miro

FORMERLY REALTIMEBOARD

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, 2019 through December 31, 2019.

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, 2019, to December 31, 2019, to provide reasonable assurance that Realtimeboard Inc. dba 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, 2019, to December 31, 2019, to provide reasonable assurance that Realtimeboard Inc. dba 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*). Realtimeboard Inc. dba 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, 2019, to December 31, 2019, to provide reasonable assurance that Realtimeboard Inc. dba Miro's service commitments and system requirements were achieved based on the applicable trust services criteria.

INDEPENDENT SERVICE AUDITOR’S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

Board of Directors
Realtimeboard Inc. dba Miro
201 Spear Street, Suite 1100
San Francisco, CA 94105

Scope

We have examined Realtimeboard Inc. dba Miro's accompanying assertion titled "Assertion of Realtimeboard Inc. dba Miro Management" (assertion) that the controls within Realtimeboard Inc. dba Miro's Online Collaborative Whiteboard Platform System (system) were effective throughout the period January 1, 2019, to December 31, 2019, to provide reasonable assurance that Realtimeboard Inc. dba 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

Realtimeboard Inc. dba 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 Realtimeboard Inc. dba Miro's service commitments and system requirements were achieved. Realtimeboard Inc. dba Miro has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Realtimeboard Inc. dba 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 Realtimeboard Inc. dba 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 Realtimeboard Inc. dba 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 Realtimeboard Inc. dba Miro's Online Collaborative Whiteboard Platform system were effective throughout the period January 1, 2019, to December 31, 2019, to provide reasonable assurance that Realtimeboard Inc. dba 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

March 11, 2020

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 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 US 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

Miro's network infrastructure is designed enable the organization to provide its services. This infrastructure and its components are formally documented using a network diagram and system inventory. The network diagram is maintained by the IT Operations Management Team (DevOps), stored in Confluence, updated on an as needed basis, and reviewed at least annually. The network diagram is used to show the isolation of the organization's production environments, and the organization has monitoring systems running in Digital Ocean and deployment systems running in Hetzner.

The organization's production network is housed entirely within Amazon Web Services (AWS) and located in the eu-west-1 region, with the us-east-1 region used for disaster recovery backup. The perimeter of the production network is protected using virtual private clouds (VPCs) and security groups, with access into the environment for administrative functions secured using virtual private network (VPN) connections. External traffic is proxied into the environment using Elastic Load Balancers (ELBs), which are attached to specific VPCs. Amazon Elastic Cloud Compute (EC2) instances are used to provided compute resources, and database services are implemented using PostgreSQL with encrypted Elastic Block Store (EBS) volumes. Encrypted Amazon Simple Storage Service (S3) buckets are used for file storage, and security policies are applied to the S3 buckets to restrict access. Orchestration and configuration of the organization's AWS environment and resources are executed using HashiCorp, Terraform and Ansible.

To document system components, the organization maintains a formal systems inventory of its production systems, and application programming interfaces (APIs) of the cloud service providers in use are used to ensure that the inventory is up to date. All production systems are located within the cloud environment, and the system inventory documents the following:

- System name
- Internal team owner
- Description
- Model and version of primary software
- Function and use
- Location

Software

The organization manually maintains an inventory of software critical to the provision of services. The inventory includes the following applications:

- LastPass
- Stripe
- Zabbix
- OpsGenie
- Grafana
- Elasticsearch
- Atlassian Bamboo
- Atlassian Bitbucket
- Nexus
- Rollbar
- Slack
- Confluence
- Jira

People

The organization's board of directors consists of four members, including the organization's two founders and two members who are external from the company. The board is responsible for providing oversight functions for the organization.

The organization's structure consists of three levels of hierarchy: Executive Management (CEO, COO, VP Operations, CMO), Middle Management (Head of Departments), and Operational Staff (Team Leads, Staff, etc.).

- Executive Management: A team of individuals at the highest level of organizational management who have the day-to-day responsibilities of managing a company; they hold specific executive powers conferred onto them with and by authority of the board of directors and/or the shareholders.
- Middle Management: The intermediate management of the company, being subordinate to the Executive Management.
- InfoSec Committee: A team of individuals consisting of the Head of Development, Operations Team Lead, HR Managers, Application Security Manager, Legal Counsel, and any other individuals as required.
- CEO: The Chief Executive Officer is the highest-ranking corporate officer in charge of total management of the company.
- COO: The Chief Operating Officer is responsible for the daily operations of the business and routinely reports to the highest-ranking executive.
- VP Operations: The VP is responsible for the daily operations of the company.
- Application Security Manager: The Manager oversees the execution of the Information Security Policy and implementation of security controls through the SDLC and reports to the Head of Development.

