Federato Security Standards

1.0 Federato Security Standards

1.1 Federato will maintain a comprehensive information security program ("Federato Security Standards") which includes administrative, technical and physical safeguards to protect Customer Data. Federato safeguards are maintained to appropriately protect Customer Data based on commercially reasonable and industry standard resources available to Federato and the type of the Customer Data. The Federato security standards are designed to:

(a) Protect the availability, integrity and confidentiality of Customer Data;

(b) Protect against any anticipated threats or hazards to the confidentiality, integrity, availability of Customer Data;

(c) Protect against any unlawful unauthorized access, unlawful use, disclosure, alteration, or destruction by Federato of Customer Data; and

(d) Protect against any accidental loss, destruction, damage to Customer Data.

1.2 Federato will also monitor, evaluate and modify the Federato Security Standards to ensure:

(a) Use of industry standard technology pertinent to the protection of Customer Data;

(b) Commercially reasonable updates to the Services, Subscription Services, Federato Security Standards or Federato's systems, based on relevant changes in internal procedures for the protection of Customer Data, or as necessary to comply with applicable law;

(c) Federato relevant internal changes to Federato's technical environment including third parties, outsourcing arrangements, infrastructure and information systems.

2.0 Governance. Federato will maintain a governance program which includes:

2.1 Compliance with the baseline of security controls for a Software as a Service (SaaS) Cloud Service Provider

2.2 Policies and procedures based consistent with SOC2 requirements and other industry standard frameworks;

2.3 Data classification;

2.4 Geo-location options for storage of Customer Data;

2.5 Risk management; and

2.6 Third party security risk management.

3.0 Access Controls. Federato will maintain policies, procedures and logical controls designed to:

3.1 Limit access to Federato facilities and systems where those systems are limited to authorized persons;

3.2 Limit Federato employees' access to Customer Data by enforcing segregation of duties;

3.3 Protect from unauthorized access to Customer Data;

3.4 Remove or restrict Federato employees' access to Customer Data in a timely manner when access thereto is no longer required to perform Services, or upon Customer request;

3.5 Require multi-factor authentication through Federated Service for Federato access to Customer Data for the provision of Services; and.

4.0 Human Resource Security. Federato will maintain security and privacy policies and procedures for Human Resource including:

4.1 Performing pre-employment background screening commensurate with such employee's level of access to data, subject to applicable law;

4.2 Requiring all employees sign non-disclosure agreements;

4.3 Annual security and privacy role based training (including requirements of the Federato Security Standards, the importance of security Customer Data, and how to diagnose phishing attacks); and

4.4 Promoting a culture of security awareness through periodic trainings, blogs and programs which reward security best practices.

5.0 Physical and Environmental Security. Federato will maintain controls that are designed to protect from unauthorized access and against environmental hazards, including:

5.1 Controlled access to Federato facilities;

5.2 Inheritance of Physical and Environmental security controls from FedRAMP Moderate compliant Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) CSPs.

5.3 Logging and monitoring of access and unauthorized access to Federato facilities and systems;

5.4 Camera monitoring of Federato facilities;

5.5 Temperature, fire protection, humidity monitoring of Federato facilities; and

5.6 Uninterrupted power supplies to Federato facilities to maintain normal working conditions in compliance with our Business Continuity Plan.

6.0 Secure Development Lifecycle. Federato will maintain policies and procedures which will reasonably assure that development is done with commercially reasonable security practices including:

6.1 Secure development policies;

6.2 Secure development training;

6.3 Vulnerability management and remediation within timelines within the policy;

6.4 Segregation of duties for development review and release management;

6.5 Federato has and will maintain a formal change management program with segregation of duties.

7.0 Monitoring. Federato will provide network, system and application monitoring including servers, disks and Security events for any potential problems designed to:

7.1 Review changes to systems and infrastructure;

7.2 Review changes which handle systems, authentication authorization and auditing;

7.3 Review privileged access to Federato systems;

7.4 Review access to Federato production environment including abnormal access; and

8.0 Encryption. Federato will provide reasonable assurance of the protection of Customer Data through encryption algorithms within NIST guidelines, which includes:

8.1 Transmission encryption using AES 128 with TLS 1.2 or higher;

8.2 Encryption at rest using AES 256; and

8.3 Full disk encryption on all hard drives with access to production data with AES 256.

9.0 Incident Response. Federato will maintain an incident response policy with procedures to provide Customer with reasonable assurances that Federato can respond to any type of security event or breach, and which includes:

9.1 Roles and responsibilities with a team and a dedicated leader which is tested annually;

9.2 Methods for investigation and escalation assessing the event to determine the risk the event poses including proper escalation;

9.3 Processes regarding internal communications, reporting and notification and external reporting and notification to customers within forty-eight (48) hours of unauthorized disclosure of or access to Customer Data;

9.4 Appropriate documentation of the event, incident and investigation of what was done and by whom with authorization for later analysis and possible legal action; and

9.5 An audit of the incident conducting root cause analysis and remediation.

10.0 Contingency Planning. Federato will maintain policies and procedures for the response and or recovery of an emergency or other occurrence either natural or pandemic that could damage or affect systems, and the environment of customer data. Such procedures include:

10.1 Data resiliency through redundancy to recover data;

10.2 Business Continuity and Disaster Recovery plan which is communicated and made available within an event to minimize the impact and or loss of vital resources;

10.3 Annual testing of the Business Continuity Plan and Disaster Recovery Plan (Executive Summary available to Customer upon request); and

10.4 Auditing of the Disaster Recovery test.

11.0 Audit and Testing.

11.1 For no additional fees once annually upon Customer request Federato will provide Customer with reasonable assurances of its environments by providing SOC 2 Type II auditing reports.

12.0 Disposal.

12.1 Federato has policies and procedures to provide reasonable assurance to the appropriate return and/or disposal of Customer Data including:

(a) Secure shredding of printed documents and Customer Confidential Information; and

(b) Secure destruction of Customer Data with a certificate of destruction provided by Federato.

12.2 For a period of thirty (30) days from expiration or termination of the Agreement, Federato will provide Customer with continued access to the Subscription Services so it may remove such Customer Data.

13.0 Endpoint Devices. Federato has policies, procedures and technical controls to protect endpoint devices including:

13.1 Malware protection which cannot be disabled on the machine, regular updates and patches;

13.2 Full Disk Encryption (mitigating control as Customer Data is not stored on endpoint devices);

13.3 Regular updates and patching of the Subscription Services, Federato's systems and browsers; and

13.4 No write to removable media (USB).

14.0 Malware and Patching. Throughout the Agreement Term and in accordance with standard industry practice, Federato will:

14.1 Perform regular monitoring for security patches;

14.2 Apply patches in a timely manner after testing through change control; and

14.3 Regularly update systems and networks with new releases.

15.0 Shared Security Model. Customer acknowledges the security of the Subscription Services is a shared responsibility between Federato and Customer. Accordingly Customer will administer controls as recommended by commercially reasonable security frameworks (e.g., NIST, ISO, Federato's security recommendations). Administrative security within the Subscription Services is the responsibility of the Customer. Technical security, as outlined in this Exhibit, is the responsibility of Federato.