Technical and Organizational Measures (TOMs)
MK.IO

The document outlines the technical and organizational measures (TOMs) applicable to MediaKind's MK.IO service offerings (excludes MK.IO components supplied to MediaKind by third parties). If requested, MediaKind can provide evidence of these measures through current attestations, reports, or extracts from independent bodies.

This document applies to the configuration of the MK.IO Control Plane by Customers, as well as the encoding, distribution (including packaging, encryption, and streaming) and storage of Content via MK.IO services.

Definitions

Customer – A customer of MediaKind that has subscribed to MK.IO services.

Control Plane – The web User Interface (UI) and Application Programming Interface (API) made available by MediaKind, and which is used by the Customer to configure MK.IO.

Data Plane – The software and instances thereof responsible for the encoding and/or distribution (as applicable) of Content. Data Plane software is configured via, but operates independently from, the Control Plane.

Configuration Data – Configuration and user account data stored in the MK.IO control plane for the purpose of configuring MK.IO.

Content –any multimedia file (whether text, graphics, video, images, audio or any other media, data, information or material and including associated metadata) that a Customer encodes, distributes and/or stores using MK.IO.

Encryption Credentials – MK.IO internal encryption credentials used to provide AES and Enterprise DRM capability to Customers.

End User – Parties consuming the Content which has been encoded, distributed and/or stored using MK.IO.

Roles

Customer is responsible for Content and for determining what Content is encoded, distributed and/or stored using MK.IO. Where Content contains personal data, Customer is either the controller (or processor, where applicable) of such personal data, and MediaKind is a processor (or sub-processer, where applicable). Customer determines what personal data is embedded within the Content, and MediaKind will only process such personal data in accordance with the terms of the relevant Data Processing Agreement or otherwise upon Customer's instructions (such as instructions stored as Configuration Data).

Security Policies

MediaKind manages its IT and security governance in a manner designed to comply with industry standards (such as ISO 27001 and SOC2 Type II) and will enforce its IT and security policies that are obligatory for all employees, contractors, and relevant sub-processors. These policies will undergo periodic review and amendments as necessary to ensure business continuity.

All MediaKind staff will participate in annual business ethics, security and data privacy training, certifying their adherence to MediaKind's code of business ethics, and security and data privacy policies each year.

Security Management

MediaKind will maintain an incident response plan and adhere to its documented incident response policies, including prompt data and/or security breach notification to MK.IO Customers. This notification will occur without undue delay when a breach is known or reasonably suspected to affect Configuration Data, Content, or Encryption Credentials.

Risk Management

MediaKind will periodically evaluate the risks associated with the encoding and distribution of Content and the storage of Configuration Data in MK.IO and will develop an action plan to mitigate any identified risks. MK.IO will also periodically perform risk assessments to identify possible avenues for breaches of the Control Plane, Content exfiltration, or Encryption Credentials, as well as to ensure continuity of service.

Physical Security

MK.IO will host its product infrastructure with leading cloud providers, including Microsoft Azure, Amazon Web Services (AWS), and Google Cloud Platform (GCP).

MK.IO product infrastructure will be distributed across data centers in the United States and other regions as necessary. We leverage the audited security and compliance programs of these cloud providers to ensure the effectiveness of their physical, environmental, and infrastructure security controls. These providers guarantee high service availability, ensuring redundancy for all power, network, and HVAC services. The business continuity and disaster recovery plans for the services we use will be independently validated as part of their SOC 2 Type 2 reports and ISO 27001 certifications, among others.

Data Portability/Erasure

Data portability and erasure is supported by built in functions provided by the cloud infrastructure providers.

Data Minimization

Based on privacy by design principles MediaKind's services are developed and designed in compliance with applicable privacy regulations to ensure that only the scope of personal data required to enable service functionality is collected and processed, e.g. for support services, only basic contact data required to facilitate the provision of support is collected. In most instances, the amount of, and relevance of, personal data processed in connection with use of MK.IO services is determined or directed by the Customer.

