TD-506 Last Updated: January 4, 2024

Technical and Organizational Manual

Overview

This MIM Software Technical and Organizational Measures (TOM) provides a high-level overview of the technical and organizational measures implemented by MIM Software Inc. (“MIM Software”) to protect personal data and ensure the ongoing confidentiality, integrity, and availability of MIM Services.

MIM Software® may revise these measures from time to time in the interest of improving operational security. You may obtain the latest version of this document from the MIM Software website.

Terms and Definitions

Within this document, the following definitions apply:

- CORE: An integral part of MIM Software’s day-to-day operations. This internal and protected database is used to manage Customer contact information, Customer communication involving technical support activities, portions of software design control, and other various quality system processes.
- Customer: Any user or potential user of MIM Services.
- Customer Data: Any personal data provided or submitted by the Customer that is processed by MIM Software.
- Data Center: A physically secured facility, or facilities, containing server equipment that hosts MIM Services.
- HubSpot: A software-as-a-service (SaaS) product for distributing marketing and technical materials, as well as hosting customer contact information for sales, marketing, and support activities.
- InfoSec Workgroup: A representative group of information technology and software engineer personnel who work to secure personal data in MIM Services.
- Medical Data: Any healthcare-related patient medical Personal Data relating to an identified or identifiable natural person.

- MIM®: A software solution provided by MIM Software to the Customer for multi-modality image review, fusion, storage, and processing comprising any number of software licenses and products.
- MIMcloud®: A software-as-a-service solution provided by MIM Software to the Customer for multi-modality image storage and sharing.
- MIM ID: A set of unique, identifying credentials, including multi-factor authentication, connected using the OAuth standard to various cloud hosted services.
- MIM Zero Footprint™: A software-as-a-service solution provided by MIM Software to the Customer for accessing MIM from a web browser.
- MIMweb: A software-as-a-service solution provided by MIM Software for the purpose of accessing MIM Software training materials, marketing materials, and software downloads.
- MIM Services: MIM, MIMweb, MIMcloud, and MIM Zero Footprint.
- Personnel: MIM Software employees.
- Personal Data: Any information relating to an identified or identifiable natural person.
- Personal Identifiable Data: Any Customer Data excluding Medical Data.
- Personal Data Breach: A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed, not including Service Incidents.
- Service Incident: An interruption to the normal functionality, accessibility, and/or availability of MIM Services including attempts to gain unlawful entry to or interfere with the system operations of MIM Services that temporarily disrupt availability but do not disclose Personal Data.
- Strong Encryption: The use of industry-standard encryption measures compliant with MIM Software's Encryption Policy.

1. Organization of Information Security

Objective

To describe MIM Software's information security structure.

Measures

- MIM Software employs information technology Personnel with full-time responsibility for information security.

- MIM Software employs software engineer Personnel with secondary responsibility for information security as part of their work.
- Information technology and software engineer Personnel comprise the InfoSec Workgroup which works to secure Personal Data in MIM Software products.
- The InfoSec Workgroup reports directly to MIM Software's Security Officer.
- MIM Software has a comprehensive set of information security policies that are approved by the Security Officer and disseminated to all Personnel.
- All Personnel are given training in information security.
- Personnel sign confidentiality agreements that apply during and after employment.

2. Information Security Management System

Objective

To demonstrate MIM Software's ongoing commitment to improving information security.

Measures

- MIM Software has implemented an ISMS (Information Security Management System) that serves as the foundation for its information security practices.
- The ISMS consists of a policy framework, information security resources, and defined roles for participation in security objectives based on the data minimization principle.
- The ISMS prescribes systematic security audits, review by management and information security Personnel, and corrective actions as necessary.

3. Physical Access

Objective

To protect physical assets that contain Customer Data.

Measures - CORE

- CORE is hosted on Amazon Web Services™ (AWS) in the US-East-2 region.
- Information related to AWS data center security can be obtained from the AWS website.

