GENERAL PARTNER
DATA PROCESSING ADDENDUM

This SailPoint General Partner Data Processing Addendum ("**DPA**") forms part of the Agreement (as defined below) between SailPoint and Partner and shall be effective on the effective date of the Agreement ("**Effective Date**"). All capitalized terms not defined in this DPA shall have the meanings set forth in the Agreement.

1. Definitions

1.1. The following terms shall have meanings ascribed for the purposes of this DPA:

"**Affiliate**" has the meaning set forth in the Agreement, or if no such meaning is given, means an entity that controls, is controlled by or shares common control with a party, where such control arises from either (i) a direct or indirect ownership interest of more than 50% or (ii) the power to direct or cause the direction of the management and policies, whether through the ownership of voting stock by contract, or otherwise, equal to that provided by a direct or indirect ownership of more than 50%.

"**Agreement**" means any agreement in effect between Partner and SailPoint that is a partner type agreement between SailPoint and Partner and/or incorporates this DPA by reference.

"**Customer**" means an entity (i) which may acquire, through SailPoint or Partner, the right to use SailPoint Offerings for its own internal business use; (ii) to which a Partner may provide managed services for SailPoint Offerings; (iii) to which Partner may provide delivery or advisory services; or (iv) as otherwise defined in an agreement entered into between Partner and SailPoint.

"**Data Protection Laws**" means all data protection and privacy laws applicable to the respective party in its role in the Processing of Personal Information under the Agreement, including, but not limited to, (i) the Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) ("**GDPR**") as implemented by countries within the EEA; (ii) the European Union e-Privacy Directive 2002/58/EC as implemented by countries within the EEA; (iii) all laws relating to data protection, the processing of personal information, privacy and/or electronic communications in force from time to time in the United Kingdom of Great Britain and Northern Ireland (collectively, the "**UK**"), including the UK GDPR (as defined in section 3 of the Data Protection Act 2018) and the Data Protection Act 2018 (collectively "**UK Privacy Law**"); (iv), the Swiss Federal Act on Data Protection ("**FADP**" and as revised as of 25 September 2020, the "**Revised FADP**"); (v) the California Consumer Privacy Act, Cal. Civ. Code § 1798.100, et seq. as amended by the California Privacy Rights Act, as may be amended from time-to-time ("**CCPA**"), and any accompanying legally binding regulations that are promulgated to address provisions in the CCPA; and/or (vi) other laws that are similar, equivalent to, successors to, or that are intended to or implement the laws that are identified in (i), (ii), (iii), (iv) and (v) above.

"**Order**" means a quote, or an ordering document (including online order form) for SaaS Services intended for Internal Business Use of the Customer named for the Order during the Order Term and which is accepted through either: (i) Customer's signature on the SailPoint quote; or (ii) Customer's submission to SailPoint of a purchase order or other ordering document to order the SaaS Services). For purposes of determining each party's rights and obligations arising under the Agreement with respect to a given Order, "Order" does not include any preprinted or other terms and conditions on a Partner purchase order or ordering document that are inconsistent with, or additional to, the terms of the Agreement.

"**Other Services**" means, collectively or individually, all technical and non-technical consulting and advisory services identified in an Order as Professional Services (which may be identified as "Setup Services" or "Expert Services") or Training Services purchased and performed or delivered by SailPoint. For purposes of clarity, "Other Services" does not include the SaaS Services, or Support.

"**Partner**" means the party identified in the applicable Agreement in effect between SailPoint and such party.

"**Personal Information**" means: any information (i) relating to an identified or identifiable natural person; or (ii) defined as "personally identifiable information", "personal information", "personal data" or similar terms, as such terms are defined under Data Protection Laws.

"**Process**", "**Processes**", "**Processing**", and "**Processed**" means any operation or set of operations performed upon Personal Information, whether or not by automatic means.

"**Professional Services**" means consulting services provided by SailPoint to Customer and/or Partner that support Customer's and/or Partner's deployment, extension and use of SailPoint Offerings and include, but are not limited to, implementation services, implementation support, best practices consultations, and integration efforts as further described in, and subject to, the Agreement (including the applicable Order).

"**SaaS Services**" means any internet-accessible software-as-a-service offering hosted by SailPoint, its Affiliates or SailPoint's or its Affiliates' service providers, that is available for purchase.

"**SailPoint Offerings**" means any Software and Services made available or otherwise provided by SailPoint.

"**SCCs**" means, collectively, (i) where Personal Information of data subjects in the EEA is involved, the Standard Contractual Clauses as approved by the European Commission in the form set out in Commission Implementing Decision (EU)2021/914 of 4 June 2021 for the transfer of personal data to third countries pursuant to GDPR ("**EU SCCs**"), and (ii) where Personal Information of data subjects in the UK is involved, the EU SCCs as amended by the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner under Section 119A(1) Data Protection Act 2018 ("**UK SCCs**"), in each case, as completed as described in Section 5 below.

"**Security Incident**" means any unauthorised or unlawful breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to Personal Information on systems managed by or otherwise controlled by either Party.

"**Services**" means services provided by SailPoint which may include: (i) SaaS Services; (ii) Support; and (iii) Other Services provided by SailPoint to Customer and/or Partner pursuant to the Agreement.

"**Software**" means the object code version of the specific SailPoint computer software licensed to Customers and/or Partners under an Order, including any updates, modifications, new versions or releases.

"**Sub-processor**" or "**Subprocessor**" means any entity engaged to assist in fulfilling its obligations with respect to processing Personal Information.

"**Support**" means SailPoint's support and maintenance services for SailPoint Offerings as described in, and provided in accordance with the SailPoint Support Policy: at https://www.sailpoint.com/legal/.

"**Training Services**" means SailPoint's courses and other product-related training available through SailPoint's Identity University, on-site at SailPoint's, Customer's, Partner's, or a third party's location, or online via a SailPoint-provided website, as agreed by the parties.

1.2. Capitalised terms used in this DPA that are not defined in this Section 1 (Definitions) shall have the meaning ascribed to them elsewhere in this DPA and/or the Agreement or in applicable Data Protection Laws unless otherwise specified.

2. Jurisdiction-Specific Addenda

2.1. **California**. Pursuant to the Agreement, each Party ("**Disclosing Party**") may disclose Personal Information to the other Party ("**Receiving Party**") that it has received consent to disclose or otherwise been directed to disclose by a data subject. In such cases, each Receiving Party, as a Third Party, shall (i) process Personal Information provided by the Disclosing Party solely for the limited and specified purposes set forth in the Agreement and this DPA, including, but not limited to, promotion of each Party's business interests, customer referrals, joint marketing opportunities, executive round tables, marketing campaigns, paid media, and joint webinars, (ii) comply with all applicable sections of the CCPA and its regulations, including by providing the level of privacy protection required of businesses by the CCPA and its regulations; (iii) provide the Disclosing Party with information required for Disclosing Party to take reasonable and appropriate steps to ensure that Receiving Party uses Personal Information in a manner consistent with its obligation under the CCPA and its regulations; (iv) notify Disclosing Party after it makes a determination that it can no longer meet its obligations under the CCPA and its regulations, and (v) provide Disclosing Party the right, upon reasonable notice, including under (iv) above, to take reasonable and appropriate steps to stop and remediate unauthorized use of Personal Information made available to Receiving Party. The terms "Third Party" and "Personal Information," as used in this section, shall have the meanings set forth in the CCPA.

2.2. To the extent that the provisions of Section 2.1 may apply to Personal Information subject to similiar Data Protection Laws outside of California, the Parties shall treat such Personal Information as described therein without the need for subsequent or additional agreement between the Parties.

3. Updates to DPA.

SailPoint may update this DPA from time to time in the event of changes to applicable Data Protection Laws,the introduction of new laws, regulations, or other legally binding requirements to which either party is subject.

4. Roles and Scope of Processing

4.1. **Processing of Personal Information.** Partner: (i) agrees that it will comply with its obligations under Data Protection Laws in respect of its Processing of Personal Information and (ii) represents and warrants that it has provided all fair processing notices and obtained all consents and rights necessary under Data Protection Laws to transfer the Personal Information to SailPoint and for SailPoint to Process Personal Information as a Controller pursuant to the Agreement and this DPA.

4.2. Independent Controllers. The Parties acknowledge and agree that each Party shall act as an independent Controller with respect to any Personal Information collected or processed in connection with the Agreement. The Parties understand and agree that they (a) are acting, and shall act, independently of one another in their respective processing of such Personal Information, and are not and shall not be 'joint controllers' of such Personal Information within the meaning of Article 26(1) of the GDPR; (b) shall provide reasonable cooperation and assistance to the other Party as necessary for the other Party's compliance with applicable Data Protection Laws (at the other Party's reasonable expense) with respect to such Personal Information; and (c) shall be bound by the Standard Contractual Clauses with respect to any Restricted Transfers of such Personal Information that are made between them. Each Party will be responsible for its compliance with applicable Data Protection Laws. Without limiting the foregoing, each Controller agrees to the following:

(a) Each Controller is independently responsible for compliance with applicable Data Protection Laws in connection with its processing of Personal Information under the Agreement and this DPA, including, but not limited to, Data Subject notice and transparency requirements, the requirement to obtain any legally required consents, or any other necessary steps to lawfully conduct its business, and shall delete or destroy all Personal Information upon the conclusion of its purpose for Processing such Personal Information.

(b) Each party agrees to only Process the Personal Information it receives from the other party in accordance with the Agreement and this DPA.

4.3. Details of Data Processing.

(a) Categories of data subjects whose Personal Information is transferred:

Partner customers, Partner prospective customers, SailPoint customers, SailPoint prospective customers

(b) Categories of Personal Information transferred:

First name, last name, work address, work email, phone number, contact details, employer, job title/role

(c) Sensitive data transferred (if applicable):

None

(d) The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis)

Continuous

(e) Nature of the processing:

The mutual promotion of each Party's business interests pursuant to the Agreement.

(f) Purpose(s) of the data transfer and further processing:

To facilitate activities related to the mutual promotion of each Party's business interests.

(g) The period for which the Personal Information will be retained, or, if that is not possible, the criteria used to determine that period:

Data will be retained by each party independently for a period to last upon the conclusion of each party's independent purposes for processing.

5. Standard Contractual Clauses

5.1. To the extