Technical and Organizational Security Measures

Information Security Organization

Mitel has an information security organization that is responsible for planning, implementing, and overseeing all information security measures. At the head of this organization is the Chief Information Security Officer (CISO), who takes over the strategic direction and coordination of information security measures. The CISO is supported by a team of IT security experts who are responsible for the operational implementation and continuous improvement of security measures.

Security Policies

Mitel is committed to maintaining the highest security standards through security policies that safeguard our customers' data and business operations. Our policies are designed to align with industry's best practices, regulatory requirements, and risk management frameworks, ensuring confidentiality, integrity, and availability. Mitel policies apply to anyone who has access to Mitel information systems and data. We periodically review and amend our security policies to maintain protection of employee and customer information.

Network and System Security

Network Security is a critical component of Mitel's overall security posture, encompassing measures to protect the integrity, confidentiality, and availability of data and resources within Mitel's network.

- **Secure Configuration**: Mitel ensures that network devices and systems are securely configured. This includes applying security patches and updates.
- **Network Segmentation**: The Mitel network is segmented to limit the impact of a security breach. Customer data is segmented physically and logically for all cloud platforms as well as from the corporate network. Production, test and development environments are also kept separated.
- **Monitoring and Logging**: Mitel implements monitoring and logging to track network activity and identify any unusual or suspicious behavior.
- **Firewalls**: Mitel utilizes firewalls to monitor and control incoming and outgoing network traffic based on predetermined security rules, ensuring that only authorized and secure communications are allowed.
- **IDS/IPS**: Mitel implements IDS/IPS at the perimeter firewalls. High severity real-time threats against known vulnerabilities are blocked by IPS and alerts are forwarded to the SIEM for triage and analysis.
- **Secure Remote Access**: Mitel has deployed Secure Remote Access technology to encrypt all network traffic between remote devices and the corporate network.
- **Media Handling**: Mitel will implement protections to secure portable storage media from damage, destruction, theft or unauthorized copying and the personal data stored on portable media through encryption and secure removal of data when it is no longer needed. Additional similar measures will be implemented for mobile computing devices to protect personal data.

Workstations Security

Mitel implements endpoint protections on end-user devices and will monitor those devices to be following best practice security standards requiring as a minimum: strong authentication, screen saver/lock for idle time, up-to-date antivirus with regular scans, real-time software protection, firewall software, supported OS with automated patching, critical software patching, and hard disk encryption. Controls are implemented to detect and remediate workstation compliance deviations.

Data Center Cloud Infrastructure Partners

Mitel's data center cloud infrastructure partners, at a minimum, adhere to Tier III data center requirements. Such facilities are access-controlled with 24/7 on site security restricting entry into the facilities to authorized personnel. These data centers have redundant power, redundant cooling and redundant network connectivity. Our cloud partners maintain a comprehensive disaster recovery (DR) plan that includes backup strategies and procedures for recovering data and applications in the event of disaster.

Data Encryption

- **Encryption at Rest**: All sensitive data stored on company servers or storage devices is encrypted using strong encryption algorithms.
- **Encryption in Transit:** Data transmitted over the network is encrypted as per Mitel corporate standards.

Access

Physical Access Control and Security

Mitel's access controls ensure that only authorized persons have access to systems that process or use personal data and to the facilities where such processing takes place.

- All Mitel Data Center sites are secured against unauthorized access through automated access control systems and monitoring.
- Office ingress points and secured areas are secured by an electronic access control system including real-time monitoring where appropriate.
- Employee and Visitor access rights are reviewed and controlled by Mitel policy which includes employee assisted visitor logging and escort.
- A clean desk, secure disposal and physical security policy is in place.

Logical Access Control

The goal of logical access control is to ensure that only authorized persons are able to access systems that process and use personal data, and that such access is based on legitimate and authorized need to access. Data terminals (workstations, servers, network components and devices) are accessed by means of authorization and authentication in all systems. Mitel's access control regulations include the following measures:

- Strong authentication mechanisms, using passwords in combination with multi-factor authentication (MFA), are used to verify the identity of users.
- Strong and complex password policy including regular password changes.
- Role-based access control (RBAC) is implemented to restrict access to data and systems based on the principle of least privilege.
- Access to sensitive data is logged and monitored to detect and respond to unauthorized access attempts.
- Tracking and regular review of all existing privileged accounts is carried out.
- Rights management both onboarding and offboarding are controlled by Mitel policy.

