Technical and Organisational Measures(TOMs) Template

Ver 1.1

Document Control

Document Title: Technical And Organisational Measures(TOMs) Template	Effective Date: 27th May 2026
Document Code: MOENGAGE-PIMS-8038	Document Version No.: 1.1
Document Author: Sherlyn Stanley	Document Classification: Internal
Reviewed by: Girish KG & Meghna Panda	Approved by: Yashwanth Kumar

Revision History

Ver.	Revision Date	Nature of Change	Author	Reviewed by	Approved by	Date Approved
0.1	5th April 2024	Initial Draft	Sherlyn Stanley	Girish KG & Meghna Panda	Yashwanth Kumar	10th April 2024
1.0	17th Sep 2025	Annual review	Sherlyn Stanley	Girish KG & Meghna Panda	Guru Patnaik	22nd Sep 2025
1.1	20th May 2026	Annual Review	Sherlyn Stanley	Girish KG & Meghna Panda	Yashwanth Kumar	27th May 2026

Distribution

Distributed to	How	Mode
All MoEngage Employees	**Darwinbox & Scrut** Compliance Management Tool	- Online via Scrut Portal - Automated Emails on major Changes
Compliance & Governance Steering Committee	Compliance & Governance Steering Committee	- Regularly Scheduled Meetings
MoEngage Customers/Prospects	**Scrut Trust Vault** Data Sharing Portal	- Online via Scrut Trust Vault Portal - Automated Emails on major changes
External Auditors	**Scrut** Compliance Management Tool	- Regularly Scheduled Audits

moengage

TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA, PRIVACY, AND ARCHITECTURE

MoEngage takes data protection practices very seriously and has placed several controls and standards to diligently follow protocols protecting customers' data. MoEngage is committed to abiding by increased transparency regarding the processing of personal information.

A. Organization of Information Security & Data Privacy

- **Ownership**. MoEngage has appointed a Data Governance team under the Head of Security & Privacy Role, responsible for coordinating and monitoring Information security & Data privacy requirements and procedures. This team has the knowledge, experience, and authority to serve as the owner(s) of, with responsibility and accountability for, Information security & Data Privacy within the organization.

- **Roles and Responsibilities**. MoEngage has defined and allocated Data Governance responsibilities and implemented policies for Information security & data privacy in line with ISMS ISO 27001:2022 and PIMS ISO 27701:2019. Such policies (or summaries thereof) are published and communicated to respective stakeholders required to comply with such policies.

- **Project Management**. MoEngage addresses Information Security and Data Privacy in project management to identify and appropriately address security and privacy risks.

- **Risk Management**. MoEngage follows a risk management framework and conducts periodic risk assessments of its environment and systems to understand its risks and applies appropriate controls to manage and mitigate risks before Processing Protected Data.

B. Human Resources Security

- **General.** MoEngage ensures that its personnel are under a Non-Disclosure Agreement (NDA) that includes the protection of Protected Data and will provide adequate training about relevant privacy and security policies, procedures, and regulatory requirements. MoEngage further informs its personnel of the possible consequences of breaching MoEngage's security policies and procedures, including disciplinary actions, with the possibility of termination of employment for MoEngage employees and termination of contract or assignment for Representatives and temporary personnel.

- **Training**. MoEngage personnel with access to Protected Data receive appropriate, periodic education and training regarding privacy and security procedures for services to aid in the prevention of unauthorized use (or inadvertent disclosure) of Protected Data and training regarding how to effectively respond to security incidents. Training is provided before MoEngage personnel are granted access to Protected Data or begin providing services to customers. Training is regularly reinforced through refresher training courses, emails, posters, notice boards, and other training and awareness materials.

- **Background Checks.** MoEngage conducts professional history, criminal and other relevant background checks of all personnel and evaluates the results to ensure that there is no indication that the personnel may present a risk for theft of confidential data in compliance with Applicable Laws and MoEngage's policies.

C. Trusted Device Standards.

- MoEngage personnel who access Customers' confidential data:

    - Only use trusted Devices that are configured with security software (i.e., anti-virus, encryption, MDM, DLP, etc.);
    - Follow the MoEngage IT Security and Acceptable Usage policy when accessing Protected Data. These policies specify the requirements that a user device ("Devices") must satisfy to be trusted when accessing Protected Data via a restricted network [VPN]. Devices that fail to comply with this standard will not be entitled to access the Network.

- MoEngage IT Security and Acceptable Usage policy includes, at a minimum, the following:

    - Each Device is uniquely associated with a specific, individual user;
    - All operating system and application security patches are installed within the timeframe recommended or required by the issuer of the patch;
    - Devices are encrypted (i.e., full disk) and secured with a protected (SSO, two-factor authentication), and screens are locked with the automatic activation feature.;
    - Devices are periodically scanned for restricted/prohibited software; and
    - Devices run an acceptable industry-standard anti-malware solution.

- **Storage**. MoEngage has implemented policies designed to prevent the storage of Protected Data even on trusted devices or any physical storage media without prior written authorization from the MoEngage Data Governance team and Customer. MoEngage takes appropriate measures to prevent accidental exposure of Protected Data using solutions like Data Loss Prevention (DLP) and Mobile Device Management (MDM) on all laptops.

D. Personnel Access Controls

- **Access**

    - **Limited Use.** MoEngage understands and acknowledges that the Customer may grant MoEngage access to sensitive and proprietary information. MoEngage will not (i) access the Protected Data for any purpose other than as necessary to perform its obligations to Customer; or (ii) use any system to access information or log-in credentials to gain unauthorized access to Protected Data or to exceed the scope of any authorized access.

    - **Authorization**. MoEngage follows the Principle of Least Privilege and restricts, by default, and provides access to Protected Data solely to those Representatives whose access is necessary to perform MoEngage's obligations to the Customer.

    - **Suspension or Termination of Access Rights.** At Customer's reasonable request, MoEngage will promptly and without undue delay suspend or terminate the access rights to Protected Data for any of MoEngage's personnel or its Representatives reasonably suspected of breaching any of the provisions of the agreement with Customer; and

MoEngage ensures removal of access rights of all employees and external party users upon suspension or termination of their employment, or engagement.

- **Information Classification**. MoEngage internally classifies all customers' PII data as Restricted, while Non-PII Data as Confidential. MoEngage categorizes and/or tags Protected Data to help identify it and to allow for access and use to be appropriately restricted as per the defined classification level.

- **Access Policy.** MoEngage determines appropriate access control rules, rights, and restrictions for each specific user's roles towards their assets. MoEngage maintains a record of the security privileges of its personnel who have access to Protected Data, networks, and network services.

E. Access Authorization.

- MoEngage has user account creation and deletion procedures, with appropriate approvals, for granting and revoking access to the SaaS Infrastructure and Protected Data of the customer. MoEngage makes use of an enterprise access control system that requires revalidation of its personnel by managers and the governance team at regular intervals based on the principle of "least privilege" and need-to-know criteria based on job role/Performance obligations.

- For systems that process Protected Data, MoEngage revalidates (or, where appropriate, deactivates) access of users who change reporting structure and deactivates authentication credentials that have not been used for some time, not exceeding three (3) months.

- MoEngage restricts access to program source code and associated items such as software object code, designs, specifications, verification plans, and validation plans, to prevent the introduction of unauthorized functionality and to avoid unintentional changes.

F. Network Design. For systems that process Protected Data, MoEngage has implemented controls to prevent personnel from assuming access rights beyond those that they have been assigned to gain unauthorized access to Protected Data.

G. Authentication

- Where authentication mechanisms are based on passwords, MoEngage will require the password to conform to strong password control parameters (e.g., length, character complexity, and/or non-repeatability).

- MoEngage ensures that deactivated or expired identifiers and log-in credentials are not granted to other individuals.

- MoEngage monitors repeated failed attempts to gain access to the information system.

- MoEngage maintains industry-standard procedures to deactivate log-in credentials that have been corrupted or inadvertently disclosed.

- MoEngage makes use of industry-standard log-in credential protection practices, including practices designed to maintain the confidentiality and integrity of log-in credentials when they

are assigned and distributed, and during storage. Such practices are designed to ensure strong, confidential login credentials.

H. Cryptography and Key Management

- MoEngage ensures a policy on the use of cryptographic controls based on assessed risks.
- MoEngage assesses and manages the lifecycle of cryptographic algorithms, hashing algorithms, etc., and deprecates and disallows the usage of weak cypher suites and insufficient bit and block lengths.
- MoEngage has procedures for distributing, storing, archiving, and changing/updating keys; recovering, revoking/destroying, and dealing with compromised keys; and logging all transactions associated with such keys.

I. Physical and Environmental Security

MoEngage provides a completely [IaaS] Cloud-based SaaS Infrastructure to host its SaaS Infrastructure and related services to its customers. MoEngage only ensures Logical and administrative security of its SaaS infrastructure and relies on its IaaS Cloud Service provider for the Physical Security of data centres hosting physical resources.

- **Physical Access to Facilities**
    - MoEngage ensures its IaaS Cloud Service provider has
        - limited access to facilities where systems that Process Protected Data are located to authorized individuals.
        - defined Security perimeters and uses them to protect areas that contain Protected Data and Processing facilities.
        - Facilities that are monitored and access-controlled at all times (24x7) for unauthorized physical access.
        - Controlled access through key card and/or appropriate sign-in procedures for facilities with systems Processing Protected Data.

- **Physical Access to Equipment.** Physical systems hosting MoEngage services used to process or store Protected Data are protected using industry-standard processes to limit access to authorized individuals by the IaaS Cloud Service provider.
- **Protection from Disruptions**. MoEngage IaaS Cloud Service provider has implemented appropriate measures designed to protect against loss of data due to power supply failure or line interference.
- **Clear Desk**. MoEngage has policies requiring a “clean desk/clear screen” to prevent inadvertent disclosure of Protected Data.

J. Operations Security

- **Operational Policy.** MoEngage maintains written policies describing its security and privacy measures and the relevant procedures and responsibilities of its personnel who have access to Protected Data and to its systems and networks. MoEngage communicates its policies and requirements to all persons involved in the Processing of Protected Data and has implemented the appropriate management structure and control designed to ensure compliance with such policies and with applicable laws concerning the processing and protection of Protected Data.

- **Security and Processing Controls.**

- **Areas**. MoEngage maintains, documents, and implements standards and procedures to address the configuration, operation, and management of systems, networks, and services that store or Process Protected Data.
    -
- **Standards and Procedures**. Such standards and procedures include security controls, identification and patching of security vulnerabilities, change control processes and procedures, and incident prevention, detection, remediation, and management.
- **Threat intelligence**: Proactively identify and respond to evolving cyber threats, enhancing the existing risk management and operational security posture.

- **Configuration management**: Standardized and secure configuration baselines for all operational systems, reducing the attack surface and mitigating risks associated with misconfigured infrastructure.

- **Information deletion**: Protected Data is securely and permanently removed from all storage locations when no longer required, fulfilling data minimization and privacy compliance obligations.

- **Data masking**: Enhanced data protection during testing, development, and non-production environments by obscuring sensitive Protected Data, supporting privacy-by-design principles.

- **Data leakage prevention**: Formalized policies and technical controls to prevent unauthorized transmission of Protected Data, bolstering the existing measures for data loss prevention across all operational environments.

- **Monitoring activities**: A comprehensive framework for security monitoring beyond basic logging, enabling real-time detection and timely response to suspicious activities or security events.

- **Logging and Monitoring.** MoEngage maintains logs of administrator and operator activity and data recovery events related to Protected Data.

K. Communications Security and Data Transfer

- **Networks.** MoEngage ensures the following controls to secure its networks that access or Process Protected Data:

    - Network traffic passes through next-generation firewalls [NGFW], which are monitored at all times. NGFW also acts as EDR and IPS for flowing traffic.

- Cloud-based Network devices used for administration utilize industry-standard cryptographic controls when Processing Protected Data.

- Anti-spoofing filters and controls are enabled at cloud gateways and at each processing resource.

- Network, application, and server authentication passwords are required to meet minimum complexity guidelines (at least 8 characters with all of the following four classes: upper case, lower case, numeral, special character) and to be changed at least every 90 days; utilized along with Two Factor authentication.

- Initial user passwords are required to be changed at first log-on. MoEngage has a policy prohibiting the sharing of user IDs, passwords, or other login credentials.

- Protection layer against web-based threats by controlling access to malicious or inappropriate content, securing MoEngage's network infrastructure, and Protected Data.

- **Data Transfer.** MoEngage has formal data transfer policies in place to protect the transfer of information through the use of all types of communication facilities that adhere to the requirements of the agreement with the customer. Such policies are designed to protect transferred information from unauthorized interception, copying, modification, corruption, routing, and destruction.

L. System Acquisition, Development, and Maintenance

- **Security Requirements.** MoEngage adopts security requirements for the purchase, use, or development of information systems, including for application services delivered through public networks.

- **Development Requirements**. MoEngage has policies for secure development, system engineering, and support. MoEngage conducts appropriate tests for application security as part of acceptance testing processes. MoEngage also supervises and monitors the activity of outsourced system development, if any.
- **Secure coding**: MoEngage has secure coding practices and standards integrated into the development lifecycle, minimizing vulnerabilities in software and applications that process Protected Data.

M. Penetration Testing and Vulnerability Scanning & Audit Reports

- **Testing.** MoEngage performs periodic audits and penetration tests on SaaS infrastructure, application, and Processing Resources. These tests are conducted by both internal and external assessment teams. Upon written request from the Customer, MoEngage will provide a Vulnerability & Penetration testing report conducted by an independent 3rd party at the organization level, which may include an executive summary of the results and not the details of actual findings.

- **Audits**. MoEngage will respond promptly to and cooperate with reasonable requests by Customers for security audits, scanning, discovery, and testing reports.

- **Remedial Action**. If any audit or penetration testing exercise reveals any deficiencies, weaknesses, or areas of non-compliance, MoEngage will promptly take such steps as may be required, in MoEngage's reasonable discretion, to remedy those deficiencies, weaknesses, and areas of non-compliance as soon as may be practicable given the circumstances. Upon request, MoEngage will keep Customer informed of the status of any remedial action that is required to be carried out and will certify to Customer as soon as may be practicable that all necessary remedial actions have been completed.

N. Contractor Relationships

- **Policies.** MoEngage ensures information security policies or procedures are used by Representatives who impose requirements consistent with service agreements with customers.

- **Monitoring**. MoEngage ensures the monitoring and audit of service delivery by its Representatives. MoEngage reviews its Representatives' security practices against the security requirements outlined in MoEngage's agreements with such Representatives. MoEngage manages changes in Representative services that may have an impact on security.

- **Information security for the use of cloud services**: MoEngage manages risks associated with cloud computing by specifying security requirements for cloud service providers, ensuring consistent protection of Protected PII Data in cloud environments.

O. Management of Information Security Incidents and Data Breaches

- **Responsibilities and Procedures.** MoEngage ensures procedures for quick, effective, and orderly response to Information Security Incidents & Data Breaches.

- **Reporting**. MoEngage ensures to report Information Security Incidents and Data breaches through appropriate management channels to customers within 72 hrs.

- **Reporting Information Security Weaknesses**. MoEngage has implemented procedures to monitor, report, and manage any observed or suspected information security and privacy weaknesses in systems or services.

- **Assessment of and Decision on Information Security Events**. MoEngage has an incident classification scale in place to decide whether a security/privacy event should be classified as an Information Security Incident or a Data Breach. The classification scale is based on the impact and extent of an incident or breach.

- **Response Process**. MoEngage maintains a record of Information Security Incidents and Data Breaches with a description of the incident/breach, the effect of the incident/breach, the name of the reporter and to whom the incident/breach was reported, the procedure for rectifying the incident/breach, and the remedial action taken to prevent future security incidents/data breaches.

P. Information Security Aspects of Business Continuity Management

- **Planning.** MoEngage maintains emergency and contingency plans for all storage and processing resources that process Protected Data. MoEngage verifies the established and implemented information security continuity controls at regular intervals.
- **ICT readiness for business continuity**: MoEngage strengthens the existing business continuity and data recovery plans by specifically ensuring the underlying Information and Communications Technology (ICT) infrastructure is resilient and ready for disruption recovery.

- **Data Recovery.** MoEngage ensures that redundant storage and procedures for recovering data in a manner are sufficient to reconstruct Protected Data in its original state as found on the last recorded backup.

Q. Notification and Communication Obligations

- **Notification.** MoEngage, without undue delay (i.e., within 72 hours from confirmation) notify Customer if any of the following events occur:

    - any unmitigated, material security vulnerability, or weakness of which MoEngage has actual knowledge in (i) Customer's systems, or networks, or (ii) MoEngage's systems or networks, that have compromised Protected Data;

    - An Information Security Incident/data breach that compromises or is likely to compromise the security of Protected Data and weaken or impair the business operations of the Customer.

    - an Information Security Incident/data breach that negatively impacts the confidentiality, integrity, and availability of Protected Data; or

    - Known and wilful failure or inability to maintain material compliance with requirements of the agreement with customers and Applicable Laws.

- **Cooperation.**

MoEngage will: (i) respond promptly to any Customer's reasonable requests for information, cooperation, and assistance in any post-incident investigation, remediation, and communication efforts.

- **Information Security Communication.**

Except as required by Applicable Laws or by existing applicable contractual obligations, MoEngage agrees that it will not inform any third party of any of the events described above in this Section referencing, or identifying Customer, without Customer's prior written consent. MoEngage will fully cooperate with Customer and law enforcement authorities concerning any unauthorized access to Customer's systems or networks, or Protected Data. Such cooperation will include the retention of all information and data within MoEngage's possession, custody, or control that is directly related to any Information Security Incident. If disclosure is required by law, MoEngage will work with the Customer regarding the timing, content, and recipients of such disclosure. To the extent MoEngage was at fault, MoEngage will bear the cost of reproduction or any other remedial steps necessary to address the incident or compromise.

Technical and Organisational Measures for AI Operations

A. Data Isolation and Tenant Segregation

- **Logical Separation:** Enforcement of tenant isolation at both the application and infrastructure layers to ensure cross-tenant data leakage cannot occur.
- **Scoped Access:** Use of access-scoped service tokens and per-tenant authorization for all model invocations.
- **Enterprise Model Hosting:** Deployment of AI models within dedicated enterprise environments (e.g., AWS Bedrock model deployment accounts, Azure Direct Models) that structurally prevent underlying model providers from accessing customer prompts or completions.

B. Access Control and Identity Management

- **Role and Attribute-Based Access (RBAC/ABAC):** AI feature access is strictly tied to existing platform permissions. Users can only invoke AI capabilities (and use associated contextual data) on entities they are already authorized to access and modify.
- **Administrative Controls:** Workspace administrators possess granular controls to enable/disable specific AI features, restrict usage to specific roles, and define approved retrieval sources.

C. Input/Output Security and Injection Defenses

- **Prompt Injection Mitigations:** Strict logical separation between system instructions and user prompts, alongside output format constraints and deterministic validators.
- **Retrieval Sandboxing:** Retrieved context (RAG) is treated purely as data, not instructions, to prevent indirect prompt injection attacks.
- **Execution Sandboxing:** Strict output encoding, escaping, and sandboxed execution for any AI-generated code or templates (e.g., HTML/CSS/Jinja).

D. Safety Systems and Content Moderation

- **Layered Filtering:** Implementation of a multi-stage content moderation pipeline including pre-checks (input validation, blocklists), in-model provider filters (harm category thresholds), and post-checks (schema validation, brand constraints).
- **Data Masking:** Utilization of sensitive information filters and probabilistic detection to warn users or mask Personally Identifiable Information (PII) before it is processed by external foundation models.

E. Encryption and Network Security

- **Data in Transit and at Rest:** All AI-related data (prompts, outputs, embeddings) is encrypted in transit using TLS and at rest utilizing industry-standard key management practices.
- **Egress Controls:** Network segmentation and egress restrictions limit model endpoint access to approved destinations, utilizing private connectivity (e.g., AWS PrivateLink) where supported.

F. Audit Logging, Monitoring, and Rate Limiting

- **Forensic Logging:** Capture of detailed invocation events (user, timestamp, target entity, safety blocks/warnings) to support compliance and incident investigations.
- **Abuse Prevention:** Enforcement of quotas, rate limits, and anomaly detection (e.g., monitoring for usage spikes or repeated blocked prompts) to prevent unbounded consumption and system abuse.

G. Model Health and Automated Rollback

- **Drift Detection:** Continuous monitoring for distribution drift in input signals, safety drift (changes in block/refusal patterns), and sudden quality regressions.
- **Automated Triggers:** Pre-defined rollback and fallback routing mechanisms triggered by high error rates, latency spikes, or emergent abuse patterns.

Organisational Security Measures for AI Operations

A. Data Processing and Model Training Policy

- **Zero Proprietary Training Default:** Explicit prohibition on using customer proprietary data (Customer Inputs, Customer Data, Outputs) to train, fine-tune, or improve foundation models across different customers without explicit opt-in and contractual documentation.
- **Data Minimization:** Organizational directives requiring that prompts and context retrievals include only the minimum data necessary, explicitly discouraging the inclusion of PII or sensitive data unless strictly required and lawful.

B. AI Governance and Risk Assessment

- **Steering Committee & RACI:** Formal AI governance structure utilizing a defined RACI matrix (Responsible, Accountable, Consulted, Informed) overseen by the Compliance and Governance Steering Committee.
- **Tiered Risk Assessments:** Mandatory, documented risk assessments for all AI features categorized by impact tiers (Tier 0 to Tier 3), with defined mitigations and rollback triggers before deployment.

C. Change Management and Release Gates

- **Pre-Deployment Testing:** Mandatory release gates requiring Privacy, Security, Safety, and Legal reviews before material changes or new AI models are deployed.
- **Red-Teaming and Evals:** Use of offline test suites, rubric-based scoring, and adversarial red-teaming (e.g., data exfiltration and prompt attack testing) during the development lifecycle.

D. Human Oversight and User Agency

- **Draft vs. Deploy:** Generative AI outputs are strictly treated as drafts. Human review, editing, and explicit approval are required before AI-generated content or configurations can be deployed.
- **Maker-Checker Workflows:** Enforcement of peer review (maker-checker) approval workflows for high-impact AI operations where configured.

E. Vendor and Third-Party Risk Management

- **Subprocessor Due Diligence:** Strict vetting of AI subprocessors (e.g., Microsoft, Google, AWS) to ensure they publicly document and contractually commit to training restrictions, zero-retention (where applicable), and enterprise-grade security.

F. AI Risk and Incident Management

- **Impact and Risk Assessments:** We conduct comprehensive AI System Impact Assessments for all our AI systems, features, and products. This process helps us proactively identify potential AI risks, after which we carry out detailed AI Risk Assessments to evaluate and mitigate them.
- **Incident Management Procedure:** We have a robust AI Incident Management procedure in place, equipped to address, manage, and remediate any AI-specific breaches or incidents, should they occur.

G. AI Training and Reporting of AI Risks/AI glitches/AI concerns

- **AI Training for all employees:** MoEngage mandates AI awareness training for all personnel. This training enforces strict adherence to established AI prohibitions and ensures employees utilize exclusively IT- and Security-approved AI tools and platforms.
- **Reporting of AI Risks/AI glitches/AI concerns:** As part of continuous security awareness communications, employees are instructed to immediately report any identified AI risks, technical glitches, or compliance concerns to the dedicated security response channel at security@moengage.com.