YouTestMe

Information Security and Compliance Overview

Table of Contents

1 Introduction

This document provides a comprehensive overview of YouTestMe's information security and compliance framework. It outlines the policies, controls, and best practices implemented to safeguard data, regulate access, and mitigate risks. Key areas covered include access management, data protection, compliance measures, risk management, AI proctoring security, and governance policies. These measures ensure the confidentiality, integrity, and availability of user data while aligning with industry standards and regulatory requirements.

2 Information Security & Compliance Overview

2.1 Access Management & User Security

2.1.1 Access Control & User Management

2.1.1.1 Access Control and Entitlement Review

YouTestMe ensures data access is limited to authorized personnel using role-based access control (RBAC) and multi-factor authentication (MFA). Administrators assign roles and permissions aligned with business logic. Regular entitlement reviews are conducted to verify compliance with access policies, ensuring only authorized personnel maintain access.

2.1.1.2 Granting and Revoking Data Access Permissions

In YouTestMe, data access permissions are managed at two levels. Administrators grant or revoke permissions through a documented approval process at the system level, while roles and permission settings at the application level provide granular control over user access to specific features and data.

2.1.1.3 Management and Update of User Roles and Permissions

YouTestMe manages user roles and permissions using role-based access control (RBAC), allowing administrators to assign and customize roles with granular permissions. Default roles such as administrator, candidate, instructor, and proctor streamline initial setup, while unlimited custom roles enable precise alignment with organizational needs.

2.1.1.4 Defined and Enforced Access Control Policy

YouTestMe enforces a comprehensive access control policy that outlines principles and rules for granting access to information and systems. The policy includes systematic enforcement and defines responsibilities for administrators to conduct periodic reviews, ensuring access rights align with user roles and organizational requirements.

2.1.1.5 Roles and Profiles in YouTestMe

YouTestMe provides default roles aligned with general use cases, supporting need-to-know and need-to-have principles. Roles and permissions are fully customizable, allowing clients to configure access according to their specific requirements, ensuring secure and efficient management of user privileges.

2.1.1.6 Authentication and Multi-Factor Support

YouTestMe requires user authentication through standard login credentials and supports multi-factor authentication (MFA) using Time-Based One-Time Passwords (TOTP). This ensures enhanced security for accessing the application or service by adding an additional layer of verification.

2.1.1.7 Support for SAML Authentication

YouTestMe supports standard authentication mechanisms, including SAML 2.0 Single Sign-On (SSO). It integrates with various Identity Providers like OneLogin, Okta, and SSO Circle, acting as a Service Provider (SP) to ensure secure and seamless user authentication.

2.1.1.8 Password Protection and Hashing

YouTestMe secures passwords using the SHA-256 hashing algorithm. Passwords are irreversibly hashed and cannot be decrypted. Verification is performed by comparing the stored hash with a rehashed version of the input, ensuring strong protection against compromise.

2.1.1.9 Randomization of First-Time Passwords

YouTestMe ensures that first-time passwords are randomized, enhancing security by preventing predictable credentials and reducing the risk of unauthorized access during initial login processes.

2.1.1.10 Default Password Change Requirement

YouTestMe prompts users to change their default password during their first logon. This recommendation enhances account security and aligns with best practices for protecting user credentials.

2.1.1.11 Password Policy

YouTestMe supports configurable password complexity and allows setting a password expiration time, with a default of six months. Temporary passwords are recommended to be changed during first logon. Account lockdown after incorrect password entries can be enabled if required. Password history and reuse restrictions are not currently implemented.

2.1.2 IT Infrastructure & System Security

2.1.2.1 Patch Management Policy

YouTestMe maintains a patch management policy for infrastructure, combining automated and scheduled updates with ad hoc processes based on priority. Patches are applied monthly or as needed, with new releases delivered to clients according to agreed timelines, ensuring system reliability and addressing critical updates promptly.

2.1.2.2 Formal Change Control Procedure

YouTestMe enforces a formal change control procedure involving classification, security assessment, approval, fallback processes, and assigned responsibilities. This ensures all changes, including emergency modifications, are securely implemented and assessed for potential risks to maintain system integrity and reliability.