Measures - MIMcloud

- MIMcloud is hosted on Google Cloud Platform™ (GCP), and Amazon Web Services™ (AWS) in the EU, South America, US, Australia, and Asia.
- Customers can choose to store Medical Data sent to MIMcloud in AWS servers in the EU, South America, US, Australia, or Asia Data Centers.
- Information related to AWS data center security can be obtained from the AWS website.
- Information related to GCP data center security can be obtained from the GCP website.
- AWS and GCP are audited for compliance with MIM Software security policies.

Measures - MIMweb

- MIMweb is hosted both on Heroku, a platform-as-a-service (PaaS) product, for deploying software applications, and HubSpot. Both Heroku and Hubspot are hosted on AWS.
- Information related to AWS data center security can be obtained from the AWS website.
- AWS is audited for compliance with MIM Software security policies.

4. System Access

Objective

To ensure system-level access to systems containing Customer Data is only possible for approved, authenticated users.

Measures

- System-level access to MIM Software systems is granted to Personnel as necessary to fulfill business functions.

- Personnel who require system-level access to MIM Software systems must authenticate with a unique username and password, SSH key, and/or security token/certificate.
- MIM Software's Password Management Policy specifies complexity requirements, requires passwords to be stored in a Strongly Encrypted password manager and rotated on a regular basis, and prohibits sharing passwords except as necessary for business functions.
- MIM Software's Encryption Policy specifies key length and protection requirements for SSH keys.
- System-level access is revoked if no longer required.
- MIM Software has an established process to deactivate user accounts when Personnel leave the company.
- Customers do not have system-level access to MIM Software systems.
- All log-in attempts are captured in an audit log for accountability reasons.

Measures - CORE

- Subcontractors and outside parties do not have system-level access to CORE.
- Personnel who access AWS systems must supply an account token to log in.

Measures - MIMcloud

- Subcontractors and outside parties do not have system-level access to MIMcloud except as necessary to host the service based on the data minimization principle.
- Personnel who access AWS systems must supply an account token to log in.
- Personnel who access GCP systems must additionally authenticate with a second factor of authentication.

Measures - MIMweb

- Subcontractors and outside parties do not have system-level access to MIMweb except as necessary to host the service.
- Personnel who access Heroku systems must authenticate with a unique username and password.
- Personnel who access HubSpot systems must authenticate with their MIM ID.

5. Data Access/Data Deletion

Objective

To ensure persons authenticated to data processing systems are only allowed to access Customer Data they are authorized to access.

Measures

- MIM Software uses access controls to assign authenticated users the lowest level of access to Customer Data as necessary to fulfill their business functions in accordance with the purpose limitation principle.
- MIM Software has an established process for requesting access to Customer Data.
- Personnel training includes guidelines on the definition and use of Customer Data.
- MIM Software uses up-to-date, anti-malware software on all employee workstations and servers that interact with Customer Data.
- MIM Software uses well-configured firewalls to limit access to services that process Customer Data.
- Access to services that process Customer Data is logged and monitored.

Measures - CORE

- There are three access control levels to Customer Data in CORE.
    - Administrative access: Access to all Customer Data and full management privileges.
    - Standard access: Access to all Customer Data and partial management privileges.
    - No access: No access to Customer Data.
- If a Customer requests deletion of all Customer Data stored in CORE, MIM Software will verify that there is no other lawful basis to preserve the Customer Data. If there is no lawful basis, MIM Software will logically delete the Customer Data from CORE.

Measures - MIMcloud

- MIM Software uses AWS and GCP access controls to assign authenticated users the lowest level of access to Customer Data as necessary to fulfill their business functions.
- There are four access control levels used in GCP.

