

Technical & Organizational Measures

Version Number: 2.0

(Security, Privacy and Responsible AI Controls)

Purpose and Interpretation

This document describes the technical and organizational measures (“TOMs”) maintained by TestMu to protect the confidentiality, integrity, availability, privacy and resilience of information and systems, and to support the responsible development, deployment and use of artificial intelligence. These measures apply to the TestMu Agentic AI-native Quality Engineering Platform and associated products and services.

The measures are risk-based and apply as relevant to the applicable service, deployment model, processing role, data category, customer configuration, geographic region, legal requirements and contractual commitments. TestMu may implement equivalent or stronger safeguards as technologies, business operations, regulatory requirements and threats evolve. Nothing in this document limits or reduces any obligations expressly agreed in an applicable contract, Data Processing Addendum (“DPA”) or other written agreement.

Assurance Context

For its AI-enabled products and services, TestMu acts primarily as an **AI Provider** and, where applicable, as an **AI Producer/Developer, AI Partner or AI User** in accordance with the relevant operating context.

For personal data, TestMu generally acts as:

- **A processor or service provider** for customer Test-execution data and other customer-controlled content; and
- **A controller or business** for Account information, workforce data, website-user data and business-contact information.

The specific role and corresponding obligations may vary according to the relevant service, processing activity, customer arrangement, applicable law and contractual terms.

Table of Contents

<u>1. Overview</u>	<u>12. Physical and Environmental security</u>
<u>2. Governance, Risk and Compliance</u>	<u>13. Business Continuity, Backup and Disaster Recovery</u>
<u>3. People and Organizational Measures</u>	<u>14. Supplier and Sub-processor Measures</u>
<u>4. Asset, Information and Configuration Management</u>	<u>15. Incident Response and Breach Notification</u>
<u>5. Identity and Access Management</u>	<u>16. Artificial Intelligence-related Measures</u>
<u>6. Secure Product Development and Change Management</u>	<u>17. ESG and Responsible Business Measures</u>
<u>7. Cloud, Infrastructure and Network Security</u>	<u>18. Global Legal and Regulatory Applicability</u>
<u>8. Cryptography and Key Management</u>	<u>19. Customer and TestMu Shared Responsibilities</u>
<u>9. Data Protection, Privacy and Lifecycle Controls</u>	<u>20. Audit, Evidence, & Continual Improvement</u>
<u>10. Logging, Monitoring and Security Operations</u>	<u>21. Appendix A - Standards and Regulatory Alignment</u>
<u>11. Vulnerability, Threat and Assurance Management</u>	<u>22. Appendix B – Public Assurance Resources</u>

1. Overview

TestMu applies defence-in-depth safeguards across people, processes, technology and third-party relationships. Its control environment covers the design, development, acquisition, integration, testing, evaluation, deployment, operation, monitoring, maintenance and responsible use of the TestMu Agentic AI-native Quality Engineering Platform, associated products, features and supporting systems.

Where applicable, this includes generative AI, large language models (“LLMs”), natural language processing, machine-learning components, AI-enabled quality-engineering capabilities and autonomous or semi-autonomous AI/QA agents.

TestMu’s control environment is founded on the following principles:

- **Security, privacy and responsible AI by design and by default** throughout the information, service and AI-system lifecycle.
- **Risk-proportionate controls** based on information classification, processing purpose, intended use, deployment context, reasonably foreseeable misuse and potential impact on customers, individuals and other affected stakeholders.
- **Data and tenant segregation**, supported by unique tenant identification, logical isolation, least-privilege access and controls designed to prevent unauthorized cross-customer access.
- **Secure engineering and operational resilience**, including change control, vulnerability management, logging, monitoring, incident response, business continuity and disaster recovery.
- **Responsible AI governance**, including defined accountability, human oversight, transparency, data governance, security testing, performance evaluation and management of AI-specific risks.
- **Legal and contractual compliance** based on TestMu’s role, processing activity, service configuration and the laws and regulatory requirements applicable in supported jurisdictions.
- **Supplier and sub-processor oversight** through risk-based due diligence, contractual safeguards, security and privacy requirements, and ongoing monitoring proportionate to the services provided.
- **Independent assurance and continual improvement** through control testing, vulnerability assessments, internal audits, external assessments, management reviews, corrective actions and periodic updates to the control environment.

These measures apply to systems, personnel, facilities, processes and third parties within the defined scope of TestMu’s information security, privacy and AI management systems. Specific controls may vary according to the applicable product, hosting or deployment model, customer configuration, data category, geographic region and contractual commitment.

2. Governance, Risk and Compliance

TestMu maintains integrated Information Security Management System (“ISMS”), Privacy Information Management System (“PIMS”) and Artificial Intelligence Management System (“AIMS”) arrangements. These management systems provide a coordinated framework for managing information security, cybersecurity, privacy, responsible AI, operational resilience, legal compliance and associated business risks.

Senior leadership establishes strategic direction, approves policies and objectives, assigns responsibilities, and provides appropriate resources. The designated governance committee, including the Information Security & Compliance Steering Committee (“ISCSC”), oversees management-system performance, material risks, incidents, exceptions, audit findings, regulatory developments and continual-improvement actions.

Designated owners across information security, privacy, AI governance, legal, GRC, engineering, product, DevSecOps, IT and business operations are accountable for implementing and operating controls within their respective areas.

TestMu’s governance arrangements include the following:

- **Policy governance:** Policies, standards, procedures and supporting records are documented, approved by authorized personnel, communicated to relevant stakeholders, version-controlled and reviewed periodically or following material changes. All workforce members acknowledge these policies at onboarding and annually thereafter.
- **Integrated risk management:** Enterprise, information-security, cybersecurity, privacy, product, supplier, operational and AI-related risks and opportunities are identified, assessed, treated, monitored, accepted or escalated using documented criteria. Risk assessments are performed at least annually.
- **AI governance:** AI systems and approved AI tools are subject to defined accountability, lifecycle governance, risk and impact assessment, data governance, human oversight, testing, monitoring, incident management and change control proportional to their intended use and potential impact.
- **Compliance-obligation management:** Applicable legal, regulatory, contractual and standards-based obligations are recorded and periodically evaluated. Relevant changes are assessed for applicability, risk, implementation requirements and required updates to controls, policies, products or customer commitments.
- **Performance monitoring:** Control objectives, key performance indicators, key risk indicators, incidents, audit results, corrective actions, exceptions and residual risks are reported to appropriate management and governance forums.
- **Management review and assurance:** Management periodically (at least annually) reviews the continuing suitability, adequacy and effectiveness of the ISMS, PIMS and AIMS, including changes in business context, interested-party requirements, risks, audit outcomes and improvement opportunities.

- **Exception management:** Control or policy exceptions require documented business justification, risk assessment, compensating controls, accountable approval, defined ownership and an expiry or reassessment date.
- **Corrective action and continual improvement:** Identified nonconformities, control deficiencies and audit findings are documented, investigated and addressed through proportionate corrective actions, root-cause analysis and effectiveness verification.

2.1 India-Specific Applicability

For TestMu's India operations and relevant processing activities, the compliance register evaluates, as applicable:

- The Information Technology Act, 2000 and associated rules, directions and amendments;
- The Digital Personal Data Protection Act, 2023 and the Digital Personal Data Protection Rules, 2025, in accordance with their applicable commencement and transition provisions;
- Directions issued by the Indian Computer Emergency Response Team ("CERT-In") under Section 70B of the Information Technology Act, including applicable cyber-incident reporting, time-synchronization, log-retention and cooperation requirements;
- Applicable employment, workplace-safety, corporate, anti-bribery, environmental and electronic-record requirements; and
- Sector-specific cybersecurity and data-protection requirements applicable to TestMu or contractually flowed down by regulated customers.

The Securities and Exchange Board of India ("SEBI") Cybersecurity and Cyber Resilience Framework and related circulars are applied where TestMu is directly within scope or where relevant and proportionate requirements are contractually flowed down by a SEBI-regulated customer. Inclusion of such requirements does not represent that TestMu is itself a SEBI-regulated entity unless expressly applicable.

2.2 Control-Framework Alignment

TestMu's control framework is designed with reference to relevant requirements and guidance, including:

- ISO/IEC 27001:2022 and ISO/IEC 27002:2022;
- ISO/IEC 27017:2015 for cloud-security controls;
- ISO/IEC 27701:2025 for privacy information management;
- ISO/IEC 42001:2023 for artificial intelligence management systems;
- ISO/IEC 23894 for AI risk management;
- SOC 2 Trust Services Criteria;
- NIST Cybersecurity Framework and applicable NIST publications;
- NIST AI Risk Management Framework;
- Cloud Security Alliance guidance;
- OWASP application-security and generative-AI security guidance; and
- Applicable privacy, cybersecurity, digital-resilience and artificial-intelligence laws.

3. People and Organizational Measures

TestMu maintains personnel-security measures throughout the employment and engagement lifecycle. These measures apply, as appropriate, to employees, contractors, consultants, temporary personnel and other workforce members with access to TestMu information, systems, facilities or customer data.

- **Pre-employment screening:** Role-appropriate background verification is performed where lawful, proportionate and relevant to the individual's responsibilities and level of access. Screening may include identity, employment, education, professional-reference, criminal-record or other permissible checks.
- **Employment and contractual obligations:** Workforce members and relevant contractors are subject to documented confidentiality, acceptable-use, information-security, privacy, intellectual-property, responsible-AI and data-protection obligations. Such obligations continue after termination where legally and contractually applicable.
- **Code of conduct:** Personnel are required to follow TestMu's Code of Business Conduct and Ethics and applicable policies addressing professional behaviour, conflicts of interest, anti-bribery and anti-corruption, confidentiality, legal compliance and reporting of concerns.
- **Security, privacy and AI awareness:** Training is provided during onboarding and periodically thereafter. Training covers information security, privacy, phishing and social engineering, acceptable use, incident reporting, secure remote working, data handling and responsible use of AI.
- **Role-based training:** Additional training is assigned according to role and risk. This may include secure software development, cloud security, DevSecOps, privileged-access management, privacy engineering, incident response, regulatory compliance, AI lifecycle governance and AI risk or impact assessment.
- **Training effectiveness:** Completion is monitored and retained as evidence. Awareness activities may include periodic communications, assessments, simulations, policy acknowledgements and targeted retraining where gaps are identified.
- **Joiner, mover and leaver controls:** Documented processes coordinate identity creation, access authorization, role changes, device allocation, asset recovery and timely access revocation. Access is reviewed and adjusted when responsibilities change and revoked promptly when employment or engagement ends.
- **Access accountability:** Unique user identities, least-privilege access, segregation of duties, privileged-access controls and periodic access reviews are used to reduce unauthorized access and conflicts between incompatible responsibilities.
- **Consultants and third-party personnel:** Access to TestMu systems is subject to the same confidentiality, acceptable use, training and screening requirements as employees, including access revocation and disciplinary consequences.
- **Conflicts of interest:** Personnel are expected to disclose actual or potential conflicts of interest. Identified conflicts are evaluated, documented and managed through appropriate safeguards, reassignment, approval or other mitigating actions.

