Security Practices

1. Purpose

This Security Exhibit outlines the essential security and privacy practices LogicMonitor shall meet and maintain in order to fulfill its obligations under the terms of the Agreement.

LogicMonitor may update or modify these practices from time to time, provided such updates and modifications shall not result in a degradation of the overall security of the Services during the term of the Agreement.

2. Information Security Management

LogicMonitor shall maintain throughout the Term of the Agreement formal information security management program designed to protect the confidentiality, integrity and availability of Customer Data. The program shall be documented and updated based on changes in applicable legal and regulatory requirements related to privacy and data security practices and industry standards.

3. Security Policies and Procedures

LogicMonitor shall maintain formal information security policies and procedures which address the following areas:

- **A.** Risk Assessment & Treatment. Formal risk management processes shall ensure that information security risks are reviewed holistically and have the visibility of executive management.
- **B.** Personnel. Background checks shall be conducted for each individual upon hire. Mandatory information security training shall be issued within each employee's first week, and annually thereafter.
- **C.** Access Management. Authorization to access business and production systems shall be limited to individuals with a specific need based on job title and function.
- **D.** Change Management. All changes to the Service shall be documented, and each change shall be reviewed, approved, and tested prior to release.
- **E.** Encryption Management. Customer Data shall be encrypted in transit using TLS 1.2 or higher encryption with GCM ciphers or stronger. Sensitive Customer Data shall be encrypted at rest using AES-256 or an equivalent strength cipher.
- **F.** Vulnerability Management. The Service operating platform shall be scanned for security vulnerabilities on an ongoing basis. Critical and high severity vulnerabilities shall be addressed with highest priority.
- **G.** Application Security. The applications which comprise the Service shall be tested for security defects using multiple testing modalities including static analysis, dynamic analysis, and software composition analysis where appropriate. New applications and services shall undergo a formal threat modeling exercise prior to introduction into the Service environment. Critical and high severity software defects shall be addressed with highest priority.
- **H.** Penetration Testing. The Service shall be subjected to third-party penetration testing on an annual cadence. Penetration testing shall include, at minimum, the following

analyses: information gathering; manual testing of flaws that may compromise the confidentiality, integrity, or availability of Customer Data; escalation of privilege; and system compromise steps. Application source code analysis shall be included in the penetration testing process to facilitate visibility into potential vulnerabilities. Any material security defects shall be addressed with highest priority.

- **I.** Emergent Threats. Any security vulnerabilities that positively result in an imminent threat to the confidentiality or integrity of Customer Data shall be addressed on a timeline not to exceed thirty (30) days from the point discovery.
- **J.** Incident Response. LogicMonitor shall track various sources for indicators of a breach to the confidentiality or integrity of the facilities, networks, and systems that house Customer Data, and shall maintain a formal incident response procedure to promptly mitigate damages caused by such an incident. Upon the detection of a security incident that may have impacted the confidentiality or integrity of Customer Data, LogicMonitor shall notify the customer in writing within 48 hours from the point of discovery, and shall provide Customer with ongoing updates throughout the incident lifecycle until it is formally closed.
- **K.** Business Continuity Management. LogicMonitor shall maintain a program to ensure ongoing delivery of the Service in the event of a disaster or other significant event that might otherwise impact operation of the business.

4. Data Handling and Protection

LogicMonitor shall maintain formal information security policies and procedures which address the following areas:

- **A.** Service Centers. The Service shall be hosted through geographically distributed data centers operated by third parties located in the United States. All data centers shall be certified to AICPA SOC2 Type 2 or equivalent standards, and provide redundant power, cooling, and security systems. LogicMonitor shall review the controls of these facilities at least annually to confirm adequate measures are in place to protect the availability and confidentiality of the Service.
- **B.** Production Servers. All production servers shall be security hardened using CIS or higher standards, have protective software installed, and be continually monitored for events that impact data security.
- **C.** Data Segregation. LogicMonitor shall maintain no less than industry standard logical data segregation in a multi-tenant environment designed to ensure Customer Data is not accessible by unauthorized individuals. LogicMonitor shall logically isolate Customer Data, and the Customer shall control the specific data stored in the Service. Each customer tenant shall be configured with a unique encryption key to ensure data confidentiality.
- **D.** Data Regionalization. With respect to the Service, Customer may select the service center region in which Customer Data is stored. Customer Data may be transferred to and/or allowed to be accessed by Personnel located in regions in which LogicMonitor provides operations and support services as memorialized in ***https://www.logicmonitor.com/data-handling-supplement***. Operational logs and other files submitted for analysis by LogicMonitor's support services shall be stored in the United States. In no event shall any Customer Data or Customer Confidential Information be accessed, stored, or processed from or in any OFAC-sanctioned country.

- **E.** Customer Data Handling. The Service shall maintain appropriate data security controls to address the following areas:
    - i. Logical access controls such as password strength requirements, multi-factor authentication, single sign-on, and role-based authorization
    - ii. Data access controls including encryption and hashing
    - iii. Automatic logout of individual accounts following inactivity timeout
    - iv. Temporary lockout of individual accounts following multiple authentication failures that must be reset by request of the individual. No time-based unlocking of accounts.
    - v. Audit logging of authentication events and other material activities with the tenant
- **F.** Data Return and Deletion. LogicMonitor shall provide a mechanism within the Service to allow for data export, which may be used to retrieve Customer Data upon termination.