2.1.2.3 Technical Vulnerability Management

YouTestMe identifies technical vulnerabilities through regular vulnerability scans and mitigates risks via a defined, documented, and periodically reviewed patch management process. This ensures timely resolution of vulnerabilities to maintain system security and operational reliability.

2.1.2.4 System Hardening Procedures and Baseline Configurations

YouTestMe has documented system hardening procedures for virtual machines, ensuring secure configurations. Unsupported software and hardware are not permitted, aligning with best practices to maintain system integrity and compliance with security standards.

2.1.2.5 Anti-Virus/Malware Signature Updates

YouTestMe uses AVG for employee workstations and ClamAV for servers. Anti-virus and malware signatures are updated automatically based on the schedule configured within each tool, ensuring systems remain protected against the latest threats.

2.1.2.6 Control of Services, Protocols, and Ports

YouTestMe enforces HTTPS for production environments, configures NTP for time synchronization, and limits SMTP through Azure configuration. These measures ensure secure and controlled usage of essential services, protocols, and ports in network devices.

2.1.2.7 IT Communications Management

YouTestMe manages incoming and outgoing IT communications through a formalized policy outlining security principles for emails, remote work, and outsourced activities. Network architecture is comprehensively documented via logical and physical diagrams, ensuring secure and efficient communication flows.

2.1.2.8 DMZ Environment

YouTestMe does not utilize a DMZ environment within the network for transmitting, processing, or storing client systems and data. Alternative security measures are implemented to ensure secure handling and protection of client data.

2.1.2.9 Remote Administration and Security Controls

YouTestMe supports remote administration for users with designated permissions. Security measures include authentication, role-based authorization, optional two-factor authentication (2FA), and detailed audit logs, ensuring secure access and control over administrative functions within the platform.

2.1.2.10 Physical Security Policy for Secure Areas

YouTestMe enforces a management-approved physical security policy defining requirements for secure areas, including controlled entry/exit points, workspace security, restricted public access, and safeguards against external and environmental threats. The policy ensures comprehensive protection and compliance with organizational security objectives.

2.1.2.11 Physical Protection of Equipment

YouTestMe ensures equipment security through a management-approved policy covering all stages, from acquisition to disposal. This includes secure placement, restricted access, environmental protection, and proper disposal procedures, safeguarding equipment against unauthorized access, damage, and environmental risks.

2.2 Data Security & Privacy

2.2.1 Data Security & Protection

2.2.1.1 Security Measures Against Unauthorized Access, Alteration, and Deletion

YouTestMe protects data using encryption in transit and at rest, role-based access controls, and real-time monitoring to detect and prevent unauthorized access, alterations, or deletions. These measures ensure data integrity and security, complying with best practices and organizational policies.

2.2.1.2 Data Encryption at Rest

YouTestMe encrypts data at rest using 256-bit AES encryption via Microsoft Azure Disk Storage Server-Side Encryption. Cryptographic keys are managed by Azure Key Vault, with options for customer-managed or platform-managed keys. Encryption adheres to FIPS 140-2 compliance, ensuring secure storage and controlled access to data.

2.2.1.3 Data Encryption During Transmission

YouTestMe ensures all data is encrypted during transmission using Transport Layer Security (TLS) 1.2 with 256-bit AES encryption or stronger. Additionally, PostgreSQL SSL connections are utilized for encrypting client-server communications, providing robust security for all transmitted data.

2.2.1.4 Cryptographic Controls Definition and Implementation

YouTestMe enforces cryptographic control policies, including encryption, key management, and secure data handling. These policies are well-defined, applied organization-wide, and regularly reviewed to address emerging threats. Administrators ensure compliance with standards to maintain data integrity and confidentiality across all operational processes.

2.2.1.5 Information Classification and Asset Inventory

YouTestMe identifies and classifies critical information, ensuring all assets are documented in a regularly updated inventory. Each asset is assigned a clear owner responsible for its management, with roles and responsibilities formally defined to maintain security and operational integrity.