- **Policy compliance and disciplinary process:** Suspected policy violations are investigated through documented and fair processes. Appropriate corrective or disciplinary action may be taken in accordance with applicable law, contractual terms and internal procedures.
- **Remote and hybrid working:** Remote-working requirements address approved and managed devices, multifactor authentication, secure connectivity, protection from unauthorized observation or access, appropriate handling of confidential information, secure disposal, physical workspace safeguards and timely reporting of security or privacy incidents.
- **Personnel confidentiality and privacy:** Access to workforce and candidate information is restricted to authorized personnel and processed in accordance with applicable privacy, employment and records-retention requirements.
- **Reporting and non-retaliation:** Workforce members are required to promptly report suspected security incidents, privacy events, AI-related concerns, unethical conduct or policy violations through approved channels. Good-faith reporting is protected in accordance with TestMu policy and applicable law.
- **Employee Exits:** Cloud Infrastructure team, Administration, IT, and HR team ensures that the accesses to all information and assets granted to the employee are returned and revoked.

4.Assets, Information and Configuration Management

TestMu maintains risk-based controls to identify, classify, protect, configure, monitor and retire information and technology assets throughout their lifecycle.

- **Asset inventory:** Information, software, infrastructure, cloud resources, endpoints, source-code repositories, data stores, APIs, cryptographic assets, AI systems, AI models, datasets, approved AI tools and third-party services are inventoried as appropriate and assigned accountable owners.
- **Ownership and accountability:** Asset owners are responsible for determining appropriate classification, access, protection, retention, acceptable use, risk treatment and disposal requirements.
- **Information classification:** Information is classified and handled according to its sensitivity, business value, legal and contractual requirements and potential impact if disclosed, altered, lost or made unavailable.
- **Acceptable use:** Assets and information may be used only for authorized business purposes and in accordance with TestMu's acceptable-use, information-security, privacy and responsible-AI requirements.
- **Secure configuration:** Risk-based configuration baselines and hardening standards based on industry-leading practices defined by the Center for Internet Security are applied to relevant operating systems, cloud services, networks, applications, databases, endpoints, containers and other technology components.
- **Infrastructure as code:** Infrastructure-as-code and automated deployment controls are used where appropriate to promote consistency, traceability, peer review, repeatability and controlled configuration changes.

- **Configuration and change control:** Material configuration changes are authorized, tested, reviewed and traceable. Emergency changes are subject to defined approval, documentation and post-implementation review requirements.
- **Configuration-drift management:** Relevant production environments are monitored for unauthorized or unexpected changes, and material deviations are investigated and remediated according to risk.
- **Endpoint security:** Corporate endpoints are protected, as applicable, through centrally managed security configurations, full-disk encryption, endpoint detection and response, anti-malware capabilities, device management, security patching and remote-lock or remote-wipe functions.
- **Software and repository management:** Access to source-code repositories and development systems is restricted based on role and business need. Changes are traceable to authorized users and subject to applicable review, testing and approval controls.
- **Removable media and transfer restrictions:** Removable media, external storage devices and unauthorized data-transfer channels are restricted or disabled according to risk. Approved transfers are subject to appropriate authorization and protection measures.
- **Cloud and service inventory:** Approved cloud platforms, software-as-a-service applications, development tools, AI services and supporting third parties are recorded and assessed through applicable security, privacy, AI-governance and supplier-risk processes.
- **Capacity and system-health monitoring:** Capacity, availability, performance, resource utilization, system health and relevant service dependencies are monitored for production services to support reliable operation and timely remediation.
- **Asset return and disposal:** TestMu assets are returned when no longer required or upon termination of employment or engagement. Information and storage media are securely deleted, sanitized or destroyed using methods appropriate to the media, classification and applicable retention requirements.
- **Periodic review:** Asset inventories, ownership, classifications and configurations are reviewed periodically and following material changes to help ensure that records remain complete, accurate and aligned with the operating environment.

5. Identity and Access Management

TestMu maintains identity and access-management controls designed to ensure that access to information, systems and services is limited to authorized users, devices and processes according to approved business requirements.

- **Access-control principles:** Access is granted according to least privilege, need-to-know, need-to-use, segregation of duties and role-based authorization principles.
- **Unique identities:** All TestMu personnel who require access to the TestMu corporate network must have a valid, unique identifier, password, and MFA, in order to authenticate to any internally-hosted service on the TestMu corporate network. Shared or generic accounts are restricted and permitted only where technically or operationally necessary, formally authorized and subject to additional monitoring and accountability controls.

- **Access authorization:** Access requests require documented business justification and approval from an authorized manager, system owner or other designated approver before access is provisioned.
- **Strong authentication:** Multifactor authentication is enforced for relevant corporate, cloud, administrative and production access. Single sign-on is used where appropriate to centralize authentication and support consistent access-control enforcement.
- **Customer authentication:** SAML 2.0-based single sign-on is supported for customers on applicable plans or service configurations. Customers are responsible for appropriately configuring and administering their identity provider and assigned user access.
- **Privileged-access management:** Administrative, privileged and production access is restricted to authorized personnel. Such access is approved, limited in duration or provided on a just-in-time basis where supported, logged and periodically reviewed.
- **Production access:** Access to production environments and customer data is limited to authorized personnel with a documented business or support requirement. Access is subject to strong authentication, least privilege, logging and management oversight.
- **Service identities and machine access:** Service accounts, API credentials, automation identities and machine-to-machine access are restricted to defined purposes and granted only the permissions required for their intended function.
- **Credential and secrets protection:** Passwords, authentication secrets, private keys, API tokens and service credentials are protected using approved cryptographic methods. Application and infrastructure secrets are stored in managed secrets-management systems where appropriate and rotated according to risk, sensitivity and technical capability.
- **Access lifecycle management:** Joiner, mover and leaver processes support timely creation, modification and revocation of access. Access is adjusted when responsibilities change and removed promptly when no longer required.
- **Periodic access review:** User, privileged, service and third-party access is reviewed periodically based on system sensitivity and risk. Dormant, excessive, conflicting, expired or otherwise unnecessary access is removed or remediated.
- **Authentication safeguards:** Password and authentication requirements are defined according to applicable risk and system capabilities. Controls may include minimum-password requirements, failed-login protections, session management, credential rotation and prevention of known or compromised passwords.
- **TestMu enforces strong password security** through an 8-character minimum with mixed case, numbers, and symbols, 60-day mandatory rotation, and reuse prevention. Brute-force protection is achieved via account lockout after 5 failed attempts and rate limiting on repeated attempts from the same email. Passwords are stored using bcrypt hashing with random salting, vaults use approved encryption, and resets are handled only through IAM-administered, time-limited links sent to pre-registered contact channels.
- **Remote administrative access:** Remote administrative access uses approved secure channels, managed endpoints, strong authentication and appropriate logging and monitoring. Direct or unmanaged administrative access is restricted.

- **Session management:** User and administrative sessions are protected through appropriate token security, expiration, revocation and reauthentication controls based on the sensitivity of the service and activity.
- **Third-party access:** Supplier and contractor access is authorized, limited to the approved purpose and duration, monitored as appropriate and revoked when no longer required.
- **Tenant authorization and isolation:** Customer accounts are uniquely associated with tenant identifiers. Authorization controls validate user, account and tenant context to prevent unauthorized access to another customer's environment, configuration or data.
- **Logging and monitoring:** Relevant authentication events, access changes, privileged activities and failed-access attempts are logged and monitored according to risk and applicable retention requirements. Suspected unauthorized access is investigated through TestMu's incident-management process.

6. Secure Product Development and Change Management

TestMu applies security, privacy, resilience and responsible-AI controls throughout its Agile product-development and technology-change lifecycle. These controls cover product planning, architecture, design, development, integration, testing, evaluation, release, deployment, operation, monitoring, maintenance and retirement.

The controls apply to conventional software, AI-enabled functionality, generative-AI components, large language models, agentic workflows, autonomous or semi-autonomous AI/QA agents, integrations, APIs, plugins and supporting cloud infrastructure.

6.1 Agile and Secure Development Lifecycle

- **Security, privacy, resilience and responsible-AI** requirements are incorporated into product roadmaps, epics, user stories, architecture decisions, acceptance criteria and definitions of ready and done.
- **Cross-functional teams**—including product, engineering, quality assurance, DevOps/DevSecOps, security, privacy, GRC and AI-governance personnel participate according to the nature and risk of the change.
- Security and privacy requirements are reviewed during relevant Agile activities, including backlog refinement, sprint planning, design review, implementation, testing, release readiness, sprint review and retrospective processes.
- Product owners and designated control owners are responsible for ensuring that applicable security, privacy and AI requirements are appropriately prioritized and addressed.
- Security defects, privacy issues, AI-control gaps and technical debt are recorded, risk-ranked, assigned to accountable owners and tracked through remediation or formally approved risk acceptance.
- Retrospectives, post-implementation reviews and incident lessons learned are used to identify opportunities to improve engineering practices, controls and automation.