    - Owner: Access to all Customer Data and full management privileges.
    - Editor: Access to all Customer Data and partial management privileges.
    - Viewer: Access to all Customer Data and no management privileges.
    - No access: No access to Customer Data.
- Access controls are set on a per-user, per-task basis in AWS.
- MIMcloud uses the zero-knowledge principle to ensure that Medical Data cannot be decrypted by Personnel except with the Customer's prior explicit consent for troubleshooting purposes.
- If a Customer requests deletion of all Medical Data stored in MIMcloud, then the Customer's MIMcloud account is deleted. To protect against malicious actions, there is a grace period of 24 hours during which data recovery is possible.
- If Medical Data would be deleted automatically due to lifecycle expiration while the customer has an active subscription, there is a grace period of 1 year during which data recovery is possible.

Measures - MIMweb

- MIM Software uses Heroku's access controls to assign authenticated users the lowest level of access to Customer Data as necessary to fulfill their business functions.
- There are two access control levels to Customer Data in Heroku.
    - Standard access: This includes access to all Customer Data.
    - No access: This prevents the Personnel from accessing any Customer Data.
- Access to Hubspot, including access to Customer Data stored within Hubspot, must be granted by an existing Administrator. Access control is broken down into the following levels:
    - Administrator: Access to all Customer Data, and the ability to grant access to other personnel at MIM.
    - User: Access to all Customer Data.

6. Data Transmission/Storage

Objective

To ensure Customer Data is not accessed by unauthorized parties while in transit or after it is stored.

Measures

- MIM Software uses Strong Encryption for all transmission of Customer Data.
- Customer Data is protected by Strong Encryption at rest.

Measures - CORE

- Access to CORE is protected by Transport Layer Security (TLS), version 1.2 or higher. Clients will use the latest version of TLS they support.
- Customer data is stored encrypted at rest using AES-256.

Measures - MIMcloud

- Customer Data is encrypted on the Customer's machine before being sent to MIMcloud.
- Access to MIMcloud is protected by TLS version 1.2 or higher. Devices will use the latest version of TLS that they support.
- All Customer Data received by MIMcloud is automatically encrypted using Strong Encryption before being written to disk.
- All Medical Data received by MIMcloud is encrypted once again using a randomly-generated AES-128 encryption key.
- The AES key used to encrypt Medical Data is encrypted with a private key derived from the user's password.
- If a Customer shares Medical Data in MIM Zero Footprint without securing it with a password, then anyone with the link is able to access it including MIM Software.

Measures - MIMweb

- Access to MIMweb is protected by TLS version 1.2 or higher. A device will use the latest version of TLS it supports.
- Access to HubSpot is protected by TLS version 1.2 or higher. A device will use the latest version of TLS it supports.

7. Confidentiality and Integrity

Objective

To ensure Customer Data remains confidential, complete, and current during processing.

Measures

- The InfoSec Workgroup trains Personnel in application security, system administration security, and secure coding practices in accordance with the awareness principle.
- MIM Software has a central, secured repository of product source code that is only accessible to authorized Personnel.
- MIM Software has a formal code review process to comply with the GDPR principle of Data Protection by Design.
- All encryption and other cryptographic functionality used within MIM Services uses Strong Encryption.

Measures - MIMcloud

- Functional tests and unit tests performed on MIMcloud include security testing.

8. Availability

Objective

To ensure Customer Data is protected from accidental destruction or loss; to provide timely recovery of Customer Data availability in the event of a Service Incident or Personal Data Breach.

Measures - CORE

- CORE relies on the data center controls provided by Amazon Web Services as outlined here: AWS Data Center Controls
- MIM Software performs regular backups of Customer Data that are stored in the Data Center and secured using Strong Encryption.

Measures - MIMcloud

- Information related to availability and business continuity of AWS data centers is available from Amazon's Security Processes document.
- Information related to availability and business continuity of GCP data centers is available from the Google Cloud Platform web site.
- MIM Software ensures continued availability of Customer Data through comprehensive redundancy in GCP.

Measures - MIMweb

- Information related to availability and business continuity of AWS data centers is available from Amazon's Security Processes document.
- MIM Software performs regular backups of Customer Data using snapshots taken from a mirror of the production database.