2.2.1.6 Process for Identifying Processed or Stored Sensitive Data

YouTestMe employs a formalized methodology for identifying personally identifiable information (PII) and sensitive data. A defined procedure is in place to classify data based on its nature, ensuring compliance with privacy requirements and enabling appropriate data protection measures throughout its lifecycle.

2.2.1.7 Data Classification Based on Sensitivity and Criticality

YouTestMe classifies data as sensitive, confidential, or public using a documented data classification framework aligned with ISO 27001 standards. Each document is labeled with its classification in the header, ensuring proper handling and compliance with security and organizational policies.

2.2.1.8 Monitoring and Maintaining Data Classification

YouTestMe ensures data classification through strict adherence to access controls and security measures. Sensitive data is encrypted in transit and at rest, with access restricted to authorized users based on role-based permissions. Documented processes support the consistent handling of classified information to maintain data integrity and security.

2.2.1.9 Access Control for Classified Data

Access to classified data in YouTestMe is restricted using role-based access control (RBAC) and encryption. Permission changes require documented approvals, and access logs are maintained to monitor activities, ensuring data security and compliance with organizational policies.

2.2.1.10 Frequency of Data Classification Reviews

YouTestMe reviews data classifications quarterly or during significant organizational changes to ensure alignment with security policies and ISO 27001 standards. This process maintains accuracy and consistency in the application of classifications across all data.

2.2.1.11 Documented Data Policies and Procedures

YouTestMe maintains documented policies and procedures for data quality, lifecycle management, and classification, aligned with ISO 27001 standards. These policies are reviewed annually to ensure compliance and effectiveness.

2.2.1.12 Data Ownership and Management

Data ownership in YouTestMe is defined by assigning responsibility to administrators, who oversee the lifecycle of each dataset and ensure compliance with organizational policies. This approach ensures that data is managed effectively, adhering to defined access controls and classification standards.

2.2.2 Data Management & Compliance

2.2.2.1 Data Protection Impact and Privacy Assessments

YouTestMe conducts Data Protection Impact Assessments (DPIA) and Privacy Impact Assessments (PIA) on sensitive and personal data at least annually or when significant changes in data processing occur. These

assessments are performed using a defined procedure to identify and mitigate potential risks for data subjects.

2.2.2.2 Backup Policy and Capabilities

YouTestMe supports full daily backups, with configurable frequency and timing to meet client requirements. A hot-standby database ensures data availability and redundancy, enabling rapid recovery and continuity of operations in case of system failure or data loss.

2.2.2.3 Data Backup Frequency and Storage Locations

YouTestMe performs daily data backups, which are securely stored in multiple locations, including Azure Blob Storage and off-site SFTP servers. This approach ensures data redundancy, security, and availability, safeguarding client information against potential data loss or system failure.

2.2.2.4 Data Retention Periods and Implementation

YouTestMe enforces retention periods based on data domains through automated rules in storage and database systems. Administrators can define retention for proctoring-related data, while clients maintain responsibility for managing the data lifecycle according to their specific policies and requirements.

2.2.2.5 Documentation on Retention Periods

YouTestMe maintains documented retention policies as part of its data management framework. These policies define retention periods based on data domains and outline procedures for data lifecycle management, ensuring compliance with organizational and regulatory requirements.

2.2.2.6 Data Lifecycle Management

The data lifecycle in YouTestMe is primarily managed by the client, with administrators controlling creation, usage, and secure deletion based on organizational policies. Retention policies for proctoring data are enforced through automated tools to ensure compliance and secure handling throughout the data lifecycle.

2.2.2.7 Data Analytics and Reporting Tools

YouTestMe provides advanced data analytics and reporting through custom-built reports, Apache Superset integration, and predefined templates. Features include customizable reports, detailed test summaries, question performance analysis, and exportable formats. Administrators and instructors can schedule automated reports, apply advanced filters, and leverage visual tools like radar charts for actionable insights.