6.2 Security, Privacy and Responsible AI by Design

- **Security, privacy, data-protection, accessibility, resilience and responsible AI** requirements are identified during product planning and translated into appropriate design, implementation, testing and operational controls.
- **Material products, features, integrations and architectural changes are evaluated** for information security, privacy, tenant isolation, data flows, regulatory impact, human oversight and responsible AI considerations.
- **Data-protection-by-design measures include** purpose limitation, data minimization, access restriction, appropriate retention, deletion, transparency and protection of personal or confidential information.
- **AI enabled capabilities are designed** with safeguards proportionate to their intended purpose, level of autonomy, reasonably foreseeable misuse and potential impact on customers, individuals and other stakeholders.

6.3 Architecture Review and Threat Modelling

- Risk-based architecture and design reviews are performed for material new products, features, integrations and infrastructure changes before production release.
- Threat modelling considers assets, identities, trust boundaries, data flows, external interfaces, APIs, tenant-isolation controls, attack surfaces, dependencies, abuse cases and failure scenarios.
- AI and agentic threat modelling additionally considers prompt injection, indirect prompt injection, insecure output handling, excessive agency, privilege escalation, tool misuse, model or data poisoning, sensitive-information disclosure, hallucination, unsafe actions, denial of service and unauthorized cross-tenant access.
- Agentic workflows are evaluated for the combined risk arising from models, prompts, memory, retrieval sources, tools, APIs, plugins, credentials, orchestration logic and external systems.
- Security and privacy assumptions, material risks, required mitigations and residual risks are documented and tracked where appropriate.

6.4 Agentic AI Engineering Controls

Agentic AI systems are subject to additional safeguards proportionate to their autonomy, access and potential impact:

- **Purpose and authority boundaries:** Each agent or agentic workflow has a defined purpose, intended users, authorized actions, data-access boundaries and prohibited activities.
- **Least Autonomy:** Agents are provided only the tools, permissions, data and execution capabilities necessary for their approved purpose.
- **Tool and API control:** Access to tools, plugins, APIs, browsers, code-execution environments and external systems is authenticated, authorized and restricted according to risk.
- **Action validation:** Inputs, instructions, intermediate reasoning artefacts where retained, tool calls, parameters and outputs are validated as appropriate before further processing or execution.

- **High-impact actions:** Destructive, security-sensitive, externally consequential or otherwise high-risk actions require appropriate confirmation, human approval or another independent control before execution.
- **Execution isolation:** Agent-generated code and untrusted content are executed only in appropriately restricted, isolated or sandboxed environments where technically applicable.
- **Memory and context protection:** Persistent and temporary agent memory is governed through access control, data minimization, tenant segregation, retention and deletion requirements.
- **Prompt-injection resistance:** Controls are implemented to distinguish trusted instructions from untrusted content and to restrict the ability of retrieved or user-supplied content to override authorized system behaviour.
- **Output handling:** Agent-generated outputs are treated as untrusted until appropriately validated, particularly before use in code execution, database operations, external communications or security-sensitive workflows.
- **Human oversight:** Human-review and intervention mechanisms are implemented according to the risk and impact of the agentic activity.
- **Safe interruption:** Material agentic workflows include appropriate methods to pause, disable, terminate, contain or roll back activity when unsafe, unauthorized or unexpected behaviour is identified.
- **Auditability:** Relevant prompts, responses, tool invocations, actions, errors, approvals and security events are logged where appropriate, subject to privacy, confidentiality and retention requirements.

6.5 AI-Assisted Software Development

- Use of generative AI, coding assistants and autonomous development agents is limited to approved tools, accounts and business purposes.
- Developers must not submit customer data, credentials, source code, personal data, confidential information or other restricted content to unauthorized or unapproved AI services.
- AI-generated code, scripts, configurations, test cases and documentation are treated as untrusted contributions and remain subject to human accountability.
- AI-generated changes must undergo applicable peer review, security testing, functional testing, dependency analysis and approval before production deployment.
- AI-generated code is evaluated for security weaknesses, inaccurate assumptions, insecure dependencies, licensing risks, embedded secrets, malicious or unexpected functionality and maintainability.
- Autonomous development agents operate under defined repository, branch, tool, network and deployment permissions. They are not permitted to independently approve or deploy material production changes unless an expressly approved control design provides equivalent independent validation.
- Material use of AI-assisted development tools is subject to supplier-risk, privacy, data-handling and responsible-AI requirements.

6.6 Environment and Data Segregation

- Development, testing, staging and production environments are logically segregated, with access restricted according to role and business need.
- Production customer data is not used for development or testing unless specifically authorized, necessary for an approved purpose and protected through appropriate minimization, masking, isolation, access, retention and deletion controls.
- Synthetic, anonymized, or otherwise non-production data is preferred for development and testing where feasible.
- Production credentials, secrets and cryptographic keys are segregated from non-production environments.
- Test environments and agentic execution environments are configured to prevent unauthorized access to production systems, customer tenants or external resources.

6.7 Source-Code and Repository Controls

- Source code, prompts, agent instructions, infrastructure definitions, configurations and relevant AI artefacts are maintained in approved repositories with role-based access and traceable change history.
- Protected branches, peer review, approval requirements and merge controls are applied according to repository and change risk.
- Direct changes to protected production branches are restricted.
- Material changes are linked to an authorized user story, issue, ticket, change request or equivalent record.
- Repository access, administrative permissions, service identities and integration tokens are periodically reviewed.

6.8 Automated DevSecOps and CI/CD Controls

TestMu integrates automated security and quality controls into build and deployment pipelines where appropriate. These may include:

- Static application security testing;
- Dynamic application security testing;
- Interactive or runtime application testing where applicable;
- Software-composition and dependency analysis;
- Secret and credential scanning;
- Infrastructure-as-code scanning;
- Container and image scanning;
- API-security testing;
- License and provenance checks;
- Malware or malicious-package detection;
- Unit, integration, regression and security testing;
- Code-quality and coverage checks; and
- Policy-as-code and configuration-compliance checks.

Automated findings are evaluated according to severity, exploitability, exposure and business impact. Defined quality or security gates may prevent promotion or deployment when unacceptable conditions are identified.

Exceptions to mandatory pipeline controls require documented risk assessment, accountable approval, compensating controls and a defined remediation or expiry date.

6.9 Dependency and Software Supply-Chain Security

- Open-source software, libraries, packages, container images, models and other third-party components are inventoried or tracked as appropriate.
- Components are obtained from approved or trusted sources where feasible and evaluated for known vulnerabilities, malicious content, licensing concerns, integrity and maintenance status.
- Material vulnerabilities and supply-chain risks are prioritized according to severity, exploitability, exposure, availability of remediation and potential customer impact.
- Software bills of materials or equivalent component records may be maintained or provided where appropriate to the product, applicable requirement, customer commitment and available tooling.
- Build systems, package repositories, artefact repositories and deployment pipelines are protected against unauthorized modification.
- Relevant build artefacts are versioned, traceable and integrity-checked as appropriate.

6.10 Secrets and Credential Management

- Credentials, cryptographic keys, API tokens and other secrets must not be intentionally embedded in source code, prompts, scripts, configuration files or AI-agent instructions.
- Managed secrets systems are used where appropriate to store and provide controlled access to sensitive credentials.
- Automated secret scanning is applied to relevant repositories and pipelines.
- Secrets are scoped according to least privilege, rotated based on risk and revoked when compromised or no longer required.
- Agentic systems must not expose credentials or sensitive tokens through prompts, responses, logs or tool outputs.

6.11 AI Evaluation and Adversarial Testing

Before material AI-enabled or agentic functionality is released, proportionate evaluation may include:

- Functional accuracy and task-completion testing;
- Reliability, consistency and robustness testing;
- Security and adversarial testing;
- Prompt-injection and jailbreak testing;
- Tool-use and excessive-agency testing;
- Sensitive-information disclosure testing;
- Hallucination and unsupported-output testing;
- Bias, fairness and harmful-content evaluation where relevant;

- Tenant-isolation and authorization testing;
- Human-oversight and escalation-path testing;
- Performance, latency, capacity and failure-mode testing; and
- Testing of fallback, interruption and recovery mechanisms.

Evaluation criteria, test results, known limitations, required mitigations and release decisions are documented according to risk.

6.12 Change Classification, Approval and Release

- Changes are classified according to their nature, complexity, security impact, privacy impact, AI risk, customer impact and operational criticality.
- Material changes require documented review, testing and approval before production release.
- Release evidence may include requirements, risk classification, code review, security-testing results, AI-evaluation results, privacy review, approvals, deployment records and post-release validation.
- Material changes to AI models, providers, prompts, tools, permissions, autonomy, data sources, retrieval mechanisms or intended use are evaluated to determine whether updated risk or impact assessment is required.
- Deployment permissions are restricted, and relevant build and release activities are logged and attributable to authorized identities.
- Segregation of duties or equivalent independent validation is applied to material production changes.

6.13 Automated Deployment, Rollback and Recovery

- Changes are deployed through controlled and repeatable CI/CD processes where appropriate.
- Progressive delivery, feature flags, staged rollout, canary deployment or equivalent techniques may be used according to change risk and service architecture.
- Material releases include appropriate rollback, recovery, disablement or mitigation arrangements.
- Code promotions use Blue-Green Deployment—two identical environments where updates are deployed and tested on the idle one before traffic is switched over, enabling zero-downtime releases and instant rollback if issues arise.
- AI and agentic features may be restricted, suspended or disabled where monitoring identifies unsafe, unauthorized or materially degraded behaviour.
- Deployment outcomes are monitored for functional errors, security events, performance degradation, privacy issues, AI anomalies and unintended impacts.

6.14 Emergency Changes

- Emergency changes are limited to urgent security, availability, legal, privacy or operational requirements.

- Emergency changes are implemented by authorized personnel and subject to proportionate testing and approval based on the circumstances.
- The change, justification, risk, implementation actions and outcome are documented.
- Emergency changes undergo retrospective review, validation and any required corrective action.

