Miro Security Policy

RealtimeBoard, Inc. dba Miro ("Miro") considers protection of Customer Content a top priority. As further described in this Miro Security Policy, Miro uses commercially reasonable organizational and technical measures designed to prevent unauthorized access, use, alteration or disclosure of Customer Content stored on systems under Miro's control. In order to protect our network from evolving threats and disruptions, ensuring effective security controls, Miro may modify this Security Policy, with notice to Customer, to reflect new features and updated practices, but any such modifications will not materially decrease Miro's security obligations during a Subscription Term.

This policy is issued under and forms part of the Master Cloud Agreement or other Miro agreement which references this policy, and any capitalized terms not defined herein shall have the meanings ascribed to them in such Miro agreement.

1. Customer Content Access and Management Controls. Miro implements formal procedures to limit its personnel's access to Customer Content as follows:

1.1. Requires unique user access authorization through secure logins and passwords, including multi-factor authentication for Cloud Hosting administrator access and individually assigned Secure Socket Shell (SSH) keys for external engineer access;
1.2. Limits the Customer Content accessible to Miro personnel on a "need to know basis";
1.3. Limits access to Miro's production environment by Miro's personnel on the basis of business need;
1.4. Prohibits Miro personnel from storing Customer Content on electronic portable storage devices, such as computer laptops, portable drives and other similar devices;
1.5. Logically separates each of Miro's users' data and maintains measures designed to prevent Customer Content from being exposed to or accessed by other users.

2. Data Encryption. Miro provides industry standard encryption for Customer Content as follows:

2.1. Implements encryption in transport and at rest;
2.2. Uses strong encryption methodologies to protect Customer Content, including AES 256-bit encryption for Customer Content stored in Miro's production environment;
2.3. Encrypts all Customer Content located in cloud storage while at rest; and
2.4. Implements full-disk encryption for hard-drives on all personnel individual workstations.

3. Network Security, Physical Security and Environmental Controls.

3.1. Miro implements properly configured and patched firewalls, network access controls and other technical measures designed to prevent unauthorized access to systems processing Customer Content;
3.2. Miro maintains effective controls to ensure that security patches for systems and applications used to provide the Service are properly assessed, tested and applied;
3.3. Miro monitors privileged access to applications that process Customer Content, including cloud services;
3.4. Remote access to Miro's environments is controlled with a virtual private network or other device ("VPN") or private lines, consistent with industry best practices. Two-factor authentication is required for all remote access;
3.5. Miro operates on Amazon Web Services ("AWS") and is protected by Amazon's security and environmental controls. Detailed information about AWS security is available at https://aws.amazon.com/security/, and http://aws.amazon.com/security/sharing-the-security-responsibility/. AWS ISO certification and SOC Reports are available at https://aws.amazon.com/compliance/iso-certified/, and https://aws.amazon.com/compliance/soc-faqs/, respectively; and
3.6. Customer Content hosted in AWS is AES-256 encrypted both in transit and at rest. AWS does not have access to unencrypted Customer Content.

4. Independent Security Assessments. Miro periodically assesses the security of its systems and the Service as follows:

4.1. Annual penetration testing of the Service is conducted by independent third-party security experts that includes black box automated and manual penetration testing of the infrastructure and application (including mobile versions). At Customer's request, Miro will provide to Customer a high-level summary of the most recent penetration test, subject to reasonable confidentiality protections;
4.2. Miro hires accredited third parties to perform audits and to attest to SOC 2, Type 2 and SOC 3 compliance standards annually; and
4.3. Monthly vulnerability scanning.

5. Incident Response. If Miro becomes aware of unauthorized access or disclosure of Customer Content under its control (an "Incident"), Miro will:

5.1. Take reasonable measures to mitigate the harmful effects of the Incident and prevent further unauthorized access or disclosure;
5.2. Upon confirmation of the Incident, notify the Customer's designated security contact by email within 72 hours. Notwithstanding the foregoing, Miro is not required to make such notice to the extent prohibited by Laws, and Miro may delay such notice as requested by law enforcement and/or in light of Miro's legitimate need to investigate or remediate the matter before providing notice; and
5.3. Each notice of an Incident will include:
    5.3.1 The extent to which Customer Content has been, or is reasonably believed to have been, used, accessed, acquired or disclosed during the Incident;

5.3.2 A description of what happened, including the date of the Incident and the date of discovery of the Incident, if known;
5.3.3 The scope of the Incident, to the extent known; and
5.3.4 A description of Miro's response to the Incident, including steps Miro has taken to mitigate any harm caused by the Incident.

6. Business Continuity Management.

6.1. Miro maintains a business continuity and disaster recovery plan in accordance with industry trends and standards; and
6.2. Miro maintains processes to ensure failover redundancy with its systems, networks and data storage.

7. Personnel Management.

7.1. Miro performs employment verification, including proof of identity validation, check of education records and employment track, and criminal background checks for new hires in positions requiring access to systems and applications storing Customer Content in accordance with applicable Law;
7.2. Miro provides training for its personnel who are involved in the processing of Customer Content to ensure they understand their obligations to not collect, process or use Customer Content without authorization and to keep Customer Content confidential, including following the termination of any role involving Customer Content;
7.3. Miro conducts routine and random monitoring of employee systems activity; and
7.4. Upon employee termination, whether voluntary or involuntary, Miro immediately disables all access to Miro systems, including Miro's physical facilities.