Data Security Exhibit

1. **Purpose.** This Data Security Exhibit sets forth the information security program and infrastructure policies that Sumo Logic shall meet and maintain in order to help protect Customer Data from unauthorized use, access or disclosure, during the term of the Agreement.

2. **Information Security Management Program.** Sumo Logic shall maintain throughout the Term of the Agreement an information security management program (the "**ISMP**") designed to protect and secure Customer Data from unauthorized access or use. The ISMP shall be documented and updated based on changes in applicable legal and regulatory requirements related to privacy and data security practices and industry standards. Sumo Logic incorporates commercially reasonable and appropriate methods and safeguards designed to protect the security, confidentiality, and availability of Customer Data. Sumo Logic shall, at a minimum, implement measures designed to adhere to applicable information security practices as identified in International Organization for Standardization 27001 (ISO/IEC 27001) (or a substantially equivalent or replacement standard) or other authoritative sources (e.g. SOC2).

3. **Independent Assessments.** On an annual basis, Sumo Logic has an independent third-party organization conduct an independent assessment consisting of a Report on Controls at a Service Organization Relevant to Security, Availability, Processing, Integrity, Confidentiality and/or Privacy (SOC2 Type II) or such other assessment at its sole discretion (e.g. ISO 27001 Certificate). Additionally, Sumo Logic undergoes regular penetration testing from independent third parties at least on an annual basis.

4. **Information Security Policies.** Sumo Logic shall implement information security and privacy policies that address the roles and responsibilities of Sumo Logic 's personnel who have access to Customer Data in connection with providing the Services. All Sumo Logic personnel with access to Customer Data shall receive annual training on Sumo Logic 's ISMP.

5. **Information Security Infrastructure.**
    a. **Access Controls**. Sumo Logic shall implement and maintain, throughout the Term and at all times while Sumo Logic has access to or possession of Customer Data, reasonable access controls (physical, technical, and administrative) that are designed to protect Customer Data.

    b. **Encryption**. Sumo Logic shall implement measures designed to encrypt Customer Data (i) at rest within the SaaS Services at a minimum AES algorithm with a default value of 256-bit strength; and (ii) in transit using TLS 1.2 encryption or stronger.

c. **Network and Host Security**. Sumo Logic has implemented measures designed to address network intrusion detection and firewalls. Sumo Logic uses reasonable efforts designed to ensure that the SaaS Services' operating systems and applications that are associated with Customer Data are patched or secured to mitigate the impact of security vulnerabilities in accordance with Sumo Logic's patch management processes.

d. **Data Management.** Sumo Logic has reasonable information security infrastructure controls in place for Customer Data obtained, transported, and retained by Sumo Logic for the provision of the Services.

6. **Business Continuity.** Sumo Logic shall maintain a business continuity plan, which is designed to ensure Sumo Logic shall be able to continue to provide the SaaS Services in accordance with the Agreement in the event of a disaster or other significant event that may impact Sumo Logic's operations.

Notwithstanding the foregoing, Customer understands and acknowledges that Customer shall be solely responsible for implementing and maintaining access and security controls on its own systems.