RealtimeBoard, Inc. dba Miro

System and Organization Controls Report (SOC 3)

Independent Report of the Controls to meet the criteria for the Security, Availability, and Confidentiality categories for the period of January 1, 2020 through December 31, 2020.

KirkpatrickPrice

4235 Hillsboro Pike
Suite 300
Nashville, TN 37215

TABLE OF CONTENTS

ASSERTION OF REALTIMEBOARD, INC. DBA MIRO MANAGEMENT

ASSERTION OF REALTIMEBOARD, INC. DBA MIRO MANAGEMENT

We are responsible for designing, implementing, operating, and maintaining effective controls within RealtimeBoard, Inc. dba Miro's online collaborative whiteboard platform system (system) throughout the period January 1, 2020, to December 31, 2020, to provide reasonable assurance that RealtimeBoard, Inc. dba Miro's (Miro's) service commitments and system requirements relevant to Security, Availability, and Confidentiality were achieved. Our description of the boundaries of the system is presented in section A and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period January 1, 2020, to December 31, 2020, to provide reasonable assurance that Miro's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*). Miro's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in section B.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period January 1, 2020, to December 31, 2020, to provide reasonable assurance that Miro's service commitments and system requirements were achieved based on the applicable trust services criteria.

INDEPENDENT SERVICE AUDITOR'S REPORT

Grisha Pavlotsky
VP Operations
RealtimeBoard, Inc. dba Miro
525 Brannan Street, Suite 100
San Francisco, CA 94107

Scope

We have examined RealtimeBoard, Inc. dba Miro's (Miro's) accompanying assertion titled "Assertion of RealtimeBoard, Inc. dba Miro Management" (assertion) that the controls within Miro's online collaborative whiteboard platform system (system) were effective throughout the period January 1, 2020, to December 31, 2020, to provide reasonable assurance that Miro's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Service Organization's Responsibilities

Miro is responsible for its service commitment and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Miro's service commitments and system requirements were achieved. Miro has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Miro is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that controls were not effective to achieve Miro's service commitments and system requirements based on the applicable trust services criteria

- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Miro's service commitments and system requirements based on the applicable trust services criteria

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within Miro's online collaborative whiteboard platform system were effective throughout the period January 1, 2020, to December 31, 2020, to provide reasonable assurance that Miro's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Joseph Kirkpatrick
CPA, CISSP, CGEIT, CISA, CRISC, QSA
4235 Hillsboro Pike, Suite 300
Nashville, TN 37215

February 15, 2021

REALTIMEBOARD, INC. DBA MIRO'S DESCRIPTION OF ITS ONLINE COLLABORATIVE WHITEBOARD PLATFORM SYSTEM

SECTION A:
REALTIMEBOARD, INC. DBA MIRO'S DESCRIPTION OF THE BOUNDARIES OF ITS ONLINE COLLABORATIVE WHITEBOARD PLATFORM SYSTEM

Services Provided

RealtimeBoard, Inc. dba Miro (Miro) provides online collaboration services delivered as a hosted solution, Miro.com, over the internet. The Miro (previously RealtimeBoard) web application is a software as a service (SaaS) solution accessible to customers through a self-service website. The web application is also expanded by Windows and MacOS desktop applications as well as iOS and Android mobile applications. Miro is an online collaborative whiteboard platform for visual team collaboration that enables remote team users to add pictures, mockups, drawings, videos, sticky notes, office documents, and Google Drive files on an endless canvas, discuss uploads with teammates, and leverage the real-time visual collaboration without emails.