6.15 Vulnerability and Defect Remediation

- Security vulnerabilities, privacy defects, AI-control weaknesses and other material issues identified during development, testing or production operation are recorded and risk-ranked.
- Remediation priority considers severity, exploitability, exposure, affected data, customer impact, service criticality and available mitigating controls.
- Remediation timelines by severity: **Critical – 0–7 days, High – 15 days, Medium – 30 days, Low – 45 days.**
- Remediation is tracked to closure or subject to documented risk acceptance, compensating controls and an approved review date.
- Material vulnerabilities or incidents are handled through applicable vulnerability-management, incident-response and customer-notification processes.

6.16 Post-Deployment Monitoring and Improvement

- Relevant production releases are monitored for availability, security, privacy, performance, regressions, anomalous activity and unexpected behaviour.
- AI and agentic systems are monitored, as appropriate, for output quality, tool-use failures, unauthorized actions, prompt attacks, data leakage, abnormal resource consumption and deviations from intended behaviour.
- Customer feedback, operational metrics, incidents, evaluation results, audit findings and emerging threats are used to improve product design and controls.
- Significant failures or incidents are subject to root-cause analysis, corrective action and lessons-learned review.

6.17 Retirement and Decommissioning

Products, features, AI models, agents, integrations and supporting components reaching end of life are retired through controlled processes addressing:

- Customer and stakeholder communication where required;
- Dependency and integration management;
- Revocation of access, credentials, tools and service identities;
- Data retention, export, return and deletion requirements;
- Removal of obsolete code, prompts, models and infrastructure;
- Secure disposal or sanitization of associated assets; and
- Preservation of required legal, audit and operational records.

7. Cloud, Infrastructure and Network Security

TestMu applies layered cloud, infrastructure and network-security controls based on system criticality, data classification, deployment model and contractual requirements.

- Production, development, testing and corporate environments are logically segregated using cloud accounts, virtual private clouds, subnets, security zones and routing controls.
- Firewalls, web application protections, DDoS safeguards, rate limiting and appropriate ingress and egress controls protect service boundaries.
- Publicly exposed services, administrative interfaces, ports, protocols and firewall rules are minimized and periodically reviewed.
- Systems, workloads, containers and cloud services are securely configured, hardened, patched and monitored. Material security-posture and configuration findings are risk-ranked and remediated.
- Administrative and service access is restricted through role-based authorization, least privilege, strong authentication, managed identities and appropriate logging.
- Infrastructure, network, authentication and application telemetry supports anomaly detection, investigation and incident response.
- APIs and integrations use appropriate authentication, authorization, input validation, rate limiting, secrets protection and monitoring.
- Customer accounts are associated with unique tenant identifiers. Application and authorization controls validate tenant context to prevent unauthorized cross-customer access.
- Test execution uses ephemeral virtual machines, containers, browser sessions or devices where applicable, followed by automated cleanup, reset or sanitization.
- AI agents and agentic workflows operate within defined permission and network boundaries. Access to tools, APIs, plugins, repositories and external destinations is restricted according to purpose and risk.
- Untrusted agent-generated code or content is executed in restricted or isolated environments where technically applicable. Material agent actions and tool invocations are logged and capable of being suspended or terminated.
- Production services use appropriate redundancy, availability-zone distribution, capacity monitoring, scaling and recovery arrangements.
- Regional deployment, data-location and remote-access controls are applied according to the subscribed service, available architecture, applicable law and contractual commitments.
- Cloud and network environments are subject to vulnerability scanning, security assessment and periodic penetration testing. Identified findings are tracked through remediation, mitigation or approved risk acceptance.
- At TestMu, wireless corporate network access is provided through company owned Access Points (APs) secured using WPA3 encryption. Access to the corporate wireless network is restricted to authorized users, who are required to authenticate using their valid corporate credentials.

8. Cryptography and Key Management

TestMu applies risk-based cryptographic controls to protect customer data, credentials, communications and other sensitive information.

- Customer data is encrypted in transit using TLS 1.2 or higher and at rest using AES-256 or equivalent cloud-native encryption, where applicable.
- Cryptographic keys are managed through approved cloud key-management or secrets-management services, with restricted access, least privilege, separation of duties, logging and lifecycle controls.
- Keys, certificates, tokens and secrets are securely generated, stored, distributed, rotated, revoked, expired and retired according to their sensitivity, risk and technical capability.
- Application and infrastructure secrets are stored in approved secrets-management systems and are not intentionally embedded in source code, scripts, prompts, agent instructions or configuration files.
- Passwords are protected using strong salted, adaptive and industry-accepted hashing methods. TestMu does not intentionally store user passwords in plaintext.
- Approved cryptographic algorithms, protocols, key lengths and configurations are used. Deprecated or vulnerable cryptography is disabled or replaced through managed change and remediation processes.
- Keys for production environments are separate and different from those of non-production environments.
- Private keys and other sensitive cryptographic material are accessible only to authorized users, services and workloads with a documented business requirement.
- Certificate validity, expiration and renewal are monitored through automated or operational processes, as appropriate.
- Cryptographic failures, unauthorized key access and suspected compromise are handled through applicable incident-response, credential-revocation and key-rotation procedures.
- Customer-managed encryption keys or other enhanced key-management arrangements are provided only where technically available and expressly included in the applicable service or contractual arrangement.

9. Data Protection, Privacy and Lifecycle Controls

TestMu applies privacy and data-protection controls throughout the collection, use, storage, transfer, disclosure, retention and deletion of personal and customer data.

- Processing is limited to documented and legitimate purposes, customer instructions and applicable legal requirements, with data minimization, accuracy, storage limitation, confidentiality and privacy by design and by default.
- TestMu generally acts as a processor or service provider for customer Test-execution data and as a controller or business for Account, workforce, website-user and business-contact data. Specific roles depend on the processing activity and contractual arrangement. Test execution data and other customer content belongs to the customer. TestMu does not require and its services do not process special categories of personal data or other regulated data within Test execution data.

- Personal-data inventories, processing records, data-flow documentation, lawful-basis assessments, retention requirements and privacy or data-protection impact assessments are maintained where applicable.
- Customer accounts and data are logically segregated through unique tenant identifiers and authorization controls. Access to customer data is limited to authorized personnel with a documented business need and is logged as appropriate.
- Customer Test-execution data is retained according to the subscribed service, customer configuration and contract. The standard retention period is generally 30 days unless another period is selected or agreed.
- Security and infrastructure logs are generally retained for 3 to 6 months, and troubleshooting records for up to 90 days, subject to their purpose, service configuration, legal requirements and contractual commitments.
- TestMu does not use personal data to make solely automated decisions, including profiling. AI generated outputs within the TestMu platform are with the authorised users and are not used to evaluate and make determinations about natural persons.
- Data-subject and customer requests concerning access, correction, deletion, restriction, portability, objection or withdrawal of consent are handled through documented procedures according to TestMu's processing role and applicable law.
- Privacy notices and consent or other lawful processing mechanisms are provided where TestMu determines the purposes and means of processing.
- International transfers are supported through applicable contractual and legal safeguards, which may include data processing agreements, Standard Contractual Clauses, the UK Addendum, adequacy mechanisms and transfer-risk assessments.
- For India, TestMu implements applicable Data Fiduciary or Data Processor requirements under the Digital Personal Data Protection Act, 2023 and the Digital Personal Data Protection Rules, 2025, in accordance with their commencement and transition provisions. Relevant controls include notice and consent or permitted-use requirements, reasonable security safeguards, processor governance, rights and grievance handling, retention and deletion, breach response and additional obligations if TestMu is designated as a Significant Data Fiduciary.
- Applicable provisions of the Information Technology Act, 2000, the SPDI Rules, 2011 and associated requirements remain tracked until superseded, repealed or determined no longer applicable.
- Customer data processed through TestMu's enterprise AI capabilities is not used to train, retrain or fine-tune models made available to other customers, in accordance with applicable service terms.
- Data-loss prevention, masking, redaction, access restrictions, encryption and secure-transfer mechanisms are applied according to information classification and processing risk.
- Personal and customer data is retained only for the applicable purpose, service, legal or contractual period and is securely deleted or anonymized when no longer required.
- Data and media sanitization use methods designed to render information unrecoverable, including controls aligned with NIST SP 800-88 where applicable. Data in backups is removed through controlled backup-expiry and deletion cycles.

- Privacy incidents and personal-data breaches are assessed, contained, documented and notified in accordance with applicable law, TestMu's processing role and contractual requirements.

10. Logging, Monitoring and Security Operations

TestMu maintains risk-based logging, monitoring and security-operations capabilities to detect, investigate and respond to operational, security, privacy and AI-related events.

- Relevant authentication, privileged-access, system, application, API, cloud, network and security events are logged and protected against unauthorized access, alteration and deletion.
- Centralized monitoring and security analytics correlate relevant events and generate alerts for investigation and response by designated personnel.
- Monitoring covers service availability, suspicious access, anomalous behaviour, malware, abuse, potential data exfiltration, configuration changes, control failures and indicators of compromise.
- Key logging criteria include capturing user IDs, system activities, event details, and network information.
- AI and agentic systems are monitored, as appropriate, for abnormal tool use, unauthorized actions, prompt attacks, data leakage, excessive resource consumption and deviations from intended behaviour.
- Log access is restricted according to least privilege. System clocks are synchronized with approved time sources to support accurate event correlation and investigation.
- Log-retention periods are determined according to operational, security, privacy, legal, investigative and contractual requirements.
- Alerts are classified, prioritized, investigated, escalated and documented according to severity and potential business or customer impact.
- Security operations use documented procedures, threat intelligence and defined escalation paths to support detection, containment, investigation and recovery.
- Continuous monitoring and on-call response capabilities support material production, availability and security events.
- Monitoring activities are performed with appropriate data minimization, confidentiality, access restriction and privacy safeguards.
- For systems and entities subject to CERT-In Directions, TestMu enables relevant ICT-system logs, synchronizes system clocks with approved time sources, retains required logs securely for at least 180 days within India and makes them available to CERT-In when lawfully required. Longer retention applies where required by law, contract or an authorized investigation.

11. Vulnerability, Threat and Assurance Management

TestMu maintains risk-based vulnerability, threat and assurance processes covering applications, APIs, cloud infrastructure, networks, endpoints, dependencies and AI-enabled systems.

