **protecting customer data, respecting applicable rights, maintaining accountability, assessing foreseeable impacts, enabling appropriate human oversight, communicating material limitations and continually improving its AIMS.**

Our commitment: TestMu develops, provides and uses AI in ways designed to be **lawful, secure, reliable, transparent, accountable, privacy-respecting and subject to meaningful human oversight.**

TestMu integrates responsible AI considerations into product development, business operations, procurement, supplier management, customer engagement and the AI system lifecycle.

These commitments are implemented through **defined organizational responsibilities, documented processes, risk-based controls, monitoring, internal audit and management review.**

4. Scope

This Policy applies across the lifecycle of AI systems that TestMu develops, provides, integrates, operates, maintains, tests, evaluates or uses.

It covers AI models, machine-learning components, generative AI, large language models, natural-language processing, computer vision, agents, AI-assisted analytics, prompts, datasets, evaluation assets, APIs, integrations and AI-enabled workflows.

4.1 Organizational and geographical scope

The Policy applies to all **relevant TestMu legal entities, offices, operations and remote-working locations globally**, including the United States and India, and any location from which TestMu develops, provides, operates, supports, procures or uses AI.

It applies to Product Management, Engineering, Quality Assurance, Architecture, DevOps, DevSecOps, Cloud Operations, Site Reliability Engineering, IT, Information Security, Privacy, GRC, Legal, Procurement, Customer Success, Support, Sales, Marketing, HR, Finance, Administration and Executive Management.

4.2 Interested parties

The Policy addresses the applicable needs, expectations and responsibilities of **customers and authorized users; employees, interns, contractors and consultants; suppliers, subprocessors, AI model providers and technology partners; investors; auditors and certification bodies; regulators and authorities; and individuals or groups potentially affected by TestMu AI systems.**

Responsibilities are determined according to each party's role, contractual relationship, access permissions, processing activities and applicable legal obligations.

4.3 AI-related assets

The Policy covers **AI systems, models, algorithms, datasets and data sources, prompts, embeddings, APIs, analytics engines, agents, plugins, integrations, evaluation and benchmark assets, AI-generated outputs, feedback, logs, monitoring records and supporting cloud or technical infrastructure.**

4.4 Product and service scope

The Policy applies, where AI-enabled or AI-supporting, to **KaneAI and Kane CLI; Test Manager and Test Intelligence; HyperExecute AI-assisted capabilities; SmartUI and Visual AI; accessibility-related AI capabilities; Real Device Cloud; web, mobile and native-app testing; agent, bot, voice and agent-to-agent testing; platform APIs, integrations, plugins and supporting infrastructure.**

Specific functionality and availability depend on the product, deployment configuration and applicable customer agreement.

4.5 Internal AI use

Approved enterprise AI may support coding, documentation, analysis, customer support, security operations and other authorized business processes.

Internal AI use is subject to TestMu's information classification, access control, privacy, security, procurement, acceptable-use and human-review requirements.

4.6 AI roles and scope determination

TestMu primarily acts as an **AI provider** for its AI-enabled Quality Engineering products and may act as an AI developer, integrator or user of third-party AI systems, depending on the use case.

The applicable legal role and associated responsibilities are determined according to the system, intended purpose, jurisdiction and deployment arrangement.

A feature is not automatically classified as AI solely because it uses automation or deterministic rules. TestMu performs use-case and feature-level screening to determine the applicable governance requirements, legal role and risk classification.

5. AI Governance & Framework Alignments

5.1 Leadership and Governance

Executive Management is accountable for the effectiveness of the AIMS, and provides the direction, resources and oversight necessary to support responsible AI.

The **AI Governance Committee provides cross-functional oversight**, supported by the AI Risk Officer or designated AI governance function, Product and AI System Owners, Engineering, DevSecOps, Information Security, Privacy, Legal, GRC, Procurement, HR and other relevant control owners.

Responsibilities are assigned for AI system design, development, data management, testing, release, operation, monitoring, incident handling, change management and retirement.

Segregation of duties and independent review are applied proportionately to risk.

5.2 AI Inventory and Accountability

In-scope AI systems and approved internal AI tools are registered with an **accountable owner, intended purpose, lifecycle status, data categories, model and provider dependencies, risk classification and applicable obligations**.

The inventory supports risk management, impact assessment, supplier oversight, change management and management reporting.