5. Business Continuity Management

LogicMonitor shall maintain a formal business continuity management program designed to ensure the continuous operation of business processes which support delivery of the Services. The program shall be documented within LogicMonitor's formal information security policies and procedures, and shall specifically address the following areas:

- **A.** Business Technology Resiliency Planning. All business resources and technology services required for day-to-day business shall be sourced and implemented with resiliency as a primary goal.
    - i. LogicMonitor's corporate offices shall be operated such that any office could cease to exist without impact to business operations.
    - ii. All LogicMonitor employees shall be issued laptop computers as their personal workstations. In the event a corporate office becomes unavailable for use, employees shall continue to access business systems using internet access provided elsewhere.
    - iii. As security controls are implemented and maintained for business technology services, they shall be evaluated to meet continuity requirements.
    - iv. Business Continuity obligations for the operation of LogicMonitor's Services shall be maintained as defined in Section 5 of this Exhibit.
- **B.** Business Systems Resiliency Testing. LogicMonitor's business continuity plans shall be tested on an ongoing basis. Use of business systems by mobile and remote employees shall be used to provide performance indicators that inform required service levels.

6. Disaster Recovery

LogicMonitor shall maintain a formal disaster recovery program to ensure the resiliency of the Services through multiple types of potentially disruptive events.

- **A.** Architecture for Disaster Recovery. Anticipation of disaster recovery needs shall be a primary consideration in the design and implementation of systems and processes used to operate the Services.

- i. The Services shall operate only out of datacenters and IaaS providers that can provide high levels of redundancy in systems that provide power, cooling, network connectivity, fire suppression, flood control, and earthquake resiliency.
- ii. All hardware and network devices shall be deployed with sufficient redundancies to ensure stable and continuous operation that is tolerant of outages that affect both individual components.
- iii. Sufficient processes and procedures shall be maintained to meet a Recovery Time Objective (RTO) not to exceed 12 hours. The Recovery Point Objective (RPO) shall not exceed 36 hours. Service Level Indicators shall be maintained to report on overall availability targets.

- **B.** Backup and Restore
  - i. All customer data stored and processed by the Services shall undergo backup processes to ensure recoverability from incidents which impact security or availability. Backup data shall be created on a frequency targeted to meet the indicated RTO and RPO.
  - ii. Backup data shall be stored in multiple locations to ensure recoverability from an incident impacting any specific facility. Where backup data is transmitted across public networks, HTTP over TLS shall be used to encrypt transmission.
- **C.** Disaster Recovery Testing
  - i. Formal documentation describing the disaster recovery testing process for the Services shall be reviewed and updated at least annually.
  - ii. The backup/restore procedures upon which the Services' disaster recovery processes are based shall undergo continuous testing as part of regular capacity management exercises.
  - iii. A complete test of the Services' disaster recovery process, including simulation of datacenter failure, shall be conducted on an annual basis. Each test shall be followed by a report of the testing exercise, confirmation whether current RTO and RPO targets were met, as well as lessons learned and process improvements to decrease RTO and RPO values.
- D. Customer Communications. In the case of a significant disruption of the Services, LogicMonitor shall communicate such outages primarily via a notification service located at ***https://status.logicmonitor.com/***. Upon a significant disruption, customers may also receive notification via email or phone from a technical account manager.

7. Subprocessor Security

LogicMonitor shall conduct security assessments of its subprocessors that process Customer Data to ensure effectiveness of their security operational practices. LogicMonitor's current subprocessors are listed at ***https://www.logicmonitor.com/data-handling-supplement***.

8. Independent Assessments

On an annual basis, the Security Program shall be audited by an independent third-party to validate compliance with industry standards including the AICPA SOC2 Type 2 trust service principles, ISO/IEC 27001:2013, ISO/IEC 27017:2015, and ISO/IEC 27018:2014 . Upon written request, LogicMonitor shall provide evidence of these audit activities in the form of third-party assessment reports and/or certificates.

If LogicMonitor's existing third-party audit processes or a security incident demonstrate a material breach of our obligations to uphold the commitments made in this Exhibit, LogicMonitor will respond to the customer's reasonable written requests for more detailed information relevant to its security and privacy program. LogicMonitor may charge its then-current professional services rates for such responses. If it is demonstrated that LogicMonitor is failing to comply with any of its security and privacy obligations under this Agreement, then, LogicMonitor will take the necessary steps to comply at no additional cost to the Customer.

9. Shared Security Model

Notwithstanding the foregoing, Customer acknowledges that security is a shared responsibility between LogicMonitor and the Customer. Customer understands that the Service provides various security controls which must be properly configured according to LogicMonitor's documented best-practices, published at ***https://www.logicmonitor.com/support/getting-started/advanced-logicmonitor-setup/ security-best-practices***, to provide adequate protection for Customer Data.