MOVIUS

Movius Hosting & Delivery Policies

Last updated: March 2022

Table of Contents

Movius Hosting & Delivery Policies

Unless otherwise stated, these Movius Hosting & Delivery Policies (the "Policies") describe the Movius Cloud Services subscribed by you. These Policies may reference other Movius documents. Any reference to "Customer" in these Policies or in such other documents shall be deemed to refer to "you" as defined in the ordering document.

Overview

The Movius Cloud Services are provided under the terms of the agreement, ordering document and these Policies. Movius' delivery of the services is conditioned on you and your users' compliance with your obligations and responsibilities defined in such documents and incorporated policies. These Policies and the documents referenced herein, are subject to change at Movius' discretion. Movius policy changes will not result in a material reduction in the level of performance, security or availability of Movius Cloud Services during the Service Period.

Access: Movius Cloud Services are hosted at IBM SoftLayer data center facilities globally. Movius defines the services' network and system architecture, hardware and software requirements. Movius may access the environment to perform the Cloud Services including the provisioning of services.

Hours: The Movius Cloud Services are designed to be available 24 hours a day, 7 days a week, 365 days a year, except during system maintenance periods and technology upgrades and as otherwise set forth in the agreements, the ordering document and these Policies.

1. Movius Cloud Security Policy

1.1. User Encryption for External Connections

The Movius application encrypts all VoIP calls using SIP over TLS 1.2 with 256-bit SHA2 encryption. Minutes calls use the carrier's network and so utilize security inherent in underlying network technology.

Customer access to the Movius Management Portal is through the Internet. TLS encryption technology is enabled for this access. TLS connections are negotiated for at least 256-bit encryption or stronger. The private key used to generate the cipher key is at least

2048 bits. It is recommended that the latest available browsers certified for the Movius Portal, which are compatible with higher cipher strengths and have improved security, be utilized. Certified browsers include Safari 9+; Internet Explorer 11; Firefox 49+ and Chrome 54+.

RESTful web services are used to extract recordings. Data is decrypted automatically by the Web Services API and presented in unencrypted form to clients. HTTPS is used to ensure security of requests and responses to the API client.

1.2. Segregation in Networks

Movius partner data centers contain isolated networks used to deliver Cloud Services to Movius Customers. Networking technologies are deployed in a layered approach designed to protect Customer data at the physical, data link, network, transport, and program level. Access controls are multi-tiered, consisting of the network, system, database, and program layers. Access is based on a “least privilege” policies.

1.3. Network Access Control

Movius operations teams access Customer environments through a segregated network connection, which is dedicated to administrative access and isolated from Movius' internal corporate network traffic. The dedicated network functions as a secured access gateway between support systems and target program and database servers. Authentication, authorization, and accounting are implemented through standard security mechanisms designed to ensure that only approved operations and support engineers have access to the systems. Cryptographic controls are implemented to provide Movius operations and support with secured, easily configured access to target programs.

1.4. Network Bandwidth and Latency

Movius assures that adequate bandwidth exists for carrying IP-based telephony and data traffic to support its cloud-based subscribers with the highest quality service for the portion of the connections under the control of Movius and/or the providers of any leased data center facilities.

However, Movius cannot control the quality of any IP telephony or data service used by its Customers or their end Users to connect to the Movius Cloud Architecture. In certain situations, the quality of such service is under control of the Customer or End Users. In such cases, in order to assure adequate real-time usability by the End Users it is the responsibility of the Customer and the End Users to ensure that their access to Movius Cloud Services is made over connections with adequate performance to not adversely affect such use.

1.5. Network Routing Control

1.5.1. Routers

Router controls implemented for the Movius Cloud Service provide the connection point between the Movius Cloud Service and the Internet Service Provider(s). Border routers are deployed in a redundant, fault tolerant configuration. Routers are also used to enforce traffic policies at the perimeter.

1.5.2. Firewalls

Firewalls are used to enforce access rule sets for both external and internal VLANs within the Movius Cloud Architecture. Rule sets limit access by protocol, port source IP address, destination IP address, etc. to identify authorized sources, destinations, and traffic types. The firewalls in use protect against (block) anonymous proxies.

Movius uses a whitelisted firewall to only allow certain IP addresses to access the IPSEC tunnel to the Movius Cloud Services. This includes protection against BOGON addresses.

1.6. Network Security Management

1.6.1. Network Controls

Movius Cloud Services protect network traffic interfacing with the Movius Cloud Services using a combination of Firewalls and Intrusion Detection Systems (IDS) or Intrusion Detection and Prevention Systems (IDPS) as appropriate.

Firewalls use stateful packet inspection to limit access by protocol, port source IP address, destination IP address, etc. to identify authorized sources, destinations, and traffic types. These firewalls

also provide barriers between the public and private VLANs within the Movius Cloud Services architecture.

1.6.2. Network Vulnerability Assessments

Movius utilizes network vulnerability assessment tools to identify security threats and vulnerabilities. Formal procedures are in place to assess, validate, prioritize, and remediate identified issues. Movius subscribes to vulnerability notification systems to stay apprised of security incidents, advisories, and other related information. Movius takes actions on the notification of a threat or risk once confirmed that a valid risk exists, that the recommended changes are applicable to service environments, and the changes will not otherwise adversely affect the services.

1.6.3. Anti-Virus Controls

Movius employs anti-virus software to scan uploaded files when deemed necessary. Virus definitions are updated daily.

1.6.4. Configuration Control/Audit

Movius uses a centralized system for managing the access and integrity of network device configurations. Change controls are in place to ensure only approved changes are applied. Regular audits are also performed to confirm compliance with security and operational procedures.

1.7. System Hardening

Movius employs standardized system hardening practices across cloud devices. This includes restricting protocol access, removing or disabling unnecessary software and services, removing unnecessary user accounts, patch management, and logging.

1.8. Physical Security Safeguards

Movius provides secured computing facilities for both office locations and production cloud infrastructure. Common controls between office locations and Cloud datacenters currently include, for instance:

- Physical access requires authorization and is monitored.
- Everyone must visibly wear official identification while onsite
- Visitors must sign a visitor's register and be escorted and/or observed when on the premises

- Possession of keys/access cards and the ability to access the locations is monitored. Staff leaving Movius employment must return keys/cards

Additional physical security safeguards are in place for all Cloud data centers, which currently include safeguards such as:

- Premises are monitored by CCTV
- Entrances are protected by physical barriers designed to prevent vehicles from unauthorized entry
- Entrances are manned 24 hours a day, 365 days a year by security guards who perform visual identity recognition and visitor escort management

1.9. System Access Control & Password Management

Access to Movius Cloud systems is controlled by restricting access to only authorized personnel. Movius enforces strong password policies on infrastructure components and cloud management systems used to operate the Movius Cloud environment. This includes requiring a minimum password length, password complexity, and regular password changes. Strong passwords or multi-factor authentication are used throughout the infrastructure to reduce the risk of intruders gaining access through exploitation of user accounts. System access controls include system authentication, authorization, access approval, provisioning, and revocation for employees and any other Movius-defined 'users'.

Customers are responsible for all User administration for the Movius Management Portal. Movius does not manage Customer End User accounts. Customers may configure the additional built-in security features.

1.10. Review of Access Rights

Network and operating system accounts for Movius employees are reviewed regularly to ensure appropriate employee access levels. In the event of employee terminations, Movius takes prompt actions to terminate network, telephony, and physical access for such former employees. Customers are responsible for managing and reviewing access for their own employee administrative accounts.

1.11. Security-Related Maintenance

Movius performs security related change management and maintenance as defined and described in the Movius Cloud Change Management Policy. For any security patch bundle, Movius will apply and test the security patch bundle on a stage environment first. Movius will apply the security patch bundle to the production environment of the Cloud Service after Movius successfully completes testing on the stage environment.

1.12. Data Management / Protection

Safeguards provide security for any Customer or End User data stored in the Movius Cloud. Customers and End Users are responsible for the data security of any network or device used to access the Movius Cloud Services.

1.12.1. Data Protection

Please see section 1.1 on protection offered for data transmission. In addition, Voice and SMS recording metadata and SMS content is encrypted at rest using AES-256-CBC.

1.12.3. Data Disposal

Upon termination of services (as described in the Movius Cloud Suspension and Termination Policy) or at a Customer's request, Movius will delete customer data in a manner designed to ensure that the data cannot be accessed or read, unless there is a legal obligation imposed on Movius preventing it from deleting all or part of the data. Customer data is removed from all primary and backup locations.

1.12.4. Security Incident Response

In the event of an incident of unauthorized access to or handling of Customer data, the Movius Incident response team will work with the Customer and the appropriate technical teams to respond to the incident. The goal of the incident response will be to restore the confidentiality, integrity, and availability of the Customer's environment, and to establish root causes and remediation steps.

If Movius determines that Customer's data has been misappropriated, Movius will report such misappropriation to the Customer within 72 hours of making such determination, unless prohibited by law.

1.12.5. Data Privacy

Movius complies with applicable privacy and data protection laws and regulations with respect to collection, access, use, storage and disposal of Customer and End User data.

Movius uses physical, electronic, and administrative safeguards, consistent with applicable Personally Identifiable Information (PII) laws, that are designed to protect Personal Information from loss, misuse and unauthorized access, disclosure, alteration and destruction. In addition, we use standard security protocols and mechanisms to exchange the transmission of sensitive data.

Movius Cloud Services do not use, collect, access or store End User Payment Card Information (PCI).

In the Movius Cloud Services, data of different Customers and their End Users is kept logically isolated. End Users or Customers have no access, visibility, or modification abilities for data of other Customers.

1.13. Regulatory Compliance

Movius operates under Policies which are aligned with the ISO/IEC 27002 Code of Practice for information security controls, from which a comprehensive set of controls are selected, as described by ISO/IEC 27001. The Information Security Management System Family of Standards (ISO/IEC 270xx) are published by ISO (the International Organization for Standardization) and the IEC (the International Electrotechnical Commission), and are a comprehensive reference for information security management, data protection and risk management for organizations of all types and sizes. Movius participates in yearly assessments of its policies security controls which are certified by external certification bodies. Movius maintains certifications and compliance under ISO 27001, ISO 9001, SOC 2 Type 2, HIPAA Type 1, and GDPR.

Movius Cloud facilities, powered by IBM SoftLayer are compliant under ISO 27001; ISO 27017; ISO 27018, SOC 2 Type 2, and PCI Compliance.

2. Movius Cloud System Resiliency Policy

2.1. Movius Cloud Services High Availability Strategy

For business continuity in the event of an incident affecting Movius Cloud Services, Movius deploys the services on resilient computing infrastructure. Movius' production data centers have component and power redundancy with backup generators in place to help maintain availability of data center resources in the event of crisis as described below.

2.2. Redundant Power

The infrastructure design includes redundant power feeds to the data center and redundant power distribution for the data center and to the data center racks. Data center cooling components (chillers, towers, pumps, and computer room air conditioning units) include redundancy. The emergency standby power includes redundant battery backup with generator fuel stored onsite and contracts in place for refueling.

2.3. Redundant Network Infrastructure

Network designs include redundant circuits from carriers, firewall pairs, switch pairs, and load balancer pairs.

2.4. Redundant Media Servers

Any Media Servers that provide data, Web or IP telephony services as part of applications deployed by Movius in the Movius Cloud Services architecture are deployed in groups of N+1 configurations so that sufficient capacity remains available in the event of the non-availability of any component within that group of Media Servers.

2.5. Redundant Database Servers

Databases are configured to distribute workload across multiple physical servers. High availability is achieved through clustering and replication.

2.6. Redundant Storage

All Movius Cloud services data resides in redundant storage configurations with protection from individual disk or array failure.

2.7. Movius Cloud Services Backup Strategy

In support of Movius' Cloud Disaster Recovery practices (see Section 3 below), Movius periodically makes backups of production data for the sole use to minimize data loss in the event of a disaster. Database backups are stored at the primary site used to provide the Movius Cloud Services, as well as at an alternate location for redundancy purposes. A backup is retained online and/or offline for a period of at least 14 days after the date that the backup is made.

3. Movius Cloud Disaster Recovery Policy

3.1. Scope

This Policy applies only to production environments. The activities described in this Policy do not apply to a Customer's own disaster recovery, business continuity or backup plans or activities.

Disaster Recovery services are intended to provide service restoration capability in the case of a major disaster, as declared by Movius, that leads to loss of a data center and corresponding device unavailability. A major disaster would be any natural or man-made occurrence that incapacitates a physical cloud facility for days, weeks, or months. A short list of examples would be hurricanes, tornadoes, earthquakes, fires, riot-related damage, etc. Although these examples are events that would lead to long term service outages at a particular facility, Movius may, at its discretion, implement its disaster recovery plan for outages of a given facility that may only last for a relatively short period of time.

3.2. System Resiliency

Movius maintains a redundant and resilient infrastructure designed to maintain high levels of availability and to recover services in the event of a significant disaster or disruption. Movius designs its cloud services using principles of redundancy and fault-tolerance with a goal of fault-tolerance of a single node hardware failure. The Movius Cloud includes redundant capabilities such as power sources, cooling systems, telecommunications services, networking, application domains, data storage, physical and virtual servers, and databases. Movius will commence the disaster recovery plan under this Policy upon its declaration of a disaster and will target to recover the production data and use reasonable efforts to re-establish the production environment. Backups are for Movius' sole use in the event of a disaster.