9. Job Control

Objective

To ensure Customer Data is processed on a Customer's behalf in accordance with all relevant agreements including the use of subprocessors.

Measures

- MIM Software uses Braintree as a subcontractor to process Personal Identifiable Data for Customer payments.
- Braintree collects Personal Identifiable Data necessary to process payments.

Measures - CORE

- MIM Software acts as a data controller with respect to Personal Identifiable Data stored in CORE.
- MIM Software uses Personal Identifiable Data in CORE to provide the Customer with sales- and support-related services including but not limited to invoice generation, license activation, and product announcements.
- Personal Identifiable Data stored in CORE is not accessed by any processors.

Measures - MIMcloud

- MIM Software acts as a data processor and data controller with respect to Personal Data stored in MIMcloud.
- MIM Software processes Personal Data stored in MIMcloud in order to provide services to the Customer which MIM Software is obligated to perform in support of the Customer's experience including general operation of the service, troubleshooting purposes, and maintenance purposes.
- Medical Data stored in MIMcloud is not accessed by any subprocessors.
- Medical Data stored in MIMcloud is not accessible by Braintree.

Measures - MIMweb

- MIM Software acts as a data controller with respect to Personal Identifiable Data stored in MIMweb.
- MIM Software uses Personal Identifiable Data in MIMweb in order to provide access to MIM Software training materials and software downloads.
- Personal Identifiable Data stored in MIMweb is not accessed by any processors.

10. Data Separation

Objective

To ensure all Customer Data is processed separately.

Measures - CORE

- Since CORE cannot be accessed by Customers, it is unnecessary to implement a multi-tenant architecture to enforce data segregation between Customers.

Measures - MIMcloud

- MIMcloud uses logical separation within its architecture to enforce data segregation between Customers. Customers have access only to their own Customer Data.
- Medical Data stored in MIMcloud is Strongly Encrypted with encryption keys for Medical Data that reside solely with the Customer.

Measures - MIMweb

- MIMweb uses logical separation within its architecture to enforce data segregation between Customers. Customers only have access to their own Customer Data.
- When a Customer logs in to MIMweb, the Customer receives a session cookie that authenticates them as that user.

11. Service Incident and Personal Data Breach Management

Objective

To take appropriate actions in the event of a Service Incident or Personal Data Breach that affects Customer Data.

Measures

- MIM Software monitors information provided by the information security community and works to patch any known vulnerabilities in MIM Services as soon as possible.
- MIM Software Personnel install system software and security patches at regular intervals.
- MIM Software maintains up-to-date incident response plans that include Personnel responsibilities, guidelines for assessing the risk, and response plans and procedures.
- MIM Software regularly tests its incident response plans and revises them as appropriate based on the results.
- In the event of a Personal Data Breach, MIM Software will follow its data breach policy.
- Audit logging is enabled in all MIM Services to assist with diagnosing Service Incidents and Personal Data Breaches.
- The clocks of all systems used to run MIM Services are synchronized to a reference time source to ensure that timestamps in audit logs are accurate.

Measures - CORE

- Security patches are applied to AWS database systems as soon as possible by Amazon.

Measures - MIMcloud

- Security patches are applied to AWS and GCP systems as soon as possible by Amazon and Google respectively.
- Strong Encryption is used to secure Customer Data in MIMcloud that can only be reversed by the Customer.

Measures - MIMweb

- Security patches are applied to AWS systems as soon as possible by Amazon.

12. Compliance

Objective

To ensure the technical and organizational measures listed above are regularly reviewed for continued efficacy.

Measures

- MIM Software performs regular audits of its security practices and prescribes corrective actions accordingly.
- MIM Software ensures that Personnel comply with all applicable security policies through methods including but not limited to business tool reports, periodic walkthroughs, and ethical use of penetration testing products.
- MIM Software performs at least annual penetration tests of MIM Services.