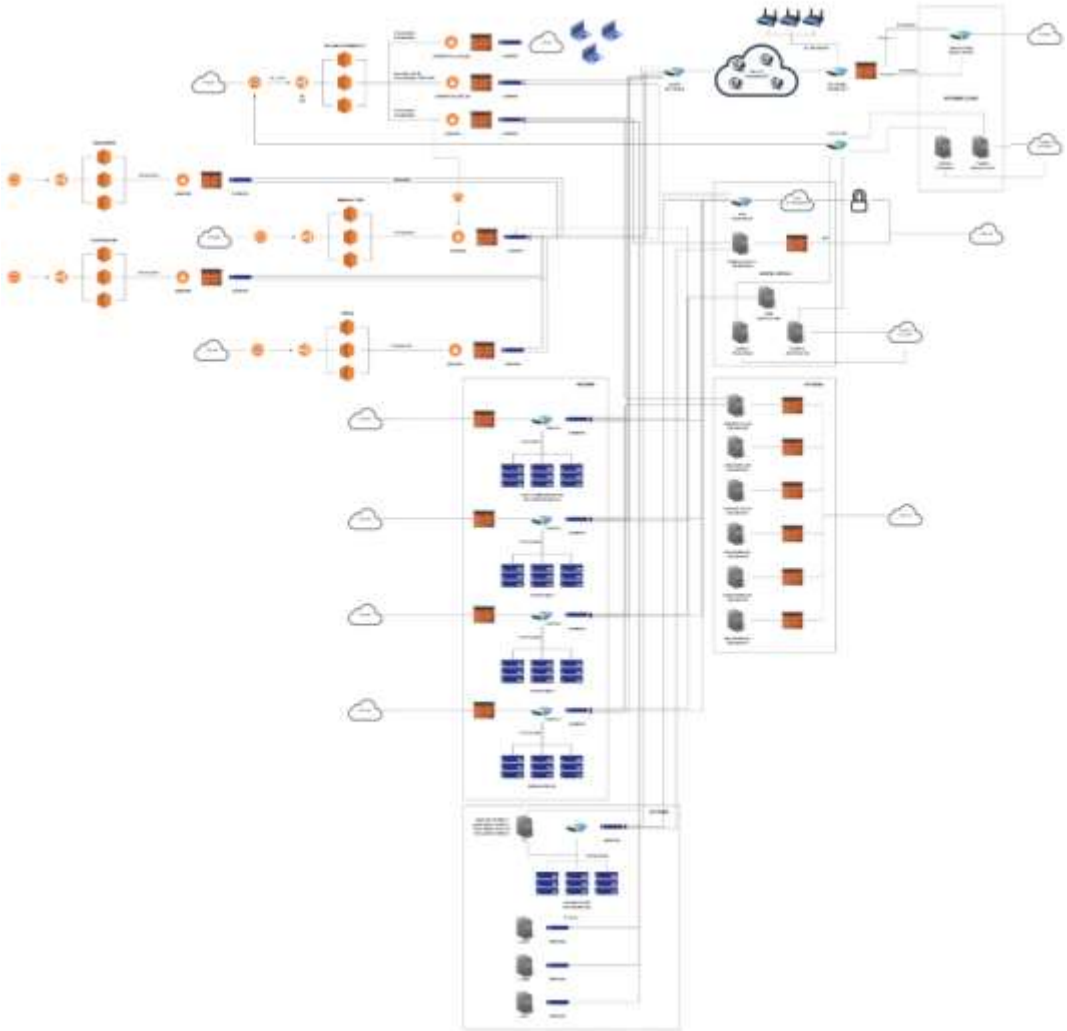
Miro's basic tools include the following:

- Whiteboarding Tools
  - Sticky Notes
  - Freehand Drawing
  - Shapes
  - Links
  - Texts
  - Presentation Mode
- Collaboration Tools
  - Real-time Collaborative Editing
  - Comments
  - Text Chat
  - Voice and Video Chat
  - Screensharing
  - Daily Notifications
- Sharing and Export Tools
  - Invite other people via email
  - Export boards as images and PDF files
  - Save to Google Drive
  - Post to Facebook
  - Embed into blogs and websites
- Visual Libraries
  - Prototyping
  - Tables and Charts
  - Business Canvases
  - Templates for Design Thinking
  - Project Management
  - Brainstorming and Creative Sessions

Multivitamin LLC, a subsidiary of RealtimeBoard, Inc., is located in Perm, Russia, and RealtimeBoard B.V., a wholly owned subsidiary, is located in Amsterdam, the Netherlands. The parent company, RealtimeBoard, Inc., has a registered address in San Francisco, California. The organization consist of over 200 employees. The Sales department is located in the office, and Marketing and Customer Success teams are located across the US and the Netherlands. Development personnel, as well as Administrative and some Marketing and general staff, are located in Perm, with some developers located in Amsterdam.

Infrastructure

The company documents its network design for purposes of showing how the office location communicates and shares resources from the Amazon Web Services (AWS) Cloud environment and how the office location is protected and segmented using Web Application Firewalls (WAFs). To outline the topology of its network, the organization maintains the network diagram below to illustrate its internal infrastructure. The network diagram is maintained by the DevOps team (IT Operations Management Team). The original diagram is stored on the Miro whiteboard and the last reviewed version is exported and stored in Confluence. The diagram is reviewed and updated at least annually.



