Vendor Information Security Schedule

Schedule Purpose. This Schedule lays out the minimum requirements for Provider's reasonable security and is appended to any agreement between the parties for goods or services. Compliance with this Schedule does not provide a safe harbor to liability in connection with the unauthorized disclosure of confidential information and Provider acknowledges that any security controls not currently contemplated here may be necessary for Provider to demonstrate a reasonable degree of care to prevent an unauthorized access or disclosure of confidential information.

1. Security Measures.

(a) **Security Program.** Provider's Security Program shall provide for regular assessment of the risks to the security of the Provider's, and/or any third party subprocessor's systems, applications, and services that are used to provide the services to Miro under the Agreement. Provider shall promptly correct any identified deficiencies in accordance with the recommendations of such assessments, predicated on the criticality of the issue.

(b) **Third Party Security Assessment.** Provider shall perform a competent and independent third-party (such as an AICPA or ISO-accredited auditor) assessment of its relevant security controls at least annually and shall provide a copy of the results of that assessment or evidence on controls or processes that have changed annually (at the conclusion of the audit or the anniversary of the execution of this Agreement, whichever is sooner) upon request. In addition, upon Miro's request, Provider shall provide Miro with a bridge letter, signed by a senior representative of Provider, confirming that processes and controls have not changed since the last audit cycle/last third-party assessment.

(c) **Disaster Recovery; Business Continuity.** Provider shall maintain, implement, and test effective business continuity procedures (including, without limitation, disaster recovery and crisis management procedures) consistent with industry standards and appropriate to the size, nature, and complexity of Provider's business.

(i) Provider shall utilize industry standard practices for data, services, and communications recoverability. Data and applications shall be replicated across multiple independent sites and alternate communication channels shall be available.

(ii) Provider shall validate and verify business continuity capabilities through realistic scenario testing.

(iii) Provider systems shall be device- and provider-independent in order to ensure portability and successful recovery of applications, backup, and/or restoration services, as applicable.

(d) **Security Program Updates.** Provider shall review and update its Security Program, at least annually, as well as when necessary to comply with changes in applicable laws and regulations pertaining to the security of Miro Data. Provider shall ensure its Security Program stays current with industry standard practices, taking into account new security standards, threats, and hazards.

2. **Administrative Security Measures.**

(a) **Security Incident Response and Reporting.** A "**Security Incident**" is the actual or suspected accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to Miro Data, transmitted, stored, or otherwise processed by Provider on behalf of Miro. In the event of a Security Incident, Provider shall:

(i) Notify Miro without undue delay, but in any regard, no later than twenty-four (24) hours after discovery.

ii) Without undue delay, perform such incident response activities as may be reasonably appropriate and in accordance with industry standards, including taking all such reasonable measures as may be deemed necessary in order to prevent or otherwise mitigate any such further Security Incident.

(iii) Upon request by Miro, promptly prepare and deliver to Miro a root cause report that describes in reasonable detail and to the extent known: (i) the nature and extent of the Security Incident; (ii) the Miro Data affected; (iii) supporting evidence, including system, network, and application logs related to the Security Incident, as may be provided in Provider's reasonable discretion, using commercially reasonable efforts to aid Miro in its own remediation and investigation efforts; (iv) investigative, corrective, and remedial actions completed, as well as planned actions and the anticipated dates that such actions will be completed; and (v) efforts taken to mitigate the risks of further Security Incidents.

(iv) In no event will Provider, unless otherwise required by applicable law, serve any notice of or otherwise publicize a Security Incident that affects or relates to Miro Data, without the prior written consent of Miro. The results of the investigation that are specific to Miro and/or Miro Data will be treated in a confidential manner.

(b) **Change Management.** Provider will employ an effective documented change management program with respect to the services.

(c) **Production Data Use.** No Miro Data will be transmitted, stored, or processed in a non-production environment. Production environments shall be logically or physically separate from all development and testing environments.

(d) **Background Checks and Training.** Provider is committed to hiring and retaining employees, contractors, Providers, and subcontractors with appropriate character, disposition, and honesty and represents and warrants that it shall: (i) perform position-appropriate employee background screening (to the extent permitted by applicable law); (ii) provide relevant data privacy and security training to its Personnel on no less than an annual basis; and (iii) require Personnel with access to Miro Data to abide by Provider's confidentiality and security obligations. Provider shall remain liable for the actions and inactions of such Personnel or approved subcontractors.

(e) **Asset Classification and Control.** Provider shall maintain current, accurate, and complete documentation on overall system, network, and application architecture, data flows, and security functionality for relevant applications that process or store Miro Data.

(f) **Product Security.** To the extent applicable, Provider's application security program is based on the Security Development Lifecycle (SDL) or an equivalent industry-standard framework designed to secure product code. Provider maintains a team of dedicated infrastructure security engineering Personnel responsible for maintaining industry standard infrastructure security controls, which include manual code review and validation, threat modeling, static code analysis, dynamic analysis, and system hardening, in order to ensure the operational security of the services.

(g) **Subcontractors.** Provider shall conduct appropriate due diligence on any subcontractors involved in performing the services or who have access to systems or applications that contain Miro Data. Provider shall include and enforce obligations regarding data security in all relevant contracts with parties that have access to or process Miro Data; such obligations shall be no less protective than the standards included in this Agreement.

(h) **Deletion and Return of Miro Data.** Upon request and at Miro's instruction, Provider shall return Miro Data to Miro and/or delete (and make irretrievable) Miro Data. Upon request, Provider will provide written confirmation to Miro that such return or destruction has been completed.