Data Anonymization (Content)

MK.IO services that encode Content do so based on encoding configurations set by the Customer using an unstructured binary file, which means that personal data is in effect anonymized when in MediaKind's control. In these circumstances, MediaKind has no control over and no visibility into the specific data elements of personal data that may be embedded within Content.

Some MK.IO services (e.g. transcript or subtitling services, if available) may, if the Customer selects those services within the encoding configurations, mean that personal data embedded within Content may no longer be anonymized and will be visible to MediaKind during the encoding process (noting most if not all of the process is conducted automatically without manual intervention by us, and takes place within seconds). Visibility of personal data embedded within Content is therefore determined by the Customer.

User Access Management

MediaKind will maintain proper controls for requesting, approving, granting, modifying, and revoking user access to systems and applications containing Configuration Data.

Access to MK.IO for MediaKind staff is authorized using multi-factor authentication, and is limited and managed using role-based access controls. Only employees and authorized contractors with a clear business need will be granted access to Configuration Data stored in MK.IO. All access requests will be approved based on individual role-based access and reviewed on a regular basis for continuing business needs.

Development and Release Management (Controls and Validation)

MediaKind will implement strict engineering governance, code review, and release controls for MK.IO software. Every code change will undergo thorough review by designated repository owners to ensure adherence to our coding standards and security practices. Approved code will be automatically submitted to our continuous integration (CI) environment for packaging and testing.

Newly developed code will first be deployed to a dedicated and separate QA environment. Network-level segmentation will prevent unauthorized access between QA and production environments.

MK.IO release packages and software codebases will be periodically scanned to identify potential security issues and if any are found we will develop an action plan to promptly mitigate any identified issues.

Business Continuity and Disaster Recovery

System Backups

MK.IO systems containing Configuration Data will be backed up at regular intervals each day (intervals may vary, but backups will normally take place at least 3 times/day). Backups are normally maintained for seven days, ensuring that restoration can be easily performed. All backups will be encrypted at rest to ensure their security. Backups will be stored in multiple regions to enhance data availability and resilience. Backups will be continuously monitored for successful execution, and alerts will be generated in the event of any exceptions. Any failure alerts will be escalated, investigated, and resolved promptly. Regular testing of the backup restoration process will be performed to ensure that the procedure is effective and reliable.

Utilizing public cloud services for hosting, backup, and recovery eliminates the need for physical infrastructure or storage media for MK.IO backups. We will not produce or use hard copy media (e.g., paper, punch cards, tape) as part of our service delivery.

Customers will not have access to the product infrastructure to initiate a failover event. Disaster recovery and resiliency operations will be managed exclusively by MediaKind's product engineering teams, ensuring a robust and reliable backup restoration process.

Business Continuity and Recovery Process

MediaKind will maintain and regularly update its comprehensive business continuity and disaster recovery plans.

For example, in the event of a Control Plane disaster, MK.IO Data Plane sites are designed to remain operational to try and minimize the impact on service delivery. Our commitment to resiliency is focused on maintaining reliable and robust Content delivery even during unexpected events.

Customer Responsibilities

MediaKind expects Customers to be responsible for managing authorized users of their MK.IO subscription and for ensuring their compliance with applicable terms of use. Where relevant, MediaKind recommends that Customers utilize a robust role-based access control (RBAC) system.

If Customers are responsible for Content storage (e.g. in their cloud tenant), (a) Customers must provide valid storage access credentials through which MK.IO can retrieve Content for encoding and distribution, and (b) Customers will be responsible for selecting the environment for hosting and streaming their data, ensuring it meets their requirements. Customers must decide whether to enable Digital Rights Management (DRM) technologies to prevent unauthorized playback and duplication of their Content, and are accountable for the publication and withdrawal of Content URLs.

Customers are required to comply with all applicable access control measures published by MediaKind, and to report any security incidents that they become aware of, to MediaKind without undue delay by sending an email to security@mediakind.com.

Customers are responsible for maintaining their own business continuity plan (which should at their discretion include provisions regarding backups for Content).

Changes to These TOMs

As part of MediaKind's ongoing security evaluations, these TOMs may be updated from time to time.