- Internal vulnerability assessments are performed at least quarterly and external vulnerability assessments are performed annually and/or following material changes, based on system criticality and risk.
- Independent penetration testing of relevant platform components is performed at least annually and, where appropriate, after significant changes.
- Security findings are validated, risk-rated, assigned to accountable owners and tracked through remediation, mitigation or formally approved risk acceptance.
- Remediation priority considers severity, exploitability, exposure, affected data, customer impact, service criticality and available compensating controls.
- Remediation timelines by severity: **Critical – 0–7 days, High – 15 days, Medium – 30 days, Low – 45 days.**
- Threat intelligence, vendor advisories, dependency alerts, attack-surface information and responsible-disclosure channels support identification and prioritization of emerging threats.
- Internet-facing assets and material changes in external exposure are monitored and assessed through appropriate attack-surface and security-testing processes.
- AI-enabled and agentic systems are subject to proportionate security and adversarial testing, including prompt-injection, jailbreak, sensitive-data disclosure, insecure output handling, excessive agency, tool misuse and unauthorized action scenarios.
- Open-source components, libraries, container images and third-party dependencies are monitored for relevant vulnerabilities and supply-chain risks.
- Remediation exceptions require documented justification, risk assessment, compensating controls, accountable approval and a defined review or expiry date.
- Material remediation is validated through rescanning, retesting or other appropriate evidence before closure.
- Independent audits and assurance activities include applicable ISO certifications and SOC 2 Type II examinations. Certification and attestation claims are limited to their current scope and validity.
- Current certificates, reports and supporting assurance evidence may be provided to customers subject to availability, confidentiality, legal and contractual restrictions.

12. Physical and Environmental Security

TestMu applies proportionate physical and environmental safeguards to offices, equipment and information-processing facilities according to site and asset risk.

- Physical and environmental protections for cloud data centres are operated by approved infrastructure providers and evaluated through relevant independent assurance reports and certifications.
- TestMu offices use appropriate access controls, visitor registration and escort procedures, surveillance, restricted areas and asset-protection measures.
- Physical access is limited to authorized personnel according to business needs. Access rights are reviewed and revoked when no longer required.
- Visitors and third-party personnel are controlled and monitored according to applicable site procedures.

- CCTVs are installed across all vantage points within the office including all the entry and exit points and the footage is retained for a minimum of 90 days.
- Environmental safeguards address power availability, fire detection and suppression, temperature, water leakage and other facility risks where TestMu operates relevant equipment.
- Critical office or technology equipment is protected through appropriate power, backup, maintenance and recovery arrangements based on operational requirements.
- Clear-desk, clear-screen, secure-printing, device-protection and confidential-disposal requirements reduce the risk of unauthorized access, viewing, removal or loss.
- Paper records, storage media and physical assets containing sensitive information are securely stored, transported and disposed of according to classification and retention requirements.
- Corporate devices must not be left unattended in unsecured locations and are protected through applicable encryption, screen-lock and device-management controls.
- Physical-security events, unauthorized access and loss or theft of assets are promptly reported and handled through applicable incident-management procedures.

13. Business Continuity, Backup and Disaster Recovery

TestMu maintains business continuity, backup and disaster-recovery measures designed to support the availability and timely recovery of critical services.

- Business continuity and disaster-recovery plans identify critical services, business dependencies, recovery teams, escalation paths, communications and restoration procedures.
- Business impact and risk assessments support the prioritization of critical processes, systems, data and third-party dependencies.
- Critical service data is backed up or replicated according to defined schedules. Backup access, encryption, integrity, retention and restoration are managed according to risk. Backups are stored in a secure environment with protection against modifications and deletions and access to these backups is restricted to authorized infrastructure personnel and logged.
- Backup and restoration procedures are periodically tested to verify that relevant data and services can be recovered.
- Data sync happens in an active-active model and is equipped to independently handle the load in case of any failures.
- High-availability architecture, service clustering, automated scaling and availability-zone redundancy are used where appropriate to reduce single points of failure.
- Continuity and disaster-recovery exercises are conducted at least annually and following material changes where appropriate. Results, lessons learned and corrective actions are documented and tracked.
- Key suppliers and cloud-service dependencies are considered in continuity and recovery planning.

- Relevant availability incidents, service disruptions and planned maintenance are communicated through TestMu's public service-status capability and other appropriate customer-notification channels.

Recovery Objectives

- **Recovery Time Objective ("RTO"):** The targeted maximum period within which an affected service should be restored following a qualifying disruption.
- **Recovery Point Objective ("RPO"):** The targeted maximum period of data that may be lost, measured from the time of disruption to the most recent recoverable data point.

For applicable standard service commitments, TestMu targets:

- **RTO:** 4 hours
- **RPO:** Less than one hour.

These objectives apply to relevant production services and qualifying disaster-recovery scenarios. Different RTO or RPO commitments may apply according to the product architecture, deployment model, subscribed service or applicable customer contract.

Actual recovery may depend on the nature and severity of the event, third-party dependencies, data integrity, customer-controlled configurations and required security or validation activities. Recovery objectives are planning and design targets and do not constitute guaranteed service levels unless expressly incorporated into an applicable agreement.

14. Supplier and Sub-processor Measures

TestMu maintains a risk-based third-party risk-management process covering suppliers, cloud and infrastructure providers, subprocessors, AI model and API providers, contractors and other third parties supporting its services.

14.1 Due Diligence and Onboarding

Before onboarding, relevant suppliers and subprocessors undergo proportionate security, privacy, AI, compliance, financial and operational due diligence.

The assessment considers service criticality, data sensitivity, processing purpose and location, access, subcontracting, international transfers, business continuity, incident response, vulnerability management, AI data use and exit requirements.

Evidence may include ISO certificates, SOC reports, PCI DSS attestations where relevant, penetration-testing summaries, privacy documentation and business-continuity information.

14.2 Contractual and Security Requirements

Relevant supplier and subprocessors agreements include appropriate requirements for:

- Confidentiality and permitted use;
- Information security and data protection;
- Access restrictions and personnel controls;
- Incident and breach notification;

- Data location and international transfers;
- Retention, return and secure deletion;
- Business continuity and recovery;
- Subcontracting and subprocessors management;
- Audit and assurance evidence; and
- AI data-use, training and secondary-use restrictions, where applicable.

Requirements are proportionate to the service, data and associated risk.

14.3 Ongoing Monitoring and Review

Material suppliers and subprocessors are periodically reviewed based on their risk and criticality.

Changes to service scope, processing location, subprocessors, security posture, AI usage, certifications or control environment are assessed for impact. Incidents, vulnerabilities, audit findings and service failures are reviewed and escalated where appropriate.

Identified risks are remediated, mitigated, contractually addressed, formally accepted or escalated. Third-party access and services are revoked when no longer required.

14.4 Customer Data and Test-Execution Data Access

TestMu applies strict access controls to customer data and test-execution data so that access is authorized, purpose-specific, least-privileged, time-bound where appropriate, monitored and auditable.

- **Default access principle:** TestMu personnel do not routinely access customer data or customer Test-execution data. Access is not granted merely because an individual holds an employee account or technical role.
- **Exceptional support and troubleshooting access:** Where access is necessary to investigate or resolve a customer-authorized support, security, technical or troubleshooting request, temporary access may be provided only to a limited number of specifically authorized personnel.
- **Authorization and time-bound access:** Access requires a documented business purpose, appropriate approval and least privilege. Just-in-time or otherwise time-bound access is used where technically supported.
- **Minimum necessary access:** Access is limited to the minimum data, system, environment, permissions and duration necessary to perform the authorized activity.
- **Customer authorization:** Customer approval or action is obtained before access where required by the product design, support process or contractual arrangement.
- **Logging and revocation:** Relevant temporary, privileged and administrative access is logged and monitored. Access is revoked or expires promptly after completion of the authorized activity.
- **No secondary use:** Access granted for support, troubleshooting, security or another authorized purpose is not used for unrelated analytics, profiling, advertising, AI model training or other unauthorized secondary processing.

- **Accountability and evidence:** Applicable approvals, support tickets, access records, session or activity logs and revocation records are maintained to support traceability and auditability.
- **No sale or disclosure:** TestMu does not sell customer data or disclose it to third parties.

14.5 Subprocessors and Infrastructure-Provider Access

TestMu does not provide subprocessors with routine user accounts, administrative privileges or unrestricted access to TestMu applications, customer environments or customer data.

Subprocessors may process customer data only to the extent technically necessary to provide their contracted services and in accordance with TestMu's documented instructions, contractual safeguards and applicable data-protection requirements.

- Cloud, storage, infrastructure, monitoring and AI service providers may process or host limited data required to deliver their services.
- Such providers are not authorized to independently use customer data for their own unrelated purposes.
- Human access by provider personnel is restricted by the provider's access controls and is expected to occur only when necessary for authorized infrastructure operations, security, support or legal obligations.
- Infrastructure and data-centre providers may have controlled physical access to facilities or underlying equipment. Such physical access does not, by itself, provide routine logical access to TestMu-managed applications, customer accounts or customer data.
- TestMu retains control of application-layer identities, authentication, authorization, tenant isolation and access to TestMu-managed production systems.
- Enterprise AI providers process data according to applicable service terms. Customer data submitted through TestMu's AI capabilities is not used to train, retrain or fine-tune models made available to other customers.

This wording recognizes the technical processing performed by infrastructure and AI providers while confirming that they are not granted routine or unrestricted application-level access to customer environments.

14.6 Subprocessors Transparency

TestMu publishes its current list of relevant subprocessors, their processing purposes and applicable processing locations at: <https://www.testmuai.com/legal/sub-processor/>

Subprocessors changes and customer notifications are managed in accordance with the applicable DPA and contractual terms.

14.7 Regulated-Customer Requirements

Where TestMu supports a regulated customer, proportionate third-party controls may incorporate applicable customer or sector requirements.

For a SEBI-regulated customer, this may include relevant Cybersecurity and Cyber Resilience Framework requirements concerning cyber governance, asset and data classification, access control, security monitoring, vulnerability management, incident cooperation, recovery, audit evidence, cloud services and exit arrangements.

Application of customer-flowed requirements does not mean that TestMu is itself a SEBI-regulated entity unless legally determined.

