Information Security Measures

This document of **Information Security Measures** describes the administrative, technical, physical, and organizational safeguards implemented by MPMX in connection with the provision of the Services. These measures form part of the ToS and the Data Processing Terms and may be updated from time to time to reflect technological developments, operational improvements, or evolving security risks, provided the overall level of protection is not materially reduced. Security documentation is descriptive and does not constitute guarantees of specific technical configurations.

1. Information Security Program

MPMX maintains a comprehensive information security program designed to:

- ensure the confidentiality, integrity, and availability of Customer Data
- protect against unauthorized or unlawful access or Processing
- prevent accidental loss, destruction, or damage
- mitigate cybersecurity risks

MPMX regularly reviews and updates its information security program and conducts periodic internal security training for personnel.

2. Certifications and Standards

MPMX maintains an information security management system aligned with internationally recognized security standards. Upon reasonable request and subject to confidentiality obligations, MPMX may provide confirmation of its certification status.

3. Encryption

MPMX implements industry-standard encryption safeguards designed to protect Customer Data, including:

- encrypted communication channels for access to the Services
- encryption of Customer Data at rest where supported by the underlying infrastructure
- secure storage of credentials, authentication secrets, and encryption keys
- access controls restricting key management to authorized personnel

MPMX may update encryption methods in accordance with industry standards and technological developments.

4. Platform Security Controls

MPMX implements security controls designed to prevent unauthorized access to the Services, including:

- logically separated production and internal business environments
- secure administrative access procedures
- monitoring for unauthorized activity and security events
- centralized logging of security-relevant actions
- secure software development lifecycle practices
- protection against malware and known industry threats

MPMX does not knowingly introduce malicious code into the Services.

5. Infrastructure and Hosting Security

The Services may be hosted on certified third-party cloud infrastructure providers. Such providers maintain physical and environmental security measures which may include:

- controlled physical access to data centersvisitor identification procedures
- surveillance and monitoring systems
- fire detection and suppression systems
- redundant power and environmental controls
- climate control protections

MPMX ensures appropriate contractual security obligations are in place with such infrastructure providers.

6. Authentication, Authorization and Access Management

MPMX implements measures designed to ensure that access to Customer Data is restricted to authorized personnel only, including:

- individualized user accounts
- role-based access controls
- application of the principle of least privilege
- secure authentication procedures
- multi-factor authentication for administrative access where appropriate
- logging and review of privileged access

MPMX limits persistent access to production environments to personnel requiring such access for operational purposes.

7. Change Management and Systems Maintenance

MPMX maintains change management procedures designed to ensure that updates, patches, and system modifications are properly reviewed, tested, and approved prior to deployment. Security updates and vulnerability remediation are applied in accordance with internal risk-based procedures.

8. Backup, Business Continuity and Disaster Recovery

MPMX maintains backup and recovery procedures designed to ensure the availability and resilience of the Services, including:

- automated backup routines
- redundant storage mechanisms where appropriate
- documented disaster recovery procedures
- periodic testing of recovery processes

9. Security Monitoring, Testing and Vulnerability Management

MPMX conducts security monitoring and maintains procedures for identifying vulnerabilities and potential threats. These procedures may include:

- automated monitoring tools
- vulnerability assessments
- patch management processes
- periodic internal security reviews

MPMX may engage qualified third-party security specialists to conduct assessments or testing where appropriate.

10. Security Incident Management

MPMX maintains an incident response process designed to detect, respond to, and mitigate security incidents. Where a confirmed security incident materially affecting Customer Data occurs, MPMX will notify Customer without undue delay and provide available information required under applicable Data Protection Law.

11. Personnel Security and Administrative Safeguards

MPMX implements administrative safeguards including:

- confidentiality obligations for personnel
- onboarding and offboarding access procedures
- periodic security awareness training
- documented internal security policies

Background verification procedures may be applied where appropriate and legally permitted.

12. Customer Responsibilities

Customer remains responsible for:

- managing user access and credentials
- configuring available security features of the Services
- ensuring lawful collection and upload of Personal Data
- maintaining appropriate backups of Customer-controlled data sources
- protecting Customer-side infrastructure and endpoints

These Information Security Measures are effective as of the date of publication. Last updated: 01 May 2026.