5.3 Risk Escalation and Decision-making

Material AI risks and impacts are assessed, treated, accepted or escalated according to defined criteria.

High residual risks require authorization at the appropriate management level. Unacceptable risks prevent deployment or continued use until appropriately treated.

Specific approval authorities, escalation thresholds and delegations are documented internally.

5.4 Reporting and Organizational Culture

Personnel and suppliers are expected to report known or suspected **unsafe, unlawful, misleading, insecure, discriminatory or unauthorized AI behavior** through established reporting channels.

TestMu supports good-faith reporting and prohibits **retaliation for raising legitimate concerns**.

5.5 Framework and Legal Alignment

TestMu's governance approach is designed to align, as applicable, with:

- **ISO/IEC 42001:2023** — Establishing, implementing, maintaining and continually improving an AI Management System.
- **ISO/IEC 42005:2025** — AI system impact assessment guidance.
- **ISO/IEC 23894** — AI risk management.

- **ISO/IEC 27001, ISO/IEC 27017 and ISO/IEC 27701** – Information security, cloud security and privacy information management, as applicable.
- **NIST AI Risk Management Framework and Generative AI Profile** – AI governance and risk management.
- **OECD AI Principles** – Responsible and trustworthy AI.
- **OWASP guidance** – Relevant large language model and agentic AI security risks.
- **Applicable laws** – AI, privacy, cybersecurity, consumer protection, intellectual property, accessibility, employment and sector-specific requirements.

TestMu evaluates the applicability of the **EU AI Act** by role, use case, jurisdiction and risk classification. Regulatory obligations are assessed and monitored as relevant to each system.

Alignment with a framework does not automatically constitute certification against that framework.

6. Guiding AI Principles

TestMu applies the following principles throughout the AI lifecycle.

6.1 Transparency and Explainability

TestMu provides **product-appropriate information about AI-enabled functionality, intended uses, material limitations and relevant human-review requirements.**

Documentation, logs, traceability and practical explanations are provided according to technical feasibility, system risk and contractual commitments.

TestMu does not represent that every AI-generated output has a fully interpretable rationale.

6.2 Accountability and Governance

AI oversight is embedded through the **AI Governance Committee, accountable AI System Owners and established management processes.**

AI-related responsibilities, risk decisions, approvals and material changes are documented and reviewed proportionately.

6.3 Fairness and Non-Discrimination

TestMu evaluates foreseeable differential impacts where relevant to the AI use case and applies **appropriate testing, monitoring and corrective measures.**

Fairness assessments consider the intended purpose, affected parties, relevant datasets, operating environment and potential adverse outcomes.

6.4 Human Oversight

AI recommendations, generated artifacts and autonomous actions are subject to **human oversight proportionate to the use case, risk and deployment configuration.**

Appropriate review, intervention, override and escalation arrangements are established for material or consequential outputs and actions.

6.5 Privacy and Data Protection by Design

TestMu applies **privacy and data protection by design and default**, including data minimization, purpose limitation, access control, retention, deletion and applicable data-subject rights.

AI processing is assessed against applicable privacy laws and the relevant controller or processor responsibilities.

6.6 Security and Robustness

AI systems are subject to **risk-based security and robustness controls**, including secure development, vulnerability management, adversarial testing, monitoring, incident response and recovery.

Controls address relevant AI-specific threats such as prompt injection, model poisoning, data leakage, insecure output handling and unauthorized agent actions.

6.7 Sustainability and Ethics

TestMu considers **resource efficiency, environmental impacts and relevant societal considerations** during AI design, procurement and operation, consistent with its ESG program.

Responsible innovation is supported by applicable ethical principles, organizational values and stakeholder engagement.

7. Core AI Policy Domains

7.1 Data Protection and Privacy

TestMu protects customer data and other information assets through **appropriate technical and organizational measures**.

Customer Data is not used to train, retrain or fine-tune AI models made available to other customers, in accordance with TestMu's published [AI Terms](#).

Customer-specific model customization, where contractually supported, remains subject to the applicable agreement and approved data-processing arrangements.

Data minimization and purpose limitation are applied to AI processing. Privacy impact assessments, AI impact assessments and other legal assessments are performed **where required by law, risk or internal governance criteria**.

TestMu supports applicable data-subject rights according to its legal role and governing agreements.

7.1.1. Data Collection and Use

TestMu defines and documents the purposes of data processing for relevant AI-powered and platform-level AI features.

