MOVIUS

MultiLine Security

Last Modified on 12/01/2023 3:13 pm EST

Movius follows the highest industry standards to ensure that you can trust us with your critical data.

Movius Internal IT Security

- We understand the importance of information security, including cybersecurity, to protect against external threats and malicious insiders.
- Our cybersecurity strategy prioritizes detection, analysis and response to threat intelligence, cyber risks, and malicious activity.
- We continuously strive to meet or exceed the industry's information security best practices and apply controls to protect our clients and the infrastructure of the company.

Security Certifications

- Our information security management program is built to comply with the ISO 27001 framework.
- The security controls for the Movius platform annually undergo SOC 2 Type 2 examination against AICPA defined standards.

Encryption

- All data is encrypted in transit and at rest.

Secure Cloud Data Center

- Your data is protected using FIPS 140-2 Level 3 compliant HSMs and customer owned encryption keys.
- Storage is compliant with:
  - Federal Information Processing Standard (FIPS) Publication 140-2
  - Federal Information Security Management Act (FISMA)
  - Health Insurance Portability and Accountability Act (HIPAA)
  - Payment Card Industry (PCI)
  - Basel II
  - California Security Breach Information Act (SB 1386)
  - EU Data Protection Directive 95/46/EC

Security Scanning

- SAST and DAST are performed for every maintenance and general release.
- Manual Penetration testing is performed annually.
- Bi-weekly vulnerability scan is performed by in-house security experts.

Disaster Recovery and Geo-redundancy

- Movius performs daily backups of production data that is only used to minimize data loss in

the event of a disaster.
- Production data is immediately written to an independent 2nd database which is either at the same location for single site installations or at a second data center in geo-redundant configurations.
- We complete re-certification and surveillance audits annually.

Manage Users and Admins

Admin Audit Logging

- All activities by Admins in Management Portal and Developers using the API are logged in Admin logs.
- Full search functionality helps you quickly track down activities of interest, including:
  - Log in
  - Adding, deleting, or viewing an account
  - Viewing or downloading a report
  - Viewing or downloading data
- You can also set up alerts for activities, such as password changes and deleted accounts. *See Manage Alerts* (https://moviuscorp.knowledgeowl.com/help/manage-alerts)

Admin Access Control

- Fine tune which organizations, data, and functions Admins can access by assigning Roles. *See What Admin Privileges are in Management Portal?* *(https://help.moviuscorp.com/help/what-admin-roles-mmp)*
- Require two factor authentication to log in. *See Enable Two Factor Authentication for Admins* (https://help.moviuscorp.com/help/enable-two-factor-authentication-2fa-for-management-portal-admins).

User Access Control

- Admins have complete control over user access to MultiLine app. It's possible immediately suspend or delete a user account from Management Portal to remove access to the application.
- Calls to a MultiLine number from a deleted account can automatically forwarded, tagged for a specific use or organization, or made generally available.
- Call or message recording is set by admins and does not allow users to turn the feature on or off, preventing any circumventing of your recording policies.

EMM Integration

- You can apply any policies from your Enterprise Management solution to the MultiLine application.
  - Apply corporate authentication and password requirement policies to MultiLine applications.
  - Enforce using MultiLine applications when using corporate apps, including phone number links and conference codes.
  - Restrict copy and paste, screenshots, and more from MultiLine to outside apps.

GDPR

- We ensure ongoing compliance with the General Data Protection Regulation (GDPR).
- Users can clearly see what data is shared and have the option to opt in or out of sharing their personal data.

Account Cancellation

- You may cancel with us at any time by contacting our Customer Success team.
- We will work with you to offload your data and then securely remove your data from the platform.