2.2.2.8 Data Transfers and Non-Personal Data Inclusion

Data transfers in YouTestMe include both personal and non-personal data, encrypted during transit to ensure security. Transfers are limited to authorized systems, such as for backups, and are performed under strict controls to maintain data integrity and confidentiality.

2.2.2.9 Data Transfer Regulations

YouTestMe ensures compliance with GDPR and other regulations by implementing encryption for all data transfers, establishing contractual safeguards, and conducting regular audits. These measures maintain secure and lawful data handling across all operations.

2.2.2.10 Monitoring and Logging of Data Transfer Activities

YouTestMe logs and monitors all data transfer activities using centralized logging tools, such as Azure Logging. These tools ensure traceability, provide detailed records for auditing, and support compliance with data security regulations, enabling administrators to review and manage transfer activities effectively.

2.2.2.11 Management of Data Transfers with Third-Party Services

YouTestMe manages data transfers to and from third-party services using secure APIs and encrypted file exchanges, adhering to industry standards. Contracts and agreements ensure compliance with data protection regulations, and all integrations prioritize encryption to safeguard data integrity and confidentiality.

2.2.2.12 Use of Data for Secondary Purposes

YouTestMe does not use data for any secondary purposes. All data is processed solely for its intended purpose, as defined by the client agreement. The client retains full control over data usage within the platform.

2.2.2.13 Strategies to Prevent Unauthorized Data Transfers or Leaks

YouTestMe employs data loss prevention tools, encryption, and role-based access controls to prevent unauthorized data transfers or leaks. Activity logging and regular penetration testing enhance security by detecting potential vulnerabilities, ensuring compliance, and maintaining robust data protection throughout the system.

2.2.2.14 Preventing Actions for Copying, Saving, and Printing During Tests

YouTestMe prevents unauthorized actions like copying, saving, and printing during tests through content copy protection, integration with a safe exam browser, and proctoring. These measures ensure a secure testing environment by restricting access and monitoring candidate activities in real time.

2.3 Monitoring, Risk & Incident Management

2.3.1 Auditing, Monitoring & Risk Management

2.3.1.1 Auditing and Monitoring Data Access and Usage

YouTestMe ensures data access and usage are monitored using detailed logging, audit trails, and permission reports. These records are integrated with tools like Zabbix or Azure Monitor, enabling administrators to track actions and detect anomalies, ensuring compliance with security standards and maintaining control over sensitive data.

2.3.1.2 Information Security Risk Assessments

YouTestMe conducts periodic Information Security risk assessments and additional assessments following significant changes. These evaluations are methodical, ensuring consistent, reproducible results to identify and mitigate potential vulnerabilities effectively, maintaining the platform's security and compliance standards.

2.3.1.3 Risk Mitigation Approach

YouTestMe applies a systematic approach to address identified risks, prioritizing treatment based on cost-benefit analysis and predefined risk appetite thresholds. Measures are implemented to mitigate, transfer, or accept risks, ensuring alignment with organizational security objectives and compliance standards.

2.3.1.4 Management-Approved Information Security Policy

YouTestMe maintains a formal, management-approved Information Security Policy, accessible to all employees and communicated to third parties. The policy outlines security objectives, responsibilities, and compliance requirements, ensuring alignment with best practices and regulatory standards.

2.3.1.5 Frequency of Information Security Policy Review

The YouTestMe Information Security Policy is formally reviewed annually to ensure its continued relevance, effectiveness, and alignment with evolving security requirements and industry standards.

2.3.1.6 Definition of Key Information Security Roles and Responsibilities

Key information security roles and responsibilities are clearly defined, documented, and assigned to ensure accountability and effective management of security policies and practices within YouTestMe.

2.3.1.7 Regular Review of Third Parties

YouTestMe conducts regular reviews and audits of third parties, ensuring that security controls, service definitions, and delivery levels are consistently implemented, operated, and maintained.

2.3.1.8 Process for Reporting Security Events

YouTestMe maintains a formal process for reporting security events, incidents, and weaknesses. This includes a clearly defined incident response and escalation procedure that is documented, communicated, and consistently applied across the organization to ensure timely notification to relevant stakeholders.