Personal data processing is limited to **authorized purposes and applicable legal bases**. Consent is obtained where required by law.

Synthetic, masked or otherwise appropriately protected data is preferred where practicable for testing and evaluation.

7.1.2. Data Storage and Transmission

TestMu applies **industry-standard encryption** to relevant AI-related data at rest and in transit, including AES-256 and TLS 1.2 or higher where supported by the applicable architecture.

Logical tenant separation, access control, appropriate retention and secure deletion are applied according to the service, deployment configuration and applicable contractual requirements.

7.1.3. Customer Data Ownership

Customers retain their contractual rights in Customer Data, including Test execution data, inputs and outputs.

TestMu processes Customer Data for authorized service purposes and in accordance with applicable agreements, privacy documentation and AI Terms.

TestMu does not use Customer Data (Inputs, Outputs, or Usage Data) to train models for use by other customers.

7.1.4. Restricted Data Uploads

Unless expressly authorized through the applicable service and contractual arrangements, customers **must not upload or process** payment-card data, protected health information, government-classified or export-controlled data, biometric identifiers or other restricted personal information.

Customers remain responsible for ensuring that submitted data is lawful and permitted under the applicable agreement and data-processing arrangements.

7.2 AI Model Security

TestMu applies **risk-based security controls to AI models and supporting components throughout their lifecycle**.

These include appropriate adversarial testing, vulnerability assessment, threat modeling, secure configuration, dependency management, monitoring and change control.

Relevant threats include **model poisoning, prompt injection, indirect prompt injection, data leakage, retrieval poisoning, insecure output handling and unauthorized model or tool access**.

7.3 Access Control and Authentication

Access to AI tools, models, APIs and supporting infrastructure is governed by **role-based access control, least privilege and appropriate authentication**.

Multi-factor authentication is required for privileged accounts according to TestMu's access-control requirements.

Privileged and relevant model-access activities are logged and monitored in accordance with applicable security, privacy and retention requirements.

7.4 API Security

AI APIs and integrations are protected through **appropriate authentication, authorization, encryption, rate limiting, input validation and monitoring**.

OAuth 2.0, token-based authentication, API gateways and other appropriate mechanisms are used according to the applicable architecture.

External integrations follow least-privilege and zero-trust principles where applicable.

7.5 Monitoring , Logging and Incident Response

TestMu monitors relevant AI systems for **security events, anomalous behavior, reliability concerns, material performance changes and other risk indicators**.

Monitoring for drift, bias and output quality is applied where relevant to the system and technically appropriate.

Audit logs are protected against unauthorized access and alteration and retained according to applicable legal, contractual and organizational requirements.

AI-related incidents are managed through TestMu's established incident-response processes, including defined roles, containment, investigation, remediation and required notification.

7.6 Ethical AI and Responsible Use

TestMu develops and uses AI to **augment human capabilities and improve quality engineering outcomes**.

AI must not be used for unlawful, harmful, manipulative, discriminatory or otherwise prohibited purposes.

AI use is governed by TestMu's Responsible AI Use & Practices, Acceptable Use Policy, AI Terms and applicable laws.

7.7 Third-Party and Vendor Management

Third-party AI models, suppliers, integrations and supporting services are subject to **risk-based due diligence**.

Assessments consider security, privacy, data use, model-training restrictions, intellectual property, licensing, subprocessors, resilience, regulatory obligations and change management.

Applicable contractual safeguards, audit rights and supplier monitoring requirements are established according to risk and contractual arrangements.

7.8 Training and Awareness

TestMu provides **AI ethics, responsible-use and security awareness training** to relevant personnel.

Specialized training is provided according to role and exposure to AI-related risks, including for Product, Engineering, DevOps, DevSecOps, Security and other personnel involved in AI development and operation.

Personnel are encouraged to report potential AI security issues, misuse and ethical concerns.

7.9 TestMu Culture and ESG Alignment

TestMu promotes a **customer-first, security-first and compliance-oriented culture** in the development and use of AI.

Its AI practices support responsible innovation, resource efficiency, accessibility and relevant ESG objectives.

The organization considers applicable UN Sustainable Development Goals, GRI reporting principles, SBTi-related initiatives and SEBI BRSR requirements where relevant to its sustainability program.

7.10 Technical and Organizational Measures (ToMs)

TestMu applies **appropriate technical and organizational measures** to AI systems and supporting infrastructure.