15. Incident Response and Breach Notification

TestMu maintains a documented incident-response process covering preparation, identification, reporting, triage, containment, eradication, recovery, evidence preservation, communication and lessons learned.

- Security, privacy, availability, supplier and AI-related events are recorded, classified and escalated according to their severity, scope and potential impact.
- Designated teams coordinate technical investigation, containment, service recovery, legal and privacy assessment, customer communications and regulatory reporting.
- Relevant evidence is protected and retained to support investigation, legal obligations, root-cause analysis and corrective action.
- The incident-response process is periodically tested, reviewed through internal assurance activities and assessed as part of applicable ISO and SOC 2 audits. The incident response plan is tested annually through an exercise involving all functions (engineering, security, legal, privacy and customer-facing functions) and lessons learnt through the same are recorded.

15.1 Customer Notification

- As a processor, TestMu notifies the affected customer without undue delay after becoming aware of a confirmed personal-data breach involving customer-controlled personal data, subject to the applicable contract and law.
- TestMu also communicates material security incidents affecting the confidentiality, integrity or availability of a customer's data or subscribed service according to applicable contractual requirements.
- Notifications are provided to the customer's designated contact, account administrator, Customer Success Manager or other agreed communication channel.
- Notifications describe, to the extent reasonably available, the nature of the incident, affected systems or data, likely consequences, containment and mitigation measures, and recommended customer actions.
- Initial information may be provided in phases as the investigation progresses. TestMu may withhold information where disclosure would compromise security, investigation integrity, legal privilege or regulatory obligations.
- The Data Protection Officer, Information Security function and other designated personnel coordinate relevant breach communications.

15.2 Regulatory and Individual Notification

- As a controller, TestMu assesses whether notification to supervisory authorities, regulators or affected individuals is required under applicable law.
- Where the GDPR or UK GDPR applies, TestMu notifies the competent supervisory authority within 72 hours after becoming aware of a notifiable personal-data breach, where feasible, and notifies affected individuals where legally required.
- Where India's DPDP framework applies, TestMu notifies the Data Protection Board of India and affects Data Principals in the form and timeframe required by the provisions then in force.
- Specified cyber incidents subject to CERT-In Directions are reported to CERT-In within six hours of noticing the incident or being informed of it. Available information may be submitted initially and supplemented as the investigation progresses.
- Other regulatory notifications are made according to the applicable jurisdiction, sector, processing role and legal timeframe.

15.3 Post-Incident Improvement

Following a material incident, TestMu performs a proportionate post-incident review to:

- Determine root cause and contributing factors;
- Assess the effectiveness of detection and response;
- Identify control, process or technology improvements;
- Assign and track corrective actions;
- Validate completion and effectiveness; and
- Update risk assessments, procedures, training and monitoring where appropriate.

Security vulnerabilities and suspected incidents may be reported through TestMu's published security channel at security@TestMu.com. Customers may also report incidents through their designated Customer Success Manager or approved support channel.

16. Artificial Intelligence -related Measures

TestMu maintains AI-specific controls through its Artificial Intelligence Management System (AIMS), AI Policy and Responsible AI Use Guidelines. These controls apply proportionately to TestMu-developed or provided AI capabilities and to approved third-party AI systems used internally. They supplement the security, privacy, resilience and supplier controls described elsewhere in this document.

TestMu acts primarily as an AI Provider for its AI-enabled products and services and, where applicable, as an AI Producer/Developer, AI Partner or AI User. Responsibilities are determined according to TestMu's role, intended use, deployment model, level of autonomy, affected stakeholders and applicable law.

- **AI governance and accountability.** TestMu assigns accountable owners, roles and decision rights for AI systems and use cases. Intended purposes, authorized users, affected stakeholders, prohibited or restricted uses, human-oversight requirements and escalation paths are defined and reviewed through AIMS governance.

- **Inventory, classification and lifecycle control.** Relevant AI systems, models, agents, prompts, datasets, APIs, providers and integrations are inventoried and assigned owners. Risk and regulatory classification considers intended use, reasonably foreseeable misuse, autonomy, data sensitivity, affected parties, jurisdiction and potential impact. Material changes trigger reassessment and controlled approval.
- **AI risk and impact assessment.** TestMu evaluates applicable security, privacy, confidentiality, fairness, bias, accuracy, reliability, robustness, safety, transparency, accessibility, intellectual-property and legal risks. Material risks are treated, monitored and reassessed. Unresolved risks require authorized acceptance, exception approval or go/no-go escalation.
- **Customer data and no-training commitment.** Customer data, prompts, inputs, outputs and test-execution data are processed only to provide, operate, support and secure the authorized service. TestMu does not use, or permit its approved enterprise AI provider to use, such information to train, retrain or fine-tune TestMu models or third-party foundation models. Training and fine-tuning using customer data are disabled for the applicable enterprise AI service configuration.
- **Microsoft Azure OpenAI.** TestMu uses Microsoft Azure OpenAI as its approved third-party enterprise AI service provider for applicable AI capabilities. Its use is subject to security, privacy and AI due diligence, contractual safeguards, access controls, data-use restrictions, secure technical configuration and ongoing supplier oversight.
- **Data protection and tenant isolation.** AI data and contextual information are protected through encryption, least-privilege access, tenant identifiers, authorization controls, logical segregation, monitoring, retention and secure-deletion measures. Sensitive data is minimized, masked, redacted or excluded where feasible. Credentials, tokens and other secrets are protected from unauthorized inclusion in prompts, outputs, logs, retrieval sources and agent memory.
- **Secure AI and agentic engineering.** Threat modelling and safeguards address prompt injection, indirect prompt injection, insecure output handling, sensitive-information disclosure, data or model poisoning, supply-chain compromise, excessive agency, tool misuse, retrieval weaknesses, cross-tenant access and unbounded resource consumption. Agents receive only approved tools, data, permissions, execution duration and resource capacity. High-impact, destructive or irreversible actions require human confirmation or equivalent independent safeguards.
- **Testing, validation and robustness.** Risk-based testing, evaluation, verification and validation address applicable accuracy, groundedness, hallucination, reliability, robustness, security, privacy, bias, harmful content, prompt attacks, tool use and fail-safe behaviour. Normal, edge, malformed, adversarial and misuse scenarios are tested as appropriate. Grounding, output validation, permission boundaries, rate limits, timeouts, retry limits, circuit breakers, rollback and safe-disablement measures support resilient operation.
- **Human oversight and transparency.** Users receive appropriate information concerning AI interaction, intended use, material limitations and responsible-use expectations. AI-generated

tests, insights, summaries, code and recommendations are treated as decision-support information unless expressly validated for another purpose. Authorized users can review, intervene, override, stop, correct or escalate AI-supported activities according to risk.

- **Deployment, monitoring and incident response.** Production release requires applicable risk, security, privacy, supplier and evaluation approvals. AI quality, abnormal behaviour, data leakage, unauthorized actions, prompt attacks, provider changes and other relevant indicators are monitored according to risk. AI incidents and near misses may be contained through suspension, rollback or disablement, investigated through TestMu's incident-management process, and used to drive corrective action and continual improvement.
- **Global legal and standards readiness.** TestMu evaluates applicable requirements under the EU AI Act, GDPR and UK GDPR, relevant United States federal and state requirements, India's DPDP framework, and applicable laws in other supported jurisdictions. Controls are designed with reference to ISO/IEC 42001, ISO/IEC 23894, ISO/IEC 42005, the NIST AI Risk Management Framework, OECD AI Principles and applicable OWASP guidance. Specific applicability depends on TestMu's role, the product and deployment model, data processed, jurisdiction and customer use case.
- **Customer assurance and shared responsibility.** TestMu maintains appropriate AI inventory, assessment, testing, approval, monitoring, incident and supplier-governance evidence. Customers remain responsible for lawful inputs, authorized users, connected systems, test objectives, customer-controlled infrastructure and appropriate review of AI-generated outputs. For customer-managed or on-premises deployments, responsibilities are allocated according to the applicable agreement and the systems and components controlled by each party.

17. ESG and Responsible Business Measures

TestMu maintains environmental, social and governance (ESG) and responsible-business measures covering enterprise risk, operations, technology, workforce practices, supplier management and stakeholder reporting. These measures are proportional to TestMu's technology and service-based business model, operating locations and applicable legal obligations. They are informed by the National Guidelines on Responsible Business Conduct (NGRBC), SEBI Business Responsibility and Sustainability Reporting (BRSR/BRSR Core) principles, GRI Standards, UN Sustainable Development Goals, GHG Protocol and relevant climate-target guidance, as applicable or voluntarily adopted.

- **ESG governance and accountability.** TestMu assigns executive oversight, accountable owners and cross-functional responsibilities for ESG objectives, risks, disclosures and improvement plans. Material ESG topics and stakeholder expectations are periodically evaluated across employees, customers, suppliers, communities, investors and regulators. ESG risks and opportunities—including climate, energy, workforce, ethical technology, supply-chain, compliance and reputational matters—are incorporated into enterprise risk management.