Incident Response

Mitel will maintain an incident response plan and follow documented incident response policies including data breach notification to Data Controller without undue delay where a breach is known or reasonably suspected to affect Client Personal Data.

Risk Management

Mitel will assess risks related to processing of Personal Data, Security and Business Operations and will create an action plan to mitigate identified risks.

Vulnerability Management

The Vulnerability Management process systematically identifies, reviews, addresses, and remediates vulnerabilities within Mitel managed computing environments. This includes:

- **Vulnerability Assessment**: Mitel conducts regular vulnerability assessments using automated scanning tools and manual techniques to identify vulnerabilities in systems, applications, and network infrastructure.

- **Patch Management**: Mitel has a patch management policy and process to promptly apply security patches and updates to meet objectives.
- **Security Advisories**: Mitel actively monitors and assesses security threats, notifications and advisories that are applicable to the Mitel environment.

Business Continuity

- **Data Backup**: Regular backups of critical data are performed. Immutable backups are stored off network and are encrypted.
- **Regular Testing**: Regular testing of the backup and restore procedures are conducted to validate their effectiveness and identify areas for improvement.
- **Monitoring and Alerts**: Monitoring and alerting are in place for backup processes and storage usage to proactively identify issues and ensure timely resolution.
- **Hybrid Workforce**: In the event of facility closures or disruptions, Mitel's workforce is equipped to work remotely to ensure business continuity.
- **Industry Standard Technologies:** To protect against loss of critical services caused by system component failures (power supply, fans, drives, or line interference) Mitel utilizes several technologies including: redundant power, cooling and networking with failover capabilities and data backups stored in a physically separate location from the primary site. Access to these backups is restricted to authorized personnel.

Organizational Measures

Data Protection Officer

Mitel has appointed a Group Data Protection Officer, based in Germany (EU), who shall be responsible for monitoring Mitel's personal data processing activities and providing independent advice on ongoing compliance with applicable data protection laws and regulations. The Group Data Protection Officer leads a global team of international data protection specialists with multidisciplinary expertise in data protection law, AI and digital ethics and experience working across various jurisdictions.

Employee Confidentiality Obligation

Mitel employees are by default obliged to maintain Mitel's business and professional secrets through confidentiality clauses in their employment agreements or may sign a case specific confidentiality agreement, when necessary.

Training and Awareness

All Mitel employees are assigned mandatory (i) global data protection and (ii) security and awareness training as part of their onboarding process and receive continuous training annually thereafter. Training completion rate is tracked and monitored and failure to comply may result in disciplinary action. Mitel Data Protection training is annually reviewed and updated to reflect new legislative and jurisprudential developments. Training includes procedures for handling, transferring and storing Personal Data and how to respond effectively to security events. Security and awareness training program is designed to educate and empower Mitel employees to recognize, report and respond to potential security risks and suspected incidents. By enhancing the awareness of our workforce, we aim to create a culture of security consciousness that permeates throughout the organization.

Contractor and vendor management

Mitel takes commercially reasonable steps to select and retain only third-party service providers that will provide guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of privacy regulations and ensure the protection of the rights of data subjects.

Data Processing Agreements

Where applicable, Mitel will enter into a Data Protection Agreement with its customers, partners and sub-processors, whereby the roles of the parties and their rights and obligations in terms of personal data processing are clearly defined and contractually agreed.

International Transfers of Personal Data

In case of transfers of personal data outside the EU, and in the absence of an adequacy decision from the EU Commission, Mitel may transfer personal data to a third country or an international organization, by concluding Standard Contractual Clauses (SCCs) in the respective module. For transfers within the Mitel Group, Mitel has executed an Intra-Group Personal Data Transfer Agreement (“Intra-Group Agreement”). The Intra-Group Agreement incorporates the EU Commission 2021 Standard Contractual Clauses and the UK Standard Contractual Clauses.