These include customer-data segregation, controlled model use, secure access, encryption, vulnerability management, monitoring, incident response and applicable human-oversight safeguards.

Customer Data is not used to train models made available to other customers, consistent with [TestMu's AI Terms](#).

AI features may use third-party model providers, including providers identified in TestMu's published [Subprocessor List](#). The processing arrangements and safeguards depend on the relevant product and deployment.

TestMu applies relevant OWASP AI and LLM security guidance through its secure development and risk-management practices.

7.11 AI Risk and Impact Assessment

TestMu conducts **AI risk and impact assessments** according to the system's intended purpose, operating context, affected parties, risk classification and applicable obligations.

Assessments consider foreseeable misuse, reliability, security, privacy, fairness, human oversight, accessibility and other relevant impacts.

Documented treatment decisions, residual-risk approvals, testing evidence and reassessment requirements support AI lifecycle governance.

8. Specific AI Products, Features & Intended Use

TestMu's AI governance requirements apply to relevant AI-enabled products and features according to their intended use and deployment configuration.

8.1 KaneAI and Kane CLI

KaneAI and Kane CLI support AI-assisted software testing activities, including test planning, generation, authoring, execution and maintenance, where supported.

AI-generated scripts, test cases, recommendations and actions are subject to appropriate validation and human oversight.

Security and data-processing controls are applied according to the deployment architecture, customer agreement and applicable model-provider arrangements.

8.2 Test Manager & Test Intelligence

AI-enabled test management and intelligence capabilities may provide insights for **test optimization, prioritization, defect analysis and quality engineering workflows**.

Relevant output quality, reliability and performance are evaluated and monitored according to the intended use.

8.3 HyperExecute AI-Assisted Capabilities

AI-assisted HyperExecute workflows are governed by applicable security, access-control, execution-isolation and monitoring requirements.

AI-generated recommendations or automation are subject to appropriate validation before use in consequential workflows.

8.4 SmartUI & Visual AI

SmartUI and related visual AI capabilities support visual comparison and the identification of potential differences or defects.

AI-generated findings may require human interpretation and validation, particularly where visual differences have material business or accessibility implications.

8.5 Accessibility AI

Accessibility-related AI capabilities support testing and the identification of potential accessibility issues.

AI-generated accessibility findings supplement rather than replace appropriate human review and standards-based evaluation.

An AI-generated result alone does not establish conformity with an accessibility standard.

8.6 Real Device Cloud, Web, Mobile & Native-App Testing

AI-assisted capabilities within TestMu's device and application-testing services are governed by **applicable data protection, tenant isolation, access-control, device security and lifecycle requirements**.

8.7 Agent, Bot, Voice & Agent-to-Agent Testing

AI-enabled agent, bot, voice and agent-to-agent testing capabilities are subject to **appropriate authorization, execution boundaries, monitoring and evaluation**.

Testing considers relevant failure modes, unsafe actions, unexpected interactions and unauthorized access or data disclosure.

8.8 Platform-Level AI APIs & Integrations

AI APIs and integrations are protected through **appropriate authentication, authorization, encryption, logging and monitoring**.

Customer-managed integrations remain subject to the applicable shared-responsibility arrangements.

9. AI Lifecycle Management , Risk & Impact Assessment

TestMu applies **documented governance throughout the AI lifecycle**, from identification and design through retirement.

9.1 AI system identification and intended purpose

Each in-scope AI system or materially distinct use case has an **accountable owner and a documented intended purpose**.

Relevant records identify affected interested parties, data categories, model and provider dependencies, operating environment, geographical applicability, risk classification and lifecycle status.

9.2 Risk and opportunity assessment

TestMu identifies and assesses AI-related risks and opportunities according to established criteria.

Assessments consider intended and reasonably foreseeable uses, potential misuse, affected parties, dependencies and applicable legal and contractual obligations.

9.3 AI system impact assessment

AI system impact assessments are performed **where required by applicable law, risk or internal governance criteria**.

They consider potential effects on individuals, groups, organizations and society, as relevant to the system.

Assessment activities are informed by applicable guidance, including ISO/IEC 42005:2025.

9.4 Testing, Evaluation, Verification & Validation

Before material deployment, relevant AI systems undergo **proportionate testing, evaluation, verification and validation (TEVV)**.