- **Ethics and responsible business conduct.** TestMu's Code of Conduct, anti-bribery and anti-corruption, conflicts-of-interest, whistleblowing, human-rights, diversity, workplace, supplier and information-governance requirements support ethical and responsible business conduct. Reported concerns are assessed, investigated and escalated through defined channels, with protection against retaliation.
- **Environmental and climate measures.** TestMu identifies and manages material environmental impacts associated with its offices, employee operations, purchased electricity, business travel, cloud infrastructure, devices and relevant value-chain activities. Energy efficiency is supported through cloud-resource optimization, autoscaling, efficient workload scheduling, virtualization, equipment power management and responsible office practices.
- **Greenhouse-gas emissions and climate risk.** Relevant Scope 1, Scope 2 and material Scope 3 emissions are measured using defined organizational and operational boundaries and recognized calculation methods. Climate-related risks, dependencies and opportunities are considered in business continuity, supplier concentration, data-centre resilience and technology planning. Environmental objectives, indicators, material variances and corrective actions are periodically reviewed.
- **Resource use and waste management.** TestMu seeks to minimize unnecessary energy, water, paper, consumables and waste where material. Electronic equipment is reused, securely refurbished or disposed of through authorized channels. Applicable India operations manage covered electronic waste through authorized recyclers or producer take-back arrangements and retain appropriate disposal evidence in accordance with the E-Waste (Management) Rules, 2022 and subsequent amendments.
- **Workforce, wellbeing and inclusion.** Fair employment, equal opportunity, non-discrimination, accessibility, respectful-workplace and prevention-of-harassment requirements apply throughout the employment lifecycle. TestMu supports employee health, safety, wellbeing, learning and professional development through proportionate programs, training and reporting mechanisms.
- **India workplace requirements.** Applicable Indian employment, wages, social-security, health, safety and workplace requirements are tracked and implemented according to each legal entity's obligations. This includes applicable measures under the Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013, including prevention, reporting, investigation and redressal arrangements.
- **Human rights and grievance mechanisms.** TestMu maintains confidential grievance, ethics and whistleblowing channels with defined investigation and escalation arrangements. Human-rights and modern-slavery risks are considered in operations and supplier assessments, including forced labour, child labour, discrimination, unsafe working conditions and unethical recruitment.
- **Sustainable technology and responsible AI.** Technology and engineering decisions consider efficient computing, storage, data transfer, workload scheduling, model selection and resource utilization without weakening security, reliability or customer requirements. AI risk and impact

assessments consider relevant societal and environmental impacts, fairness, accessibility, affected stakeholders, human agency and resource consumption.

- **Efficient AI and data lifecycle.** Where appropriate, TestMu uses proportionate models, token and resource budgets, rate limits, caching, reuse and monitoring to reduce unnecessary computation and cost. Data minimization, retention controls, secure deletion and infrastructure cleanup reduce unnecessary data storage and processing.
- **Accessibility and inclusive design.** Product accessibility and inclusive-design requirements are incorporated according to intended users, applicable accessibility standards and customer commitments. Privacy, security and responsible-AI safeguards further support the prevention of adverse impacts on employees, customers, users and other affected stakeholders.
- **Responsible procurement and value chain.** Material suppliers are evaluated for relevant environmental, labour, human-rights, ethics, security, privacy, AI and business-continuity risks. Supplier requirements are proportionate to the service, data and associated risk. Higher-risk suppliers may be required to provide policies, metrics, certifications, assessment responses or corrective-action evidence.
- **Supplier monitoring and customer support.** Material supplier ESG issues, adverse events and significant changes are escalated and considered in remediation, renewal or exit decisions. Cloud and technology suppliers are assessed for relevant energy, emissions or sustainability information where material and reasonably available. Where customers have BRSR Core value-chain or other ESG reporting obligations, TestMu supports reasonable, contractually agreed information requests while protecting confidential and security-sensitive information.
- **India ESG and SEBI applicability.** TestMu uses the NGRBC principles as an India-focused responsible-business reference covering ethics, sustainable services, employee wellbeing, stakeholder responsiveness, human rights, environmental protection, public policy, inclusive growth and responsible customer engagement. SEBI BRSR, BRSR Core and value-chain disclosure or assurance requirements are applied when legally applicable to a TestMu entity or may be voluntarily used as reporting benchmarks.
- **Regulated-customer requirements.** Where TestMu directly falls within the scope of the SEBI Cybersecurity and Cyber Resilience Framework, or contractually supports a regulated entity subject to it, applicable requirements are evaluated and implemented within TestMu's agreed scope of responsibility. Legal, contractual and evidence boundaries are documented to avoid assuming obligations outside TestMu's operational control.
- **Corporate and legal compliance.** Applicable Companies Act, 2013 requirements relating to governance, corporate social responsibility, board oversight, ethics and reporting are tracked and implemented by each relevant TestMu legal entity when the applicable thresholds and conditions are met. Environmental, labour, workplace and waste-management obligations are maintained through TestMu's compliance-management process.
- **ESG objectives and metrics.** Relevant metrics may include energy consumption, renewable electricity, Scope 1, Scope 2 and Scope 3 emissions, emissions intensity, business travel, water,

waste, e-waste disposal, workforce diversity, training, health and safety, grievances, ethics cases, supplier assessments, privacy and security events, and responsible-AI indicators.

- **Reporting, evidence and review.** TestMu documents applicable definitions, reporting boundaries, base periods, calculation and estimation methods, source systems, evidence owners and restatements to support consistency and traceability. ESG performance is reviewed at least annually and more frequently for material objectives, risks or incidents. Identified gaps are assigned corrective or improvement actions.
- **Disclosure and assurance.** Public and customer-facing ESG disclosures undergo appropriate management, legal and evidence review to reduce inaccurate, incomplete or misleading sustainability claims. Independent assurance or assessment is obtained where legally required, contractually committed or approved by management. The applicable scope, criteria, limitations and conclusions are documented and retained.
- **ESG applicability principle.** References to the NGRBC, BRSR/BRSR Core, GRI Standards, UN Sustainable Development Goals, GHG Protocol or Science Based Targets initiative guidance describe TestMu's applicable alignment, reporting or implementation approach. They do not mean that every framework is legally mandatory, independently assured, or that TestMu has obtained formal SBTi validation unless TestMu separately and expressly confirms that status.

18. Global Legal & Regulatory Applicability

TestMu maintains a global compliance register and determines the applicability of legal, regulatory, contractual and industry requirements based on the relevant legal entity, establishment, customer and data-subject location, processing role, service configuration, industry, contractual commitment, and the nature of the information or AI system. References below identify principal requirements considered and do not mean that every requirement applies to every TestMu service, deployment or customer.

- **Global management and assurance frameworks.** TestMu's control environment is designed with reference to applicable frameworks including ISO/IEC 27001 and ISO/IEC 27002, ISO/IEC 27017, ISO/IEC 27018, ISO/IEC 27701, ISO/IEC 42001, ISO/IEC 23894, ISO/IEC 42005, SOC 2 Trust Services Criteria, NIST Cybersecurity Framework 2.0, NIST SP 800-53, NIST AI Risk Management Framework, CSA Cloud Controls Matrix, CIS Controls, and applicable OWASP application, API, LLM and agentic-AI security guidance. Certification and assurance claims are limited to their documented scope and validity.
- **European Union and EEA.** TestMu evaluates applicable requirements under the EU General Data Protection Regulation, ePrivacy requirements (Cookie Policy) and the EU AI Act. NIS2, DORA, the Cyber Resilience Act and other sector-specific requirements are assessed where TestMu is directly subject to them or contractually supports an in-scope customer. Restricted international transfers are supported through applicable EU Standard Contractual Clauses, transfer assessments and supplementary safeguards.
- **United Kingdom.** TestMu evaluates applicable requirements under the UK GDPR, Data Protection Act 2018, Privacy and Electronic Communications Regulations and the Data (Use

and Access) Act 2025. International transfers use appropriate safeguards, which may include the UK International Data Transfer Agreement or UK Addendum to the EU Standard Contractual Clauses.

- **United States.** TestMu evaluates applicable federal and state privacy, breach-notification, consumer-protection, cybersecurity and AI requirements. These may include the California Consumer Privacy Act, as amended by the California Privacy Rights Act, and other comprehensive state privacy laws. HIPAA, GLBA, NYDFS cybersecurity requirements and other sector-specific obligations apply only where TestMu is legally in scope or has expressly agreed to support them.
- **India.** TestMu evaluates applicable requirements under the Digital Personal Data Protection Act, 2023 and rules or notifications issued under it according to their commencement and transition provisions. Relevant requirements also include the Information Technology Act, 2000 and applicable rules, CERT-In Directions and sector-specific frameworks such as the SEBI Cybersecurity and Cyber Resilience Framework where directly applicable or contractually flowed down.
- **Other operating and customer jurisdictions.** TestMu evaluates applicable privacy, cybersecurity, AI, consumer-protection, employment and data-transfer requirements in other jurisdictions where it operates or provides services. These may include Brazil's LGPD, Canada's PIPEDA and provincial requirements, the Australian Privacy Act, Singapore's PDPA, Japan's APPI, the Philippines Data Privacy Act, the UAE PDPL, Saudi Arabia's PDPL and other applicable national or regional laws.
- **Payment, health and regulated data.** PCI DSS responsibilities apply only to payment-card environments and activities within TestMu's defined scope. HIPAA safeguards and Business Associate Agreement obligations apply where TestMu has expressly agreed to process protected health information. Government-classified, export-controlled or otherwise restricted information requires prior written authorization and an approved service and security configuration.
- **Regulatory monitoring and implementation.** TestMu's Legal, Privacy, Information Security and GRC functions monitor material regulatory developments and translate applicable obligations into policies, contractual requirements, risk and impact assessments, technical and organizational controls, training, monitoring and compliance evidence.
- **Cross-border data transfers.** International transfers use applicable legal mechanisms and proportionate supplementary safeguards. These may include data-processing agreements, Standard Contractual Clauses, the UK Addendum or IDTA, transfer-risk assessments, encryption, access restrictions and regional hosting where offered.
- **Customer and sector-specific requirements.** Requirements applicable to a regulated customer are assessed and implemented within TestMu's agreed scope of responsibility. Customer-flowed requirements do not make TestMu directly subject to the customer's regulatory framework unless independently required by law. Applicable responsibilities, evidence requirements and control boundaries are documented through contracts, assessments or shared-responsibility arrangements.

- **Conflicting requirements and legal interpretation.** Actual or potential conflicts among legal, regulatory, contractual and customer requirements are escalated to Legal, the Data Protection Officer or another accountable officer for documented assessment, approval and direction.
- **Government and law-enforcement requests.** Government, regulatory and law-enforcement requests are assessed for legal validity, jurisdiction, scope, authority and proportionality. Requests are handled in accordance with TestMu's documented procedures, applicable law and contractual commitments, including customer notification where legally permitted. In any case, TestMu endeavours that direct access to customer data is provided upon received requests only and all such records of requests and disclosures are maintained.
- **Applicability principle.** References to laws, regulations, standards and frameworks describe TestMu's compliance-evaluation and alignment approach. They do not represent that every requirement applies to TestMu, every legal entity, every product or every customer deployment. Formal compliance, certification or assurance claims are made only where the applicable scope and status have been separately established.

