SECURITY EXHIBIT

MotionCX Information Security Program Overview

MotionCX maintains a comprehensive, documented information security program (the “Program”) designed to appropriately protect the confidentiality, integrity, and availability of information technology systems and data, including without limitation Customer Data, and to comply with applicable legal requirements. The Program comprises administrative, technical, and physical safeguards against reasonably foreseeable threats or hazards to Customer Data, including without limitation unauthorized and/or accidental access or damage to, or use, disclosure, alteration or destruction of Customer Data.

Without limitation, Program features include:

- **Documented Information Security Policies:**
  - MotionCX maintains documented information security policies that are mandatory for all employees and independent contractors with access to information technology systems.
  - These policies are reviewed on at least an annual basis (more frequently if warranted by relevant changes in the I.T. environment, operations, risk assessment, etc.) and updated as appropriate.
- **Incident Response Planning:**
  - In the event of a security incident, MotionCX is prepared to respond according to its documented plans, which are tested and reviewed regularly and updated as warranted.
  - These plans include, without limitation, roles and responsibilities for the incident response team, assessment of risk and identification of potentially impacted individuals and entities, containment and eradication, reporting, notifications and disclosures, preservation and recordkeeping, remediation and recovery, root cause analysis and incorporating lessons learned.
  - In the event Customer Data is impacted by a security incident, MotionCX will notify the affected customer, investigate, and comply with applicable legal requirements regarding notification.
- **Business Continuity and Disaster Recovery Planning:**
  - MotionCX systems are separately assessed for business-continuity and disaster-recovery requirements. These systems have, to the extent warranted by risk assessment, separately defined, documented, maintained, and annually validated business-continuity and disaster-recovery plans. Recovery-point and recovery-time objectives for MotionCX systems, if provided, will be established with consideration given to the architecture and intended use.

  - Customer Data is backed up securely. Customer Data on physical media intended for off-site storage, if any, such as media containing backup files, will be encrypted prior to transport.

- **Security Awareness and Training:**
  - All MotionCX employees complete security and privacy education annually and certify each year that they will comply with MotionCX's information security policies.
  - Additional policy and process training is provided to persons granted administrative access to MotionCX systems that is specific to their role in the operation and support of the solutions MotionCX provides, and as required to maintain compliance.
  - MotionCX promotes a culture of security awareness through periodic communications from senior management with employees.
- **Access Control:**
  - If access to Customer Data is required, it is restricted to the minimum level required, including termination of such access when no longer required and upon separation of the user from MotionCX. Such access, including administrative access to any MotionCX systems ("Privileged Access"), is individual, role-based, and subject to approval and regular validation by authorized personnel following the principles of segregation of duties.
  - Technical measures are maintained enforcing timeout of inactive sessions, lockout of accounts after multiple sequential failed login attempts, strong password or passphrase authentication, and measures requiring secure transfer and storage of such passwords and passphrases.
  - Adequate measures are maintained to identify and remove redundant and dormant accounts with Privileged Access and such Privileged Access is promptly revoked upon the account owner's separation from MotionCX or upon the request of authorized personnel, such as the account owner's manager.
- **Systems Security:**
  - To the extent supported by native device or operating system functionality, computing protections for end-user systems are maintained that include endpoint firewalls, full-disk encryption, signature-based malware detection and removal, time-based screen locks, and endpoint-management solutions that enforce security configuration and patching requirements.
- **Network Security:**
  - Documented security architecture of networks managed by or on behalf of MotionCX is maintained. Such network architecture, including measures designed to prevent unauthorized network connections to systems, applications and network devices, is reviewed for compliance with secure segmentation, isolation, and defense-in-depth standards prior to implementation.

  - To the extent wireless networking is used by MotionCX, such wireless networks, if any, is encrypted, requires secure authentication, and does not provide direct access to Customer Data.