Testing considers task suitability, reliability, material failure modes, hallucinations, security vulnerabilities, prompt injection, unauthorized tool actions, data leakage and bias where relevant.

Results, limitations and required corrective actions are documented.

9.5 Release authorization

Material AI releases and significant changes are subject to **appropriate review and authorization**.

Unacceptable residual AI risks prevent deployment until appropriately treated.

9.6 Change management

Material changes to models, providers, prompts, retrieval sources, data, tools, autonomy, integrations, operating geography or intended purpose **trigger proportionate reassessment and approval**.

9.7 Monitoring and retirement

Post-release monitoring, customer feedback, incident trends, changes in law and security findings inform corrective action and continual improvement.

AI system retirement addresses **access revocation, retention, deletion, contractual dependencies and applicable records**.

10. Agentic AI, Model Security & Third Party AI Governance

10.1 Agentic AI safeguards

Agentic AI functions are designed around **defined scopes of authority, least-privilege credentials, approved tool and API access, appropriate execution boundaries and activity traceability**.

Risk-based safeguards address prompt injection, indirect instruction attacks, unauthorized data exfiltration, excessive agency and unintended tool execution.

10.2 Consequential actions

Potentially destructive, production-impacting, irreversible or externally consequential actions require appropriate restrictions, approvals or human confirmation, according to the use case and deployment.

TestMu distinguishes recommendations, autonomous actions and actions requiring customer configuration or approval.

10.3 Third-party AI providers

External AI models, APIs and supporting services are subject to **risk-based supplier assessment**.

Relevant considerations include security, privacy, data-use restrictions, training terms, subprocessors, resilience, intellectual property and change management.

10.4 Customer-hosted and on-premises deployments

For customer-hosted or on-premises deployments using customer-selected AI models, **TestMu and the customer define applicable shared responsibilities**.

Unless expressly agreed otherwise, **TestMu's responsibilities for its application are distinguished from customer-managed model training, hosting, infrastructure, encryption keys and infrastructure-level access controls**.

11. Customer Data Protection & Shared Responsibility

11.1 Customer data and AI model use

Customers retain their contractual rights in Customer Data.

TestMu does not use Customer Data to train, retrain or fine-tune AI models made available to other customers, consistent with its published [AI Terms](#).

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

11.2 Data processing and subprocessors

TestMu may use approved third-party AI models, cloud infrastructure and other subprocessors to provide relevant services.

The applicable providers, processing activities and available location information are described in TestMu's published [Subprocessor List](#).

11.3 Data residency and cross-border transfers

Data hosting, processing and support-access arrangements depend on the relevant product, purchased service, agreed configuration and applicable contractual requirements.

A selected storage region does not necessarily determine every transient processing or remote-support location.

Applicable international data transfers are governed by relevant legal and contractual safeguards.

11.4 Customer responsibilities

Customers are responsible for **lawful input data, authorized users, appropriate configurations, validation of AI-generated outputs and the use of AI features within their documented intended purpose.**

Customers should minimize unnecessary personal or sensitive information and use synthetic or appropriately masked data where practicable.

11.5 Shared responsibility

TestMu and its customers share responsibilities according to the applicable service, deployment architecture and agreement.

TestMu is responsible for controls within its operational scope, while customers remain responsible for their applications, data, configurations, user permissions and customer-managed infrastructure or models, as applicable.

12. Transparency, Human Oversight & Stakeholder Engagement

12.1 Product transparency

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

Material AI changes and known limitations are communicated through applicable product, support and contractual channels.

12.2 Human oversight

AI-generated test cases, code, recommendations, summaries and other outputs may be incomplete or inaccurate and require appropriate human review and validation.

Customers should apply appropriate review before relying on AI-generated outputs, particularly for production releases, security findings, compliance activities and regulated workflows.

12.3 Customer controls

Where supported by the relevant product and deployment, customers may configure access, review outputs, apply approvals and obtain logs or records according to the applicable agreement.

12.4 Stakeholder engagement

TestMu considers relevant stakeholder needs, expectations and feedback through product governance, support, privacy, security and incident-management processes.

Stakeholders may report suspected harmful outputs, security vulnerabilities, privacy concerns, inaccurate information or misuse through established channels.

12.5 Accessibility and redress

Accessibility-related AI findings support, rather than replace, human and standards-based evaluation.

Relevant complaints and concerns are routed to the responsible function for proportionate investigation and corrective action.