3. **Technical Security Measures.**

(a) **Physical Security.** Provider maintains physical security measures that control and restrict physical access to systems and servers that contain Miro Data, which include: i) data center monitoring by professional security staff, seven days a week and twenty-four hours a day; ii) cameras covering parking areas and secured data center entry points; iii) data center emergency and access control systems; and iv) infrastructure systems, which including environmentally appropriate protection against common natural and man-made disasters (as required by geography and location), fire suppression systems (including smoke detectors), cooling, power (including use of uninterruptible power supplies – UPS), raised floors, and comprehensive cable management. Two-factor access (e.g. badge and keypad) is required for highly sensitive areas, which include data centers. Additionally, all visitors who enter these areas must be logged and escorted by Provider Personnel who are authorized to access such areas. Access control logs shall be employed in order to maintain an audit trail of all access attempts. Provider shall limit physical access to production data centers to only authorized individuals. Access to an on-premise server room or third-party hosting facility shall also require the submission of a request through the relevant ticketing system and approval by the appropriate manager, as well as review and approval by appropriate Personnel. Provider management, on no less than a quarterly basis, reviews physical access logs to data centers and server rooms. Additionally, physical access privileges to data centers is removed promptly upon termination of any previously authorized personnel.

(b) **Physical Data.** Provider shall not maintain Miro Data in physical form unless required as part of providing and operating the services, by applicable law, and/or as authorized by Miro.

(c) **Security and Vulnerability Scanning and Patch Management.** Provider shall maintain a formal patch management program and, on at least a monthly basis, perform patch management activities on all relevant systems, devices, firmware, operating systems, applications, and other software that process Miro Data. Provider shall assess and scan for system-level, internal, and external host/network vulnerabilities, on no less than a monthly basis, as well as after any material change to such systems, and shall remediate relevant discovered vulnerabilities consistent with industry standards and in accordance with documented policies that prioritize remediation based on risk.

(d) **Application Security Tests and Assessments.** Provider shall, on at least an annual basis, perform a security assessment on relevant applications and systems that handle, maintain, or process Miro Data. The security assessments shall include, at a minimum, a service-level penetration test conducted by a reputable third-party, as well as additional tests and assessments for security vulnerabilities, as is deemed appropriate or identified by industry-recognized organizations (e.g., OWASP, CWE/SANS).

(e) **Network Security.** Provider will deploy appropriate network security and information transfer controls designed to ensure the protection of Miro Data, including firewalls, intrusion detection and prevention systems, proxy servers and secure file transfer technologies, or relevant equivalent technologies, in the operation of Provider's systems and facilities, in each case, consistent with industry standard. Traffic between Miro and Provider will be, where deemed necessary, protected, authenticated, and encrypted. Additionally, where appropriate, a distributed denial-of-service ("**DDoS**") prevention solution shall be utilized in order to protect against volumetric DDoS attacks; this service shall be tested on an annual basis.

(g) **Malicious Code Protection.** All workstations and relevant software and hosting environments must run anti-malware or end-point protection software, where possible and consistent with industry standards , that minimize any risk of disruption or impact on the performance of the service; such software shall test and scan for threat vulnerabilities, including but not limited to: trojan horses, back-doors, key-loggers, cross-site scripting ("**XSS**"), injection flaws (e.g. SQL injection attack vectors), malicious file execution, insecure direct object references, cross-site request forgery, information leakage and improper error handling, broken authentication and session management, insecure cryptographic storage, insecure communications, and failure to restrict URL access.

(h) **Security Event Logs.** Provider shall ensure that access to the environments, services, systems and applications used to host Miro Data and/or provide the services to Miro are logged for compliance, audit, and incident investigation purposes. Such security logs shall be preserved for a minimum of ninety (90) days.

(i) **Access and Authorization.** Provider shall ensure that appropriate access controls are in place, at all times, and will employ industry standard physical, administrative, and technological access control mechanisms designed to prevent unauthorized access to Provider's facilities and systems that store or enable access to Miro Data. Provider will, taking into account the "principle of least privilege," limit access to Miro Data to only those Personnel who have a need to know the information to perform and/or operate the services. Such mechanisms will have the capability of detecting, logging, and reporting access to the system or network or attempts to breach the security of the facility, compartment, system, network, application, and/or data.

(i) Provider personnel must, where technically feasible, have an individual account that authenticates the individual's access to Miro Data. Provider does not allow sharing of accounts.

(ii) Provider will utilize two-factor authentication for network access/VPN and, to the extent technically feasible, for internal tools that access Miro Data.

(iii) Provider will maintain an industry-standard (e.g. in line with an applicable third-party certification, such as SOC2, ISO 27001: 2013, etc.) process to review access controls, on at least a quarterly basis , for all personnel who have access to applications or systems that maintain or process Miro Data. To the extent Provider utilizes any third-party hosted systems to store Miro Data, it shall utilize equivalent review and validation processes to those specified herein.

iv) Provider will promptly revoke a person's access to Miro Data, once such person no longer requires access to the system(s) or application(s).

(v) Provider will implement and maintain a complex password policy that is consistent with recognized industry standards, including but not limited to, ensuring that relevant passwords have a sufficient length and are not easy to guess (e.g., consisting of letters and numbers or letters and special characters or numbers and special characters). Provider's password policy shall require that such passwords are changed at regular intervals and are not stored in clear text or otherwise written on paper.