- **Logging and Monitoring:**
  - Activity is logged and monitored and security information and event management measures are maintained designed to: a) identify unauthorized access (including without limitation Privileged Access) and activity; b) facilitate a timely and appropriate response; and c) enable internal and independent third-party audits of compliance with documented policy.
  - Network and systems monitoring includes without limitation error logs and security events, including changes affecting systems handling authentication, authorization, and auditing.
  - MotionCX continuously monitors and manages the health, including capacity and availability, of its production systems.
  - Logs are retained in compliance with MotionCX's records management plan. Measures designed to protect against unauthorized access, modification, and accidental or deliberate destruction of such logs are maintained.
- **Encryption:**
  - Customer Data not intended for public or unauthenticated viewing is encrypted when transferred over public networks, and cryptographic protocols such as HTTPS or SFTP shall be used for secure transfer of Customer Data over public networks.
  - Customer Data is encrypted at rest.
  - Documented procedures are maintained for secure cryptographic key generation, issuance, distribution, storage, rotation, revocation, recovery, backup, destruction, access, and use.
- **Secure Software Development:**
  - All software developed by MotionCX is developed, maintained, and decommissioned in accordance with a development lifecycle standard that incorporates security throughout, including without limitation secure coding principles and practices, full documentation, code review, and vulnerability testing.
  - Before new software is developed or acquired, security requirements are specified and documented.
  - All software development takes place in a test or development environment segregated from production systems, i.e., those in use for business operations. Environments and test plans are established to validate that the software works securely and as intended prior to deployment in production.
- **Physical and Environmental Security:**

  - MotionCX maintains or verifies the maintenance of appropriate physical entry controls, such as barriers, card-controlled entry points, surveillance cameras, and manned reception desks, to protect against unauthorized entry into facilities used to store Customer Data.
  - Access to such facilities is limited by job role and subject to authorized approval. Use of access badges to enter facilities and controlled areas is logged. Upon separation of authorized personnel, MotionCX revokes or procures the revocation of access and follows formal documented separation procedures including prompt removal from access-control lists and surrender of physical access badges.
  - MotionCX requires, including securing relevant contractual commitments from third-party vendors, that any person duly granted temporary permission to enter a facility with access to Customer Data, or controlled areas within such facilities, be registered upon entering the premises, must provide proof of identity upon registration, and be escorted by authorized personnel. Any temporary authorization to enter must be scheduled in advance and requires approval by authorized personnel.
  - MotionCX verifies that the operators of such facilities take all necessary and required precautions to protect their physical infrastructure against environmental threats, both naturally occurring and man-made, such as excessive ambient temperature, fire, flood, humidity, theft, and vandalism.
- **Vulnerability Management:**
  - MotionCX conducts risk assessments of systems processing Customer Data at least annually, carries out penetration testing and vulnerability assessments, including automated system and application security scanning and manual ethical hacking, before production releases and annually thereafter, engages qualified independent third-parties to perform penetration testing at least annually, carries out automated management and routine verification of compliance with security configuration requirements, and remediates identified vulnerabilities or noncompliance with security configuration requirements based on associated risk, exploitability, and impact.
  - MotionCX maintains measures designed to assess, test, and apply security patches to its systems. Upon determining that a security patch is applicable and appropriate, it implements the patch pursuant to documented severity and risk assessment guidelines. Implementation of security patches is subject to MotionCX’s change management policy (see below).
  - MotionCX takes reasonable steps to avoid service disruption when performing tests, assessments, scans, and execution of remediation activities.
- **Asset Management:**
  - MotionCX maintains an inventory of all information technology assets used in its operations.

- MotionCX implements policies and procedures requiring the secure disposal of devices and media containing Customer Data, so that Customer Data cannot be read or recovered using reasonably available means.

- **Change and Configuration Management:**
  - MotionCX follows formal processes for managing changes to production systems, applications, and databases, including without limitation documenting, testing, and approving patching and maintenance.
- **Employee Verification:**
  - MotionCX maintains and follows standard mandatory employment verification requirements for all new hires. In accordance with internal process and procedures, these requirements are periodically reviewed and may include criminal background checks, proof of identity validation, and additional checks as deemed necessary by MotionCX.
- **Third-Party Service Provider and Vendor Risk Management:**
  - MotionCX periodically assesses information security risk in connection with all third parties with access to systems storing, processing or otherwise providing access to Customer Data.

    All such third parties are contractually required to comply with minimum security requirements at least as stringent as those described here, in order to do business with MotionCX.