Information Security Requirements

These Information Security Requirements (this "**Exhibit**") are incorporated by reference into the Master Subscription Agreement or under any services agreement or similar agreement (collectively, the "Agreement") between the Customer and Jasper. This Exhibit establishes the operational and technical security measures that are in place for the protection of Customer Property in the Services. Capitalized terms used but not defined here are defined in the Agreement.

1. Information Security Program. Jasper maintains and will use commercially reasonable efforts to continually make improvements to a documented information security program, designed in accordance with industry standards and best practices.

1.1. Internal Controls. Jasper implements operational and technical controls that meet or exceed applicable and current industry standards to protect Customer Property from unauthorized access, modification, use, and deletion. Jasper performs an internal audit of the operating effectiveness of its internal security controls at least annually.

1.2. Policies. Jasper's Director of Security reviews and approves the Company's information security policies at least annually.

2. Technical Controls

2.1. Encryption of Customer Data. Jasper encrypts Customer Property at rest and in transit over untrusted networks using current industry standards.

2.1.1. Key Management. Jasper's encryption key management program includes regular rotation of encryption keys. Jasper logically separates encryption keys from Customer Data.

2.2. Access Control. Access to Customer Property is granted as needed based on job role and responsibilities, and valid business needs. All production and administrative access requires a unique user ID and password, as well as multi-factor authentication.

2.2.1. Revocation. In the event of employee termination, Jasper revokes access within two business days.

2.2.2. User Access Reviews. Jasper performs user access reviews at least semi-annually, revoking inactive and no longer needed accounts.

2.3. Device Management. Jasper personnel use Jasper-provisioned laptops that are centrally managed. Employee laptops are configured with controls that include but are not limited to, disk encryption, password protection, and inactivity lockout.

2.4. Environment Segregation. Jasper logically separates the production environment from the development and testing environments. The production environment is both logically and physically separate from Jasper's corporate offices and networks.

2.5. Network Security. Jasper implements a multi-layered network infrastructure that restricts unauthorized traffic, provides continuous monitoring, and detects and limits the impact of attacks. Jasper uses firewall or security groups technology with deny-all default policies, in addition to intrusion detection and prevention systems.

2.5.1. Hardening. Jasper configures and deploys information systems, network devices, and applications using a secure configuration baseline. Hardening includes, but is not limited to, changing default passwords, removing unnecessary software, disabling or removing unnecessary services, and regular patching.

2.5.2. WAF. Jasper uses a web application firewall designed to protect against common web application vulnerabilities, such as cross-site scripting, denial of service (DoS), and injection attacks.

2.6. Logging and Monitoring. Monitoring services, such as intrusion detection tools, are utilized to log activities and changes within the production environment. Logs are continually monitored and analyzed for anomalies. Logs are securely stored for at least one year.

2.7. Vulnerability Management. Jasper performs vulnerability scans of the systems used to provide the Services at least weekly. Identified vulnerabilities are patched in accordance with Jasper's vulnerability management policy.

2.7.1. Penetration Testing. Jasper conducts annual independent penetration testing of the applications and infrastructure used to

support the Services. Upon written request, Jasper will provide an executive summary report of the most recent penetration test report to Customer.

2.8. SDLC. Jasper implements technical and operational controls to ensure secure code development. Such measures include, but are not limited to, mandatory peer review and approval, dynamic application security testing (DAST), and dependency management.

2.8.1. Secure Code Training. Jasper developers are required to complete scoped, secure code training upon hire and annually thereafter.

3. Operational Controls

3.1. Personnel Security. Jasper performs background screening on all new hires as part of the hiring process, to the extent permitted by applicable law. Jasper personnel are required to sign confidentiality agreements upon hire.

3.2. Security Training. Jasper personnel are required to complete security awareness training upon hire and annually thereafter. Training curriculum can include but is not limited to, phishing awareness, incident reporting procedures, device security, and remote work best practices. In order to complete training, personnel must also sign their acknowledgment of Jasper's information security policies.

