SAILPOINT SAAS MANAGEMENT DATA SECURITY PROGRAM

SailPoint has implemented and shall maintain a commercially reasonable information security program for the SailPoint SaaS Management services, which shall include technical and organizational measures designed to ensure an appropriate level of security for Customer Personal Data taking into account the risks presented by the processing, in particular from accidental or unlawful destruction, loss, alteration, or unauthorized disclosure of, or access to Customer Personal Data, and the nature of the Customer Personal Data to be protected having regard to the state of the art and the cost of implementation. This document communicates the security program applicable to SailPoint SaaS Management, a SaaS Service, in accordance with SailPoint's Software as a Service Agreement (the "**SaaS Agreement**"). Except as otherwise modified or defined herein, capitalized terms shall have the same meaning as in the SaaS Agreement.

1. Security Program.

1.1. ISO27001-based Information Security Management System (ISMS): SailPoint shall maintain an ISMS risk-based security program to systematically manage and protect the organization's business information and the information of its customers and partners. With respect to SailPoint's SaaS Service, SailPoint has completed a SOC 2 Type 1 audit and ISO 27001 certification. SailPoint will complete a SOC 2 Type 1 audit annually and maintain ISO 27001 certification throughout the term of the SaaS Agreement or until such time as SailPoint receives any industry certification applicable to the SaaS Service which supersedes such certifications. Upon written request from Customer, SailPoint will provide a copy of such then-current certifications and audit reports.

1.2. Security Governance Committee: SailPoint shall maintain a security committee comprised of leaders across business units that oversees the company's security program. This committee shall meet monthly to review the operational status of the ISMS (including risks, threats, remediation actions, and other security-related issues) and drive continuous security improvement throughout the business.

1.3. Security incident response policy: SailPoint shall maintain policies and procedures to (1) investigate and respond to security incidents, including procedures to assess the threat of relevant vulnerabilities or security incidents using defined incident classifications and categorizations and (2) establish remediation and mitigation actions for events, including artifact and evidence collection procedures and defined remediation steps.

1.4. Policy maintenance: All security and privacy related policies shall be documented, reviewed, updated, and approved by management at least annually.

1.5. Communication and commitment: Security and privacy policies and procedures shall be published and communicated to all relevant and applicable personnel and subcontractors. Security shall be addressed at the highest levels of the company with executive management regularly discussing security issues and leading company-wide security initiatives.

2. Personnel Security.

2.1. Background screening: Personnel who have access to Customer Personal Data or the equipment on which it is stored shall be subject to background screening (as allowed by local laws) that shall include verification of identity, right to work and academic degrees and a check of criminal records, sex offender registries, and prohibited/denied party lists.

2.2. Confidentiality obligations: Personnel who have access to Customer Personal Data shall be subject to a binding contractual obligation with SailPoint to keep the Customer Personal Data confidential.

2.3. Security awareness training: Personnel shall receive training upon hire and at least annually thereafter covering security practices and privacy principles.

2.4. Code of conduct: SailPoint shall maintain a code of conduct and business ethics policy requiring ethical behavior and compliance with applicable laws and regulations.

3. Third-Party Security.

3.1. Screening: SailPoint shall maintain policies and procedures designed to ensure that all new sub-processors, SaaS applications, IT software, and IT service solutions are subject to reasonable due diligence to confirm their ability to meet corporate security and compliance requirements as well as business objectives.

3.2. Contractual obligations: SailPoint shall maintain controls designed to ensure that contractual agreements with sub-processors include confidentiality and privacy provisions as appropriate to protect SailPoint's interests and to ensure SailPoint can meet its security and privacy obligations to customers, partners, employees, regulators, and other stakeholders.

3.3. Monitoring and Review: As practicable, SailPoint shall periodically review existing third-party sub-processors in a manner designed to ensure the sub-processor's compliance with contractual terms, including any security and availability requirements. This review program shall review sub-processors at least annually (regardless of length of contractual term) to determine whether the sub-processor/solution is still meeting the company's objectives and the sub-processor's performance, security, and compliance postures are still appropriate given the type of access and classification of data being accessed, controls necessary to protect data, and applicable legal and regulatory requirements.