3.3. Disaster Recovery

Movius provides for the recovery and reconstitution of its production Cloud Services to the most recent available state following a disaster.

Disaster recovery operations apply to the physical loss of infrastructure at Movius facilities. Movius reserves the right to determine when to activate the Disaster Recovery Plan. During the execution of the Disaster Recovery Plan, Movius provides regular status updates to Customers.

4. Movius Cloud Service Level Objective Policy

4.1. Service Availability Provisions

Movius works to meet the Target Service Availability Level in accordance with the terms set forth in this Policy.

4.2. Target System Availability

Movius works to meet a Target System Availability Level of 99.5% of the production service, for the measurement period of one calendar month, commencing at Movius' activation of the production environment.

4.3. Measurement of Availability

Following the end of each calendar month of the Services Period under an ordering document, Movius measures the "System Availability Level" over the immediately preceding month. Movius measures the System Availability Level by dividing the difference between the total number of minutes in the monthly measurement period and any Unplanned Downtime by the total number of minutes in the measurement period and multiplying the result by 100 to reach a percent figure.

4.4. Monitoring

Movius uses a variety of software tools to monitor (i) the availability and performance of Customer's production services environment and (ii) the operation of infrastructure and network components.

Movius monitors the service infrastructure, and currently generates alerts for CPU, memory, storage, database, network components, and transactions. Movius Operations staff attend to any automated warnings and alerts associated with deviations of the environment from Movius defined monitoring thresholds and follow standard operating procedures to investigate and resolve underlying issues.

4.5. Automated Workloads

Customers may not use nor authorize the use of data scraping technologies to collect data available in the Movius Cloud Service web portal or via web service requests without the express, written permission of Movius. Customers may not perform load testing or load analysis without express, written consent from Movius.

5. Movius Cloud Change Management Policy

5.1. Movius Cloud Change Management and Maintenance

Movius performs changes to cloud hardware infrastructure, operating software and supporting application software to maintain operational stability, availability, security, performance, and currency of the Movius Service. Movius follows formal change management procedures to provide the necessary review, testing, and approval of changes prior to application in the Customer's environment. The Movius Cloud Service architecture is structured to allow for maintenance and upgrades without affecting service availability. Maintenance is usually accomplished during low traffic periods so that sufficient capacity remains available during the maintenance. Customer impacting maintenance will be done with at least 2 weeks' notice provided to Customers.

5.1.1. Emergency Maintenance

Movius may periodically be required to execute emergency maintenance in order to protect the security, performance, availability, or stability of the production environment. Emergency maintenance may include program patching and/or core system maintenance as required. Movius works to minimize the use of emergency maintenance and will work to provide 24 hours prior notice as of any emergency maintenance requiring a service interruption.

5.1.2. Testing

All patches and upgrades are applied to pre-production environments before being installed in production environments.

6. Movius Cloud Support Policy

6.1. Support Terms

The support described in this Cloud Support Policy applies only for Movius Cloud Services. More specific details around support systems and processes are provided under the ordering document. Movius support is included with subscriptions to Movius Cloud Services.

Support becomes available upon the service start date and ends upon the expiration or termination of the Cloud Services under such ordering document (the "support period"). Movius is not obligated to provide support beyond the end of the support period.

7. Movius Cloud Suspension and Termination Policy

7.1. Termination of Movius Cloud Services

Upon termination or expiration of subscribed services, Movius will delete or otherwise render inaccessible any accounts or data stored in the Movius Cloud Service.

Data shall be retained subject to legal and regulatory requirements.

As part of the service termination process, Movius makes secured protocols available by which designated Customer users can transfer Customer data from the service.

7.2. Suspension Due to Violation

If Movius detects or is otherwise informed of violation of the Movius Cloud Services terms and conditions or acceptable use policies, Movius may (after investigation) take actions not limited to suspension of End User(s) accounts, suspension of Customer administrator(s) privileges, and suspension of Customer’s Movius Cloud Services.

Movius will use reasonable efforts to restore Customer's services promptly after Movius determines, in its reasonable discretion, that the issues have been resolved or the situation has been cured.

Revisions

Revision	Date	Author	Reason for Change
v.01	August 2017	Bill Pettit	Creation
v.01.1	March 2022	Melanie Allen	Apply new template (no content revision)