13. AI Incident Management , Monitoring & Assurance

13.1 Incident management

TestMu investigates AI-related security, privacy, reliability and misuse incidents through established incident-management processes.

Activities include **detection, triage, containment, investigation, remediation, root-cause analysis and legally or contractually required notification.**

13.2 Monitoring

Relevant AI systems are monitored according to their risk classification, intended purpose and technical characteristics.

Monitoring considers **security events, reliability, material performance changes, inappropriate outputs, customer feedback and other relevant risk indicators.**

13.3 Audit and management review

The AIMS is subject to internal audit, management review, competence and awareness activities, control testing and continual improvement.

Findings and corrective actions are documented and tracked according to established governance processes.

13.4 Records and evidence

Internal AIMS evidence includes AI inventories, context and interested-party records, applicable legal registers, risk and opportunity assessments, AI impact assessments, treatment decisions, testing results, approved exceptions, supplier reviews, change records, incident records, monitoring evidence, training records, internal audits and management reviews.

These detailed records are controlled and are not automatically public.

13.5 Customer assurance

TestMu may provide appropriate assurance materials through its Trust Center or controlled customer-assurance processes, subject to confidentiality, availability and applicable contractual arrangements.

Publication of this Policy does not itself constitute certification or independent attestation.

14. Enforcement & Accountability

14.1 Employees and personnel

Employees, contractors and other personnel are responsible for **complying with applicable AI governance, security, privacy and responsible-use requirements**.

Violations may result in corrective action or disciplinary measures according to applicable organizational procedures and law.

14.2 Suppliers and partners

Suppliers and partners are responsible for complying with applicable contractual obligations and approved AI-related requirements.

Non-compliance may result in **remediation requirements, additional oversight, suspension or termination**, according to the relevant agreement.

14.3 Customers

Customer use of TestMu's AI-enabled products and services is governed by the applicable customer agreement, AI Terms and Acceptable Use Policy.

Violations may be addressed through the measures permitted by those agreements and applicable law.

14.4 Accountability

AI System Owners and relevant control owners are responsible for implementing applicable controls, maintaining required evidence, reporting material risks and supporting corrective action.

Executive Management and the AI Governance Committee oversee material AI governance matters through established management processes.

15. Review & Continuous Improvement

TestMu reviews this Policy at **least annually and following material changes** to AI technology, products, business context, risks, legal obligations or relevant stakeholder requirements.

The **AI Governance Committee and designated document owner** coordinate the review process, with appropriate input from Product, Engineering, Security, Privacy, Legal, GRC and other relevant functions.

Risk assessments, impact assessments and supplier reviews are updated according to defined schedules and material change triggers.

TestMu monitors proportionate indicators, including **AI-system assessment coverage, overdue risk treatment, release-gate completion, material incidents, supplier reassessments, employee AI literacy, human-oversight effectiveness and corrective-action closure.**

Lessons learned from audits, incidents, customer feedback, regulatory developments and management reviews inform continual improvement of the AIMS.

Material policy changes are subject to appropriate review and approval before publication.

16. Public References, Contact & Conclusion

16.1 Related TestMu policies and documentation

This Policy should be read together with the following public documents.

S. No.	Document	Public Reference
1	Terms of Service	TestMu Terms of Service
2	AI Terms	TestMu AI Terms
3	Acceptable Use Policy	TestMu Acceptable Use Policy
4	Privacy Policy	TestMu Privacy Policy
5	Data Processing Addendum (DPA)	TestMu DPA
6	Subprocessor List	TestMu Subprocessors
7	Information Security Policy	TestMu Security

16.2 Contact and reporting

Customers and interested parties may raise **AI governance questions, responsible-use concerns, security issues, privacy matters or requests for appropriate assurance** through TestMu's published contact channels.

Information security and AI governance enquiries may be directed to security@testmuai.com and grc@testmuai.com , subject to confirmation before publication.

16.3 Conclusion

TestMu is committed to **developing, providing and using AI responsibly through a structured, risk-based and continuously improving Artificial Intelligence Management System.**

Information security, privacy, fairness, transparency, accountability, human oversight and responsible innovation remain central to TestMu's approach to AI-enabled quality engineering.

This Policy communicates TestMu's organizational commitments to customers, employees, partners, regulators and other interested parties while recognizing the importance of deployment-specific controls, shared responsibilities and applicable legal and contractual obligations.