19. Customer and TestMu Shared Responsibilities

Security, privacy, availability and responsible-AI outcomes depend on both TestMu's controls and the customer's configuration and use of the services. The applicable agreement, order form, Data Processing Addendum, service documentation and deployment model define the binding allocation of responsibilities.

Control area	TestMu responsibility	Customer responsibility
Accounts and access	Operate platform identity, authentication, authorization and logging controls, including supported SSO, MFA, role-based access and session-management capabilities.	Protect credentials; configure users, roles, SSO, MFA, IP restrictions and integrations; periodically review access; and promptly remove access that is no longer required.
Customer data	Process customer data only to provide, operate, support and secure the service. Apply applicable encryption, tenant isolation, access, retention and deletion controls.	Ensure lawful collection and submission; minimize sensitive data; configure available retention and export options; and avoid submitting prohibited or restricted data unless expressly authorized.
Testing targets and content	Protect the TestMu platform and execute authorized customer instructions within the functionality of the subscribed service.	Obtain authorization to test relevant systems, applications, devices, APIs, networks and content. Prevent malicious, unlawful, unauthorized or third-party-impacting testing activities.
AI inputs and outputs	Maintain AI governance, security guardrails, testing, monitoring and the commitments stated in TestMu's AI Terms and policies. Customer data is not used to train, retrain or fine-tune TestMu models or third-party foundation models.	Provide lawful and appropriate inputs; review AI-generated outputs; maintain necessary human oversight; and avoid prohibited or high-impact use without appropriate assessment, authorization and safeguards.

Control area	TestMu responsibility	Customer responsibility
Integrations and endpoints	Secure TestMu-managed applications, infrastructure, interfaces, APIs and supported connectors within TestMu's control.	Secure customer-managed endpoints, networks, repositories, credentials, keys, connected systems, third-party integrations and on-premises infrastructure.
Configuration and deployment	Provide documented security and privacy capabilities appropriate to the subscribed service and deployment model.	Select, configure and maintain appropriate security, privacy, regional-processing, access and integration settings according to the customer's risks and obligations.
Availability and recovery	Maintain continuity, backup, resilience and recovery measures for TestMu-managed services according to applicable service commitments.	Maintain continuity and recovery arrangements for customer-controlled systems, data exports, integrations, dependencies and on-premises components.
Incident cooperation	Investigate incidents within TestMu's control, contain impact, preserve relevant evidence and provide notifications required by applicable law and contract.	Maintain current incident contacts; promptly report suspected misuse or incidents; preserve relevant customer-controlled evidence; and cooperate with investigation and response activities.
Compliance and assurance	Maintain applicable TestMu control evidence and support reasonable customer-assurance requests, subject to confidentiality, security and contractual limitations.	Determine customer-specific legal, regulatory and sector obligations and configure, assess and use the services accordingly.
Customer-managed or on-premises deployment	Remain responsible for TestMu-provided software and application-level controls within the agreed scope.	Remain responsible for customer-selected AI models, training data, infrastructure, hosting, networks, encryption keys, access controls, deployment security and operational administration unless otherwise agreed.

Shared-responsibility principle. TestMu is responsible only for systems, services and controls within its ownership or operational control. Customers remain responsible for their data, users, testing authorization, configurations, connected systems and customer-managed environments. Where responsibilities differ because of a particular product, deployment or contractual commitment, the applicable agreement and service documentation prevail.

20. Audit, Evidence, Continual Improvement

TestMu maintains documented evidence to demonstrate the implementation, operation and effectiveness of its security, privacy, AI, cloud, compliance and responsible-business controls.

- **Control evidence.** Evidence may include policies, procedures, inventories, registers, risk and impact assessments, approvals, access records, system logs, tickets, training records, testing results, supplier assessments, incident records, audit reports, corrective actions and

management-review outputs. Records are protected, retained and made available according to applicable access, retention, legal and contractual requirements.

- **Internal audit.** Internal audits are planned according to process importance, risk, regulatory and contractual requirements, material changes and previous audit results. Auditors maintain appropriate objectivity and independence from the activities being reviewed.
- **Findings and corrective action.** Audit findings, control deficiencies, incidents and other nonconformities are documented, risk-rated and assigned to accountable owners with target completion dates. Root causes, remediation actions and relevant evidence are tracked through closure. The effectiveness of material corrective actions is verified where appropriate.
- **Independent assurance.** TestMu undergoes applicable independent certification, attestation, penetration testing and other assurance activities. Certification, attestation and assessment claims are limited to their documented scope, period and validity.
- **Management review.** Management periodically reviews control performance, objectives, risks, opportunities, incidents, complaints, audit results, corrective actions, supplier issues, legal and regulatory developments, resource requirements and opportunities for improvement. Decisions and follow-up actions are documented and tracked.
- **Continual improvement.** Lessons from audits, assessments, incidents, testing, customer feedback, complaints, regulatory changes and technology developments are used to improve policies, processes, controls, training and monitoring.
- **Customer assurance.** Customers may request current certificates, independent assurance reports, testing summaries or other appropriate compliance information through their TestMu representative or applicable Trust and Assurance channel. Information is provided subject to availability, confidentiality, legal, contractual and security restrictions.
- **Reporting concerns.** Security, privacy, responsible-AI or compliance concerns may be reported through TestMu's published security, privacy, support or contractual contact channels. Reports are assessed, escalated and addressed through the applicable incident, grievance or compliance-management process.

21. Appendix A- Standards and Regulatory Alignments

The measures described in this document support TestMu's integrated security, privacy, AI governance, cloud, resilience and responsible-business control environment. They are informed by the following standards, laws, regulations and industry guidance, as applicable.

Domain	Primary references
Information security and cybersecurity	ISO/IEC 27001:2022; ISO/IEC 27002:2022; NIST Cybersecurity Framework 2.0; NIST SP 800-53; CIS Controls; SOC 2 Trust Services Criteria

Domain	Primary references
Cloud security and privacy	ISO/IEC 27017:2015; ISO/IEC 27018; CSA Cloud Controls Matrix; applicable cloud-security and shared-responsibility guidance
Privacy and data protection	ISO/IEC 27701:2025; EU GDPR; UK GDPR and Data Protection Act 2018; CCPA, as amended by CPRA; India's Digital Personal Data Protection requirements; and other applicable privacy and data-protection laws
AI management and governance	ISO/IEC 42001:2023; ISO/IEC 5338:2023; ISO/IEC 23894:2023; ISO/IEC 42005:2025; NIST AI RMF 1.0 ; applicable AI governance, lifecycle and management-system guidance
AI risk and impact assessment	ISO/IEC 23894:2023; ISO/IEC 42005:2025; NIST AI Risk Management Framework 1.0; NIST AI 600-1 Generative AI Profile
AI regulation and principles	EU AI Act (Regulation (EU) 2024/1689), as applicable; OECD AI Principles; applicable national and sector requirements
Application, API and AI security	OWASP Top 10; OWASP API Security Top 10; current applicable OWASP guidance for LLM, generative-AI and agentic applications; NIST Secure Software Development Framework; and applicable secure-development guidance
Global privacy and cybersecurity	EU and UK data-protection requirements; applicable United States federal and state privacy and breach-notification laws; Brazil LGPD; Canada PIPEDA and provincial requirements; Australian Privacy Act; Singapore PDPA; Japan APPI; Philippines Data Privacy Act; UAE PDPL; Saudi Arabia PDPL; India DPDP and CERT-In requirements; and other applicable national or sector requirements
Sector and regulated data	PCI DSS for in-scope payment-card environments; HIPAA and Business Associate Agreement requirements where TestMu agrees to process protected health information; GLBA, NYDFS, DORA, NIS2, SEBI CSCRF and other sector requirements where directly applicable or contractually supported
Business continuity and resilience	ISO 22301 guidance where applicable; NIST SP 800-53 contingency-planning controls; CSA resilience guidance; and applicable business-continuity, disaster-recovery and cloud-resilience practices
Data retention and secure disposal	NIST SP 800-88; applicable legal, contractual and industry requirements for retention, deletion, media sanitization and disposal
ESG and responsible business	NGRBC; SEBI BRSR and BRSR Core where applicable; GRI Standards; UN Sustainable Development Goals; GHG Protocol; E-Waste (Management) Rules, 2022 and amendments; and applicable Companies Act, environmental, labour and workplace requirements

Domain	Primary references
Cloud, resilience and disposal	CSA guidance; NIST SP 800-53; NIST SP 800-88; applicable continuity, cloud assurance and environmental practices

Applicability and assurance statement. The standards, laws and frameworks referenced in this appendix are used as applicable legal, governance, control-design and mapping sources. Applicability depends on TestMu’s legal entity, certification or assurance scope, product, service, deployment model, processing role, customer contract, data involved and jurisdiction. Inclusion does not imply certification, independent assurance or universal legal applicability. TestMu makes formal compliance or certification claims only where the applicable scope and current status have been established and documented.

22. Appendix B- Public Assurance Resources

The following public resources provide information concerning TestMu’s security, privacy, data protection, responsible AI, contractual requirements, subprocessors and service availability.

Resource	Location
TestMu Trust Center	https://www.testmuai.com/trust/
Security & Information Security Policy & Practices	https://www.testmuai.com/trust/security/
Privacy Center and Data-Protection Practices	https://www.testmuai.com/trust/privacy/
Responsible AI and AI Trust	https://www.testmuai.com/trust/ai/
Privacy Policy	https://www.testmuai.com/legal/privacy/
Terms of Service	https://www.testmuai.com/legal/terms-of-service/
Acceptable Use Policy	https://www.testmuai.com/legal/aup/
AI Terms	https://www.testmuai.com/legal/ai-terms/
Sub-processor List	https://www.testmuai.com/legal/sub-processor/
Data Processing Addendum	https://www.testmuai.com/legal/data-processing-addendum/
Service Status and Availability	https://status.lambdatest.io/
TestMu Compliance Center	https://trust.testmuai.com/

You may contact our 24x7 hotline at [TestMu Security](#) or [TestMu Privacy](#) to report complaints/breaches.