The company is organized into functional areas consisting of departments and departmental units that are separated according to business functionality. Each department has a Head—a member of the Middle Management team that reports to CEO, VP Operations, or COO according to his/her job description or special regulation issued by CEO. Each unit has a Team Lead that reports to his/her Department Head according to his/her job description or special regulation issued by the CEO/COO. Information security functions are managed by a cross-departmental InfoSec Committee that reports to the organization's CEO. An organization chart is documented and maintained to illustrate the structure and reporting relationships in place within the company.

The following personnel were interviewed as part of the audit engagement:

- Operations Team Lead
- DevOps Team Lead
- People Operations Team Lead
- QA Team Lead/Application Security Manager

Data

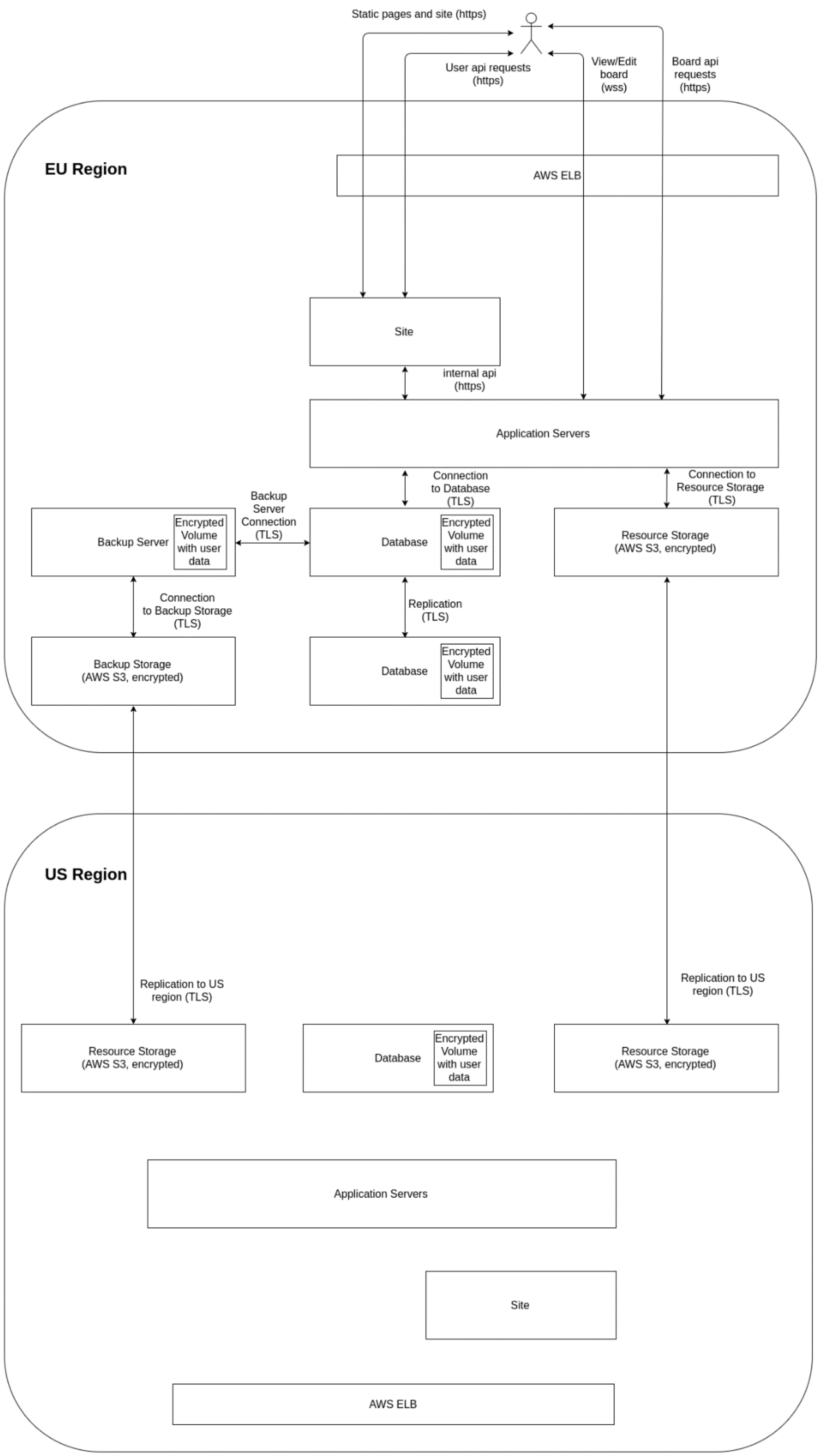
A data classification policy is documented by the organization to define the types of data handled and the handling requirements. The policy defines handling requirements for confidential information, company private data, and client private data to meet the organization's confidentiality requirements. Protection, destruction, and storage requirements to which the organization must adhere for confidential data are defined within the policy as well. Data provided by the users of the organization's application is considered confidential, and all organizational data is classified into the following categories:

- Unclassified public
- Proprietary
- Confidential
- Company private
- Client private
- Sensitive
- Trade secret

Systems that contain confidential information are classified as high-risk and are evaluated on an ongoing basis. Data retention requirements are defined through policy, and all personally identifiable information (PII) collected during the organization's service delivery process is retained according to the Privacy Policy. GDPR affects the organization's corporate retention policies, and data is backed up with a retention period of 180 days. A quarterly process is in place for identifying and securely deleting stored confidential data that exceeds defined retention requirements.

The organization secures all web traffic to the application through the use of TLS 1.2 protocols, and traffic sent to the HTTP protocol is automatically redirected to the HTTPS protocol. Open Web Application Security Project (OWASP) recommendations are followed in regard to data encryption in transit, and regular vulnerability scans and penetrations tests are performed to ensure appropriate encryption is used. VPN connections are utilized to secure remote access to the organization's network, and company laptops and workstations are required to have encryption enabled. Data at rest is encrypted using native AWS encryption abilities. EBS and S3 buckets use encrypted modes to protect the data contained.

A documented data flow diagram is maintained by the organization to illustrate the data inputs and outputs for the application. The diagram, below, is stored in Confluence and reviewed annually.


Static pages and site (https)
User api requests (https)
View/Edit board (wss)
Board api requests (https)
EU Region
AWS ELB
Site
internal api (https)
Application Servers
Connection to Database (TLS)
Connection to Resource Storage (TLS)
Backup Server Connection (TLS)
Backup Server
Encrypted Volume with user data
Database
Encrypted Volume with user data
Resource Storage (AWS S3, encrypted)
Connection to Backup Storage (TLS)
Replication (TLS)
Backup Storage (AWS S3, encrypted)
Database
Encrypted Volume with user data
US Region
Replication to US region (TLS)
Replication to US region (TLS)
Resource Storage (AWS S3, encrypted)
Database
Encrypted Volume with user data
Resource Storage (AWS S3, encrypted)
Application Servers
Site
AWS ELB

Processes and Procedures

Management has developed and communicated processes and procedures to employees to ensure the execution of policy documentation and critical business processes. Changes to these procedures are performed annually and are 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 the proposed security approaches
- Selection, documentation, and implementation of 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

SECTION B:
PRINCIPLE SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Regulatory Commitments

To meet its service commitments and system requirements, the organization is required to comply with jurisdiction privacy laws for personnel and enacts appropriate contractual amendments to ensure compliance with required jurisdictional privacy requirements. The organization's privacy policy communicates that the company complies with the California Civil Code Section 1798.83, the California Online Privacy Protection Act, and the General Data Protection Regulation (GDPR).

Contractual Commitments

The organization's terms of service govern the agreements between the organization and its customers in relation to the use of the Miro application. A service description is included that defines the scope of the applications and types of accounts, and payment terms are communicated. User responsibilities in relation to the use of the application and usage terms are detailed for the customer, and ownership and intellectual property rights are defined.

Master subscriptions agreements are used within the organization as well to communicate service terms and conditions and include license information, service descriptions, prohibited activities, required compliance with laws, and confidentiality and privacy requirements.

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.