2.3.1.9 System Logging and Monitoring

YouTestMe has logging enabled, with logs reviewed to ensure integration with common monitoring systems. Logs are configured to provide sufficient detail for thorough investigation, supporting effective incident analysis and response.

2.3.1.10 Network Intrusion Detection/Prevention System

YouTestMe does not currently have a Network Intrusion Detection System (NIDS) implemented. Network security is maintained through other measures, and additional tools or systems can be considered based on client requirements.

2.3.1.11 External Network Connections

YouTestMe communicates with external services over the internet without terminating every connection at a firewall. Security is maintained through controlled communication protocols, encryption, and other protective measures to ensure secure data exchange with external networks.

2.3.2 Incident Response & Business Continuity

2.3.2.1 Procedure for Data Breach

YouTestMe has a documented incident response plan detailing procedures for detection, containment, notification, and remediation of data breaches. This plan ensures timely action and compliance with regulatory requirements, safeguarding data integrity and minimizing impact.

2.3.2.2 Information Security Incident Management Process

YouTestMe has a defined and documented information security incident management process. Responsibilities are assigned, and procedures for identifying, reporting, and handling incidents are well-established. Monitoring systems are implemented to detect and respond to security events effectively, ensuring quick containment and resolution.

2.3.2.3 Information Security Incident Management Procedure

YouTestMe has a documented Information Security Incident Management procedure, including policies for reporting, assessing, and mitigating incidents. An Incident Response Team (IRT) is established to manage incidents promptly, ensuring containment, eradication, and recovery. Post-incident reviews are conducted to improve processes and enhance security measures.

2.3.2.4 Internal Procedures for Legal and Regulatory Issues in Security Incidents

YouTestMe has a defined and documented approach for managing legal and regulatory requirements during information security incidents. This ensures compliance through timely reporting, adherence to applicable regulations, and coordination with relevant authorities, supported by clear procedures applied consistently across the organization.

2.3.2.5 Business Continuity Plan for Critical Service Continuity

YouTestMe has a comprehensive Business Continuity Plan, addressing risk assessment, prioritization of critical processes, and asset identification. The plan ensures service continuity through an established strategy, enabling uninterrupted operation of critical services during adverse situations, supported by systematic implementation and review.

2.3.2.6 Business Continuity Plan Testing Frequency

The YouTestMe Business Continuity Plan is formally tested and reassessed at least annually. Testing includes crisis management drills, technical recovery simulations, and full user rehearsals to ensure the plan's effectiveness and readiness for execution.

2.4 Security Governance & Compliance

2.4.1 Security Policies & Compliance

2.4.1.1 Certifications, Standards, and Audits for Security Validation

YouTestMe adheres to ISO 27001 and SOC 2 Type II standards, ensuring robust security practices. These frameworks are validated through regular third-party audits, providing assurance of compliance with industry-leading security protocols and measures.

2.4.1.2 Legislative, Regulatory, and Contractual Compliance

YouTestMe maintains comprehensive documentation of all relevant legislative, regulatory, and contractual requirements related to information security. Procedures are defined and enforced to ensure compliance, with specific controls and individual responsibilities clearly documented and regularly updated to reflect any changes in requirements.

2.4.1.3 Compliance with Information Security Policies and Standards

YouTestMe ensures compliance with its information security policies and standards through mandatory annual reviews conducted by the CISO, internal audit, or relevant stakeholders. This process verifies adherence, identifies gaps, and enforces updates to maintain alignment with organizational and regulatory requirements.

2.4.1.4 Defined Data Privacy Officer Role and Responsibilities

YouTestMe has a designated Data Privacy Officer (DPO) with clearly defined and documented responsibilities. The DPO ensures compliance with data privacy regulations, oversees related processes, and serves as the primary point of contact for all privacy-related matters within the organization.