All critical assets are identified in the diagram above as well as a systems inventory. The system inventory is maintained with automated tools. For the production and test environments, ansible scripts and AWS CLI are used. For the office's inventory, Jamf is used. The DevOps team is responsible for the production and test environments. Internal tools, as well as the IT infrastructure team, are responsible for the office's inventory. Inventories are updated once a change had been applied.

Miro utilizes Stripe.com as payment processor for services. Miro performs no processing of card information either directly or indirectly within the application or adjoined systems.

Software

The software inventory list is reviewed annually. Business-critical software is listed in the asset inventory tab of the corporate risk assessment with indication of its function. Licensing information is maintained separately by IT management with the access matrix and reporting is performed using Black Duck Licensing review software. The trust team, team leads, and asset owners are involved to validate assets and related information (e.g., description, business risk level). Licensing information is maintained by IT management. It is updated ad-hoc with involvement of the team leads and legal team. Licensing information of libraries in use inside the app is supervised by the security and legal teams. Black Duck Software Composition Analysis (SCA) scans the application source code and provides information about licenses in use.

People

The organization maintains a hierarchical structure with functional business units. The organization's hierarchy includes Executive and Middle Management with a functional structure of departments and teams. The organization maintains a full organizational chart that illustrates division, department, location, and direct reports for all employees. The People Team (Human Resources (HR) team) is responsible for maintaining the Miro organizational chart. The chart included below is generated from the HR system (Bamboo).

The board of directors meets quarterly and is involved in planning, monitoring, and managing financial resources. The board of directors selects officers and executives for overseeing operation and development.

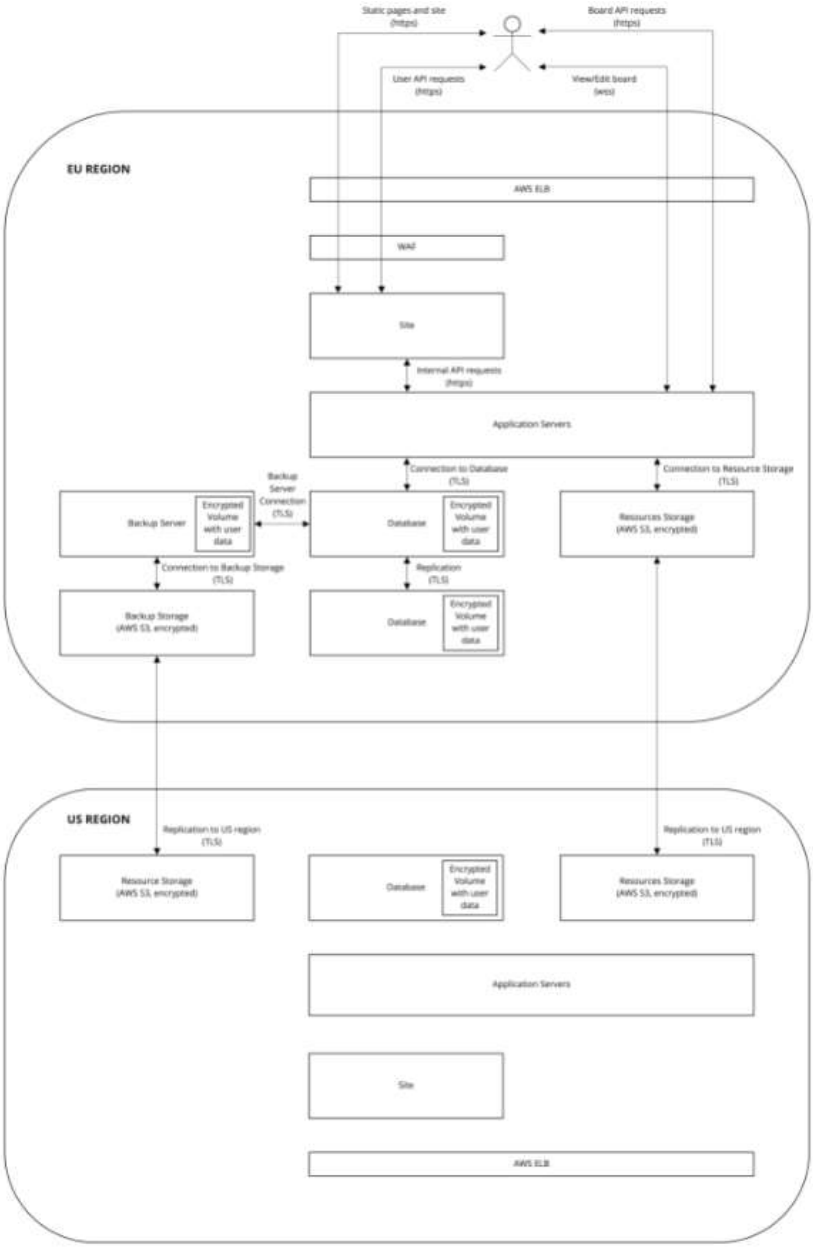
Data

Miro has an approved Data Protection Policy that describes all types of data involved into the entity's operation. Miro online whiteboarding solution generally processes and stores two types of data: profile data (name, second name and email of the user needed to distinguish the accounts) and information provided by users without inspection (uploaded to the app). All such information

is maintained as confidential and private to the owner user. This confidential and private information is available only to the user and user-defined members of its team (if applicable).

Each user entity has designated administrators who authorize team member access to information uploaded to Miro boards. User uploaded or created content is always owned by the customers. Access to production servers with databases storing customer data is restricted to a limited number of IT Operations Management personnel with credentials to access such data. All access to production environment is logged and monitored online. Miro employees cannot access user boards or see board content without customer approval.

Dataflows are documented in the diagram below to track how data enters, flows within the network, and is stored within the Miro environment.



The transmission, movement, and removal of information is restricted to authorized users and processes, and is protected during the same processes, enabling Miro to meet its commitments and requirements as they relate to security, availability, and confidentiality. The organization follows Open Web Application Security Project (OWASP) recommendations for data encryption in transit. This movement and transmission of data is protected through the following processes:

- The virtual private network (VPN) requires users to authenticate to the production environment via the Secure Shell (SSH) encryption protocol.
- Web servers use transport layer security (TLS) v1.2 encryption for web communication sessions.
- Programmed scripts are in place to perform scheduled backups of production data and systems at pre-defined intervals.
- Backup data is automatically replicated to an offsite storage facility in near real-time.
- Company laptops and workstations are required to be encrypted.
- Company laptops and workstations are configured to lock themselves automatically.

Processes and Procedures

Management has developed and communicated procedures to guide the provision of the organization's services. Changes to procedures are performed annually and authorized by management. These procedures cover the following key security life cycle areas:

- Data classification
- Categorization of information
- Assessment of the business impact resulting from proposed security approaches
- Selection, documentation, and implementation of security controls
- Performance of annual management self-assessments to assess security controls
- Authorization, changes to, and termination of information system access
- Monitoring security controls
- Management of access and roles
- Maintenance and support of the security system and necessary backup and offline storage
- Incident response
- Maintenance of restricted access to system configurations, user functionality, master passwords, powerful utilities, and security devices

SECTION B:
PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Regulatory Commitments

The organization is subject to General Data Protection Regulation (GDPR) and California Consumer Protection Act (CCPA) privacy regulations. The organization designs its security programs and business operations to maintain compliance with industry expectations and regulatory commitments. Miro's Data Processing Addendum outlines its commitments to comply with GDPR and CCPA. The organization's Master Service Agreement (MSA) notes the organization provides a platform for clients to provide data but does not process personally identifiable information (PII), PHI, PCI, or other restricted. Regulatory responsibility is passed onto clients for data hosted in the Miro environment.

Contractual Commitments

The organization uses Master Cloud Agreements (MCAs) and public-facing documents to define agreed upon services, terms, and conditions with its clients. Service level agreements (SLAs) are included within MCAs. The only SLA Miro offers to its Enterprise Customers is the customer support response SLA. This option can be chosen with an additional fee.

System Design

Miro designs its online collaborative whiteboard platform system to meet its regulatory and contractual commitments. These commitments are based on the services that Miro provides to its clients, the laws and regulations that govern the provision of those services, and the financial, operational, and compliance requirements that Miro has established for its services. Miro establishes operational requirements in its system design that support the achievement of its regulatory and contractual commitments. These requirements are communicated in Miro's system policies and procedures, system design documentation, and contracts with clients.