YouTestMe

Technical and Organizational Measures (TOMs)

Table of Contents

1 Compliance with ISO Standards

YouTestMe is committed to maintaining compliance with ISO 27001 and ISO 9001 standards, as applicable to the scope of YouTestMe Services. Additionally, YouTestMe shall ensure that the data center utilized for delivering the Services maintains IT security management certification in accordance with ISO 27001 or an equivalent recognized industry security framework. Independent, certified third parties shall conduct audits of such certifications, and upon the Customer's request, YouTestMe shall provide the relevant certificates.

2 Entity Controls

To uphold its commitment to maintaining compliance programs as outlined above, YouTestMe shall implement and continuously enforce the following security measures:

a) **Security Policy**: YouTestMe shall establish and uphold an information security policy, subject to annual review by YouTestMe, which will be distributed and communicated to all employees. A dedicated security and compliance team shall oversee and monitor the application of security controls across the organization.

b) **Employee Onboarding**: All YouTestMe personnel will undergo thorough background checks and agree to comply with YouTestMe's Code of Conduct as a condition of their employment.

c) **Employee Termination**: Upon termination of employment, YouTestMe shall revoke all credentials and access privileges to the Services associated with the departing employee within a reasonable timeframe.

d) **Access Controls for YouTestMe Personnel**: Access to YouTestMe-owned or licensed network infrastructure, servers, databases, computers, and software will be safeguarded through mandatory authentication procedures for personnel.

e) **Security Awareness Training**: All YouTestMe employees will complete security awareness and privacy training upon onboarding and annually thereafter to ensure ongoing compliance and awareness.

f) **Change Management**: YouTestMe shall implement a change management process aligned with widely accepted industry standards to oversee modifications in configurations, software, and hardware.

3 Application and Network Controls:

a) **Privileged Access for YouTestMe Personnel**: Access to network components, servers, databases, computers, and software owned or licensed by YouTestMe and used to provide the Services shall be governed by predefined access policies. Privileged access will only be granted to YouTestMe personnel to the extent necessary to fulfill their specific roles.

b) **Data Center Infrastructure Monitoring**: YouTestMe and/or its sub-processors shall actively monitor the infrastructure to detect and address potential security vulnerabilities.

c) **Anti-Virus and Malware Detection**: YouTestMe shall deploy commercially available malicious code detection tools, including antivirus and malware scanning software, on its systems. Definitions for these tools shall be regularly updated according to a defined schedule.

d) **Secure Development Practices**: YouTestMe developers shall receive training in secure coding principles, ensuring that applications are developed using industry-recognized secure development practices.

e) **Patch Management**: Patches, updates, and upgrades for operating systems, middleware, and applications shall be reviewed, tested, and deployed prudently by YouTestMe to ensure critical updates are applied promptly, in alignment with their associated risk levels.

f) **Data Segmentation**: YouTestMe shall implement robust security controls and segmentation techniques to safeguard and isolate Customer Data from other tenants.

g) **Secure Data Transmission**: Customer Data transmitted through the Services shall be protected using industry-standard protocols, such as Transport Layer Security (TLS).

h) **Encrypted Data Storage**: YouTestMe shall employ encryption technologies, such as the AES-256 encryption standard, to secure Customer Data at rest.

i) **Firewall Protections**: Network connections to the Services shall be secured with industry-standard firewalls, which will be updated regularly according to a defined schedule.

j) **Intrusion Detection**: YouTestMe shall implement and maintain intrusion detection systems at both the network and host levels to safeguard the Services and identify unauthorized or hostile network activity.

k) **System Hardening and Secure Configuration**: YouTestMe shall adhere to industry standards for system hardening and secure configurations to fortify its platforms.

l) **Penetration Testing**: As part of its security program, YouTestMe shall engage independent third parties to conduct comprehensive penetration testing of its network and applications on at least an annual basis.

m) **Vulnerability Management**: YouTestMe shall employ commercially reasonable processes to identify and address system vulnerabilities. Regular automated scanning using recognized tools shall be performed to detect security flaws. Identified vulnerabilities will be assessed, and appropriate remediation actions will be taken within a reasonable timeframe, based on the associated risk to the Services.

4 Physical Access Control

YouTestMe shall ensure that its data center sub-processor implements industry-standard technologies and practices to guarantee that access to YouTestMe systems used for delivering the Services is restricted to authorized personnel only. Such measures shall include, but are not limited to, visitor sign-in protocols, role-based access management, restricted physical access to server rooms, and alarm systems designed to detect and report unauthorized access attempts.

5 Incident Response and Notification

YouTestMe shall establish and maintain comprehensive security incident management policies and procedures, including protocols for the escalation of security incidents. In the event YouTestMe confirms that unauthorized access, acquisition, disclosure, or misuse of the Customer's Personal Data has occurred,

YouTestMe shall notify the Customer in accordance with the terms of the Agreement or as required by Applicable Law.

Following such a security incident, YouTestMe shall conduct an investigation to determine the root cause, implement corrective measures to mitigate the effects of the incident, and provide the Customer with assurances that the incident is unlikely to recur.

6 Disaster Recovery

YouTestMe shall maintain a comprehensive Disaster Recovery plan and, upon Customer's request, provide verification of its existence. This plan shall be tested annually to ensure its effectiveness, with the results reviewed by management. Necessary updates shall be made to the plan based on the results of these tests and any changes in circumstances.

7 Business Continuity

YouTestMe shall maintain a Business Continuity plan to restore operations in the event of a disaster and shall provide a summary of this plan to the Customer upon request. In the event of a disaster declaration, YouTestMe shall activate the plan to restore the Services. The Business Continuity plan shall be tested and reviewed annually, with updates made as necessary to ensure its continued effectiveness.