2.4.1.5 Understanding of Organizational Role in PII Processing

YouTestMe has a clearly defined role in PII processing, outlined in its governance policies and enforced through comprehensive procedures. These details are explicitly stated in the Data Processing Agreement (DPA) signed with clients, ensuring full compliance and alignment with applicable data protection regulations.

2.4.1.6 Adoption of Privacy by Design Methods

YouTestMe adheres to a formalized policy ensuring all systems and components related to processing personally identifiable information (PII) are designed with privacy by design and privacy by default principles. Measures such as access control, encryption, and tokenization are integrated into operations to safeguard data privacy.

2.4.1.7 Employee Restrictions Across Jurisdictions

YouTestMe enforces strict controls on employees handling data across multiple jurisdictions. Requirements for transferring personal data across regions are clearly identified, documented, and implemented to ensure compliance with relevant privacy regulations and jurisdictional laws.

2.4.1.8 Documentation of Data Flows

YouTestMe partially documents data flows for specific integrations and can provide detailed diagrams upon request.

2.4.2 Organizational Security & Awareness

2.4.2.1 Information Security Requirements for Visitors and Third Parties

YouTestMe defines and communicates information security requirements through a code of conduct acknowledged by employees, contractors, and third-party users. The code outlines responsibilities, compliance with applicable laws and policies, confidentiality obligations, and appropriate usage of information systems to ensure adherence to security standards.

2.4.2.2 Human Resources Security Policy

YouTestMe maintains a well-defined, documented, and enforced Human Resources security policy, covering onboarding, role-based access allocation, periodic reviews, and secure deprovisioning during employee exit. These processes are aligned with ISO standards to ensure consistent implementation and data protection across all employee lifecycle phases.

2.4.2.3 Organization-Wide Acceptable Use Policy

YouTestMe enforces an organization-wide Acceptable Use policy, supported by clearly defined disciplinary measures. The policy is formally communicated during employee onboarding, available in internal documentation, and regularly reinforced through mandatory training sessions, ensuring compliance and understanding across all organizational levels.

2.4.2.4 Regular Information Security Awareness for Employees

YouTestMe implements a formalized plan to deliver continuous information security awareness sessions for all employees. These sessions include training, updates on security practices, and regular assessments to ensure employees maintain a high level of awareness and adherence to security protocols.

2.4.2.5 Maintenance of Contacts with Relevant Authorities and Institutions

YouTestMe maintains documented and established contacts with relevant authorities, information security specialists, and incident response teams to ensure guidance and support in addressing security matters and incidents effectively.

2.4.2.6 Measures for Remote Access and Use of Non-Corporate Devices

YouTestMe enforces an approved policy requiring secure configurations and multi-factor authentication before connecting to information systems from remote locations or non-corporate devices. Users are

challenged with strict access controls, ensuring compliance with defined security standards as outlined in the company's procedures and policies.

2.5 Secure Software & AI Proctoring

2.5.1 AI Proctoring & Exam Security

2.5.1.1 AI Proctoring in YouTestMe

YouTestMe employs pre-trained machine learning algorithms to process behavioral data through deterministic, rule-based methods. These algorithms deliver consistent outputs for identical inputs and lack adaptive capabilities. Their purpose is to assist proctors by providing insights and metrics to enhance the evaluation of the examination process.

2.5.1.2 AI Proctoring and Use of Personal Data for Training

The AI in YouTestMe was trained using public datasets, proprietary datasets, and collaboration with partners. Personal data, including special categories of personal data, was not used in the development or training of the AI system, ensuring compliance with data protection regulations.

2.5.1.3 Ensuring Security and Integrity of the AI System

Yes, YouTestMe has implemented measures to ensure the security, integrity, and robustness of the AI system throughout its lifecycle. These include secure coding practices, robust authentication, data encryption, adversarial testing, anomaly monitoring, timely system updates, and alignment with ISO 27001 and SOC 2 Type II standards.

2.5.1.4 Risk Management in AI Proctoring

YouTestMe conducts comprehensive risk assessments to identify and evaluate potential issues, including data security, fairness, privacy concerns, and algorithmic biases. Mitigation strategies include robust encryption, data minimization, regular audits, and adherence to ethical AI principles. End-users are informed about existing and potential risks to ensure transparency.