4. Physical Security.

4.1. Corporate facility security: A facility security program shall be maintained that manages building entrances, CCTVs, and overall security of its offices, including a security perimeter (including barriers such as card controller entry gates or manned reception desks). All employees, contractors, and visitors shall be required to wear identification badges which distinguish their respective role.

4.2. Corporate data center security: Systems installed on SailPoint's premises and used to process Customer Personal Data shall be protected by measures designed to control logical or physical access; equipment used to process Customer Personal Data cannot be moved, removed, upgraded, or reconfigured without appropriate authorization and protection of the information; and, when equipment processing Customer Personal Data is decommissioned, Customer Personal Data shall be disposed of in a manner that would prevent its reconstruction.

4.3. SaaS Service data center security: SailPoint leverages Amazon Web Services (AWS) data centers for hosting the SaaS Service. AWS follows industry best practices and complies with numerous standards. Details on AWS data center physical security are available at https://aws.amazon.com/compliance/data- center/controls/.

5. Solution Security.

5.1. Software development life cycle (SDLC): SailPoint shall maintain a software development life cycle policy that defines the process by which personnel create secure products and services and the activities that personnel must perform at various stages of development (requirements, design, implementation, verification, documentation and delivery).

5.2. Secure development: Product management, development, test and deployment teams are required to follow secure application development policies and procedures that are aligned to industry-standard practices, such as the OWASP Top 10.

5.3. Vulnerability assessment: SailPoint shall conduct risk assessments, vulnerability scans and audits (including third-party penetration testing of a representative instance of the SaaS Service twice annually). Identified product solution issues shall be scored using the Common Vulnerability Scoring System (CVSS) risk-scoring methodology based on risk impact level and the likelihood and potential consequences of an issue occurring. Vulnerabilities are remediated on the basis of assessed risk. Upon the written request of Customer, SailPoint shall provide information about the identified vulnerabilities in the SaaS Service or Required Software, as applicable to such Customer, and the measures taken to remediate or address any such vulnerabilities.

6. Operational Security.

6.1. Access controls: SailPoint shall maintain policies, procedures, and logical controls to establish access authorizations for employees and third parties. Such controls shall include:

6.1.1. requiring unique user IDs to identify any user who accesses systems or data;

6.1.2. managing privileged access credentials in a privileged account management (PAM) system;

6.1.3. communicating passwords separately from user IDs;

6.1.4. requiring that user passwords are (a) changed at regular intervals; (b) of sufficient length and complexity; (c) stored in an encrypted format; (d) subject to reuse limitations; and (e) not assigned to other users, even at a different time; and

6.1.5. automatically locking out users' IDs when a number of erroneous passwords have been entered.

6.2. Least privilege: Personnel shall only be permitted access to systems and data as required for the performance of their roles; only authorized personnel are permitted physical access to infrastructure and equipment; authorized access to production resources for the SaaS Service is restricted to employees requiring access; and access rights are reviewed and certified at least annually.

6.3. Malware: SailPoint shall utilize measures intended to detect and remediate malware, viruses, ransomware, spyware, and other intentionally harmful programs that may be used to gain unauthorized access to information or systems.

6.4. Encryption: SailPoint shall use Internet industry-standard encryption methods to protect data in transit and at rest as appropriate to the sensitivity of the data and the risks associated with loss; all laptops and other removable media, including backup tapes, on which Customer Personal Data is stored shall be encrypted.

6.5. Data backups: SailPoint shall backup data and systems using alternative site storage available for restore in case of failure of the primary system. All backups shall use Internet industry-standard encryption methods to protect backups in transit and at rest.

6.6. Change management: SailPoint shall maintain change management policies and procedures to plan, test, schedule, communicate, and execute changes to SailPoint's SaaS Service infrastructure, systems, networks, and applications.

6.7. Network security: SailPoint shall implement industry-standard technologies and controls designed to protect network security, including firewalls, intrusion prevention systems, monitoring, network segmentation, VPN, and wireless security. Networks shall be designed and configured to restrict connections between trusted and untrusted networks, and network designs and controls shall be reviewed at least annually.

6.8. Data segregation: SailPoint shall implement logical controls, including logical separation, access controls and encryption, to segregate Customer's Personal Data from other Customer and SailPoint data in the SaaS Service. SailPoint shall additionally ensure that production and non-production data and systems are separated.

*****End of Page*****