3.3. Third-Party Risk Management. Jasper maintains a third-party risk management program designed to ensure that Subprocessors maintain security measures no less rigorous than Jasper's obligations set forth in this Exhibit. Jasper performs annual assessments of Subprocessors, reviewing independent audit reports, penetration test reports, and other relevant security documentation.

3.4. Physical Security

3.4.1. Data Centers. To ensure Jasper's cloud hosting provider ("Cloud Provider") has appropriate physical and environmental controls for its data centers hosting Jasper's cloud environment, Jasper validates the operating effectiveness of such controls by reviewing the Cloud Provider's independent audit reports and certifications annually.

3.4.2. Corporate Offices. Though Customer Property is not hosted at Jasper's corporate offices, Jasper's physical controls for its corporate offices include, but are not limited to, the following:

3.4.2.1 Badge access is required for all personnel.

3.4.2.2 Visitors are required to sign in.

3.4.2.3. Use of CCTV at building ingress/egress points

3.5. Incident Response. Jasper maintains a documented incident response program for responding to suspected or known security incidents. Jasper tests its incident response plan at least annually.

3.5.1 Breach Notification. In the event of the unauthorized or unlawful destruction, loss, alteration, disclosure of, or access to Customer Property ("Security Breach"), Jasper shall notify Customer within 48 hours following confirmation of the event. Upon confirmation of a Security Breach, Jasper shall promptly contain the incident to prevent further harm; begin a thorough investigation, including performing root cause analysis; and take reasonable actions to mitigate recurrence. Following notification, Jasper shall continue to provide Customer timely information about the Security Breach to the extent known to Jasper at that time, which may include, but is not limited to:

3.5.1.1. The nature and consequences of the Security Breach.

3.5.1.2. The measures taken or proposed by Jasper to mitigate or contain the Security Breach.

3.5.1.3. The status of Jasper's investigation.

3.5.1.4. The categories and approximate number of data records concerned.

3.6. Business Continuity. Jasper maintains a business continuity and disaster recovery plan covering the Services to ensure the ability to recover timely in the event of a disruption.

3.6.1. Disaster Recovery Testing. Jasper tests its disaster recovery plan at least annually. Upon written request, and no more than once annually, Jasper shall provide a copy of its disaster recovery test report to Customer.

3.6.2. Backups. Jasper performs backups of Customer Property daily, segregating such backups from the production environment. Backups are stored securely, and encrypted at rest.

4. Customer Audit Rights

4.1. Due Diligence Requests. Upon written request and no more than once annually, Customer may request access to documentation evidencing Jasper's compliance with its security obligations under this Exhibit.

4.2. Audit Rights. No more than once annually, upon Customer's written request, to confirm compliance with this Agreement, as well as any applicable laws and industry standards, Jasper shall promptly and accurately complete a written information security questionnaire provided by Customer, or a third party on Customer's behalf, regarding Jasper's business practices and information technology environment in relation to all Customer Property being handled and/or services being provided by Jasper to Customer pursuant to this Agreement. Jasper shall fully cooperate with such inquiries. Customer shall treat the information provided by Jasper in the security questionnaire as Jasper's Confidential Information.

4.3. Risk Remediation. In the event that Customer identifies any significant (high and very high severity) findings during an audit or due diligence review, Jasper will work in good faith to negotiate a mutually acceptable mitigation plan.

4.4. Penetration Testing. Customer may not perform penetration testing of the Services or any testing that could reasonably result in application downtime (e.g., stress-testing).

5. Customer Security Responsibilities

5.1. Access Management. Customer is responsible for managing user access for their workspace. Customer is responsible for managing the password complexity requirements for user access, where applicable.

5.2. Acceptable Use. Customer may not upload data that requires a certification or authorization that Jasper does not maintain, such as protected health information or cardholder data. Customer is responsible for the appropriate use of the Services.