2.5.1.5 Communication of AI Proctoring Accuracy Levels

YouTestMe ensures end-users are informed of the AI proctoring system's accuracy through clear documentation, transparent reporting with confidence scores, and training for proctors and administrators. Updates affecting accuracy are communicated proactively, ensuring stakeholders understand system reliability, limitations, and accuracy thresholds for informed decision-making.

2.5.1.6 Testing and Verification of AI Proctoring System Reliability

The AI proctoring system in YouTestMe, developed by an external vendor and fully hosted on our servers, undergoes rigorous testing and verification. Integration testing ensures seamless functionality within YouTestMe's platform, and operational validation confirms consistent outputs under real-world conditions. Regular audits, quality assurance reviews, and testing of custom configurations ensure system reliability and reproducibility. All testing methodologies and results are documented to provide transparency and

traceability for stakeholders. These measures guarantee that the system meets the reliability standards expected by end-users and administrators.

2.5.1.7 Privacy and Data Protection in AI Proctoring Training Data

YouTestMe ensures the privacy and data protection of non-personal training and processed data by using ethical, GDPR-compliant datasets, applying anonymization techniques, and minimizing data usage strictly to what is necessary for the system's functionality and operational integrity.

2.5.1.8 Alignment of AI Proctoring with Relevant Standards

YouTestMe's AI proctoring aligns with ISO/IEC 27001 for information security and ISO/IEC 27701 for privacy management. Data retention is restricted to 30 days, with secure deletion compliant with GDPR. Strict access controls, logging, and regular audits ensure effective data governance and adherence to retention policies.

2.5.1.9 Mechanisms for Facilitating AI System Auditability

YouTestMe has implemented mechanisms to ensure AI system auditability, including comprehensive logging of activities and decision-making outputs, detailed session integrity reports, and role-based access controls for data protection. Regular internal and external audits validate compliance, while documented decision-making criteria and thresholds ensure transparency and traceability for review and verification.

2.5.2 Application Security & Development

2.5.2.1 Addressing Information Security in System Acquisition and Development

Information security requirements are integrated into the business case for all system acquisitions and developments. These requirements reflect the value of the information involved and assess potential damage from security failures, ensuring robust protection measures throughout the system lifecycle.

2.5.2.2 Outsourcing of Development Activities

YouTestMe does not outsource development activities. All development is performed in-house to ensure complete control over processes, maintain high-quality standards, and uphold strict information security requirements.

2.5.2.3 Inventory of Third Parties

YouTestMe maintains a detailed inventory of third-party software components utilized within the platform, including their respective licenses. This inventory is documented in the Third-Party License Notice, ensuring transparency and compliance with all licensing requirements.

2.5.2.4 Communication of Security Requirements to Third Parties

YouTestMe systematically communicates security requirements to all third parties. They are expected to adhere to these requirements and provide regular compliance reports to ensure alignment with YouTestMe's security standards.

2.5.2.5 Application Security Vulnerability Assessments

YouTestMe conducts monthly code scans using SonarQube, bi-monthly vulnerability scans, and semi-annual penetration testing.

2.5.2.6 Provision of Security Testing Results

YouTestMe can provide a copy of the latest security testing results in full or attestation format upon request. The report includes testing details, dates, a summary of results, and confirmation that all high or critical-level findings have been remediated.

2.5.2.7 Issue Remediation Timelines

YouTestMe ensures all Critical and High issues are resolved and patched immediately before software release. Medium and Low issues are prioritized and scheduled for resolution as quickly as possible, with a commitment to addressing all identified issues promptly to maintain system security and integrity.

2.5.2.8 Automated Source Code Scanning Tools

YouTestMe utilizes SonarQube, SonarLint, and the OWASP Dependency-Check Maven plugin for automated source code and dependency scanning. These tools ensure comprehensive identification and mitigation of potential vulnerabilities, maintaining code quality and security standards.