Market Mx Privacy Policy
November 2026

1. Introduction

Market Mx is deeply committed to safeguarding your privacy. This security policy outlines the measures and practices we implement to ensure the security and integrity of Market Mx and our product Engage Mx. The policy is designed to protect the confidentiality, integrity, and availability of customer data and to comply with relevant legal and regulatory requirements.

2. Scope

This policy applies to all employees, contractors, and third parties who access or manage our SaaS application and the data within it. It covers all systems, networks, and data related to the application.

3. Data Protection

3.1 Data Encryption

- All sensitive data must be encrypted in transit using TLS 1.2 or higher.
- Data at rest must be encrypted using AES-256 or an equivalent level of encryption.

3.2 Data Retention and Disposal

- We have a no client data retention policy, unless required for critical system functions and legal purposes.
- Data is irreversibly destroyed, following NIST guidelines for media sanitization.

4. Access Control

4.1 Authentication

- Multi-factor authentication (MFA) is required for all internal users to access our applications and the same should be applied on the client side.
- Strong password policies are enforced, including regular password changes and complexity requirements.

4.2 Authorization

- Role-based access control (RBAC) is implemented to ensure users have access only to the data and systems necessary for their role.
- Regular reviews of user access rights is conducted to ensure compliance with RBAC policies.

4.3 Logging and Monitoring

- All access and administrative actions are logged and monitored.
- Logs must be retained for a minimum of 6 month and reviewed unauthorized access or suspicious activity.

5. Incident Response

5.1 Incident Reporting

- All employees and contractors must report security incidents immediately upon discovery.
- A formal incident response plan is in place, detailing the steps to be taken in the event of a security incident.

5.2 Incident Handling

- Incident response procedures include containment, eradication, and recovery steps.
- Post-incident analysis must be conducted to identify root causes and implement improvements to prevent recurrence.

6. Compliance

6.1 Regulatory Requirements

- We endeavor to comply with regulatory laws, including GDPR, CCPA, POPI and other data protection laws.

6.2 Third-Party Security

- Third-party vendors and partners are assessed for security risks and must comply with our security policies.
- Data sharing with third parties are governed by formal agreements ensuring the protection of shared data.

7. Employee Training

- All employees undergo regular security training to stay informed about the latest security threats and best practices.
- Training covers topics such as phishing, social engineering, and secure coding practices.

8. Physical Security

- Physical access to our offices is restricted to authorized personnel only.
- Security measures such as video surveillance, access controls, and alarm systems are in place to protect physical assets.

9. **Risk Management**
    - Yearly risk assessments are conducted to identify and mitigate potential security risks.

10. **Policy Review and Maintenance**
    - This security policy is reviewed and updated as needed to reflect changes in technology, laws, and business operations.
    - All updates to the policy are communicated to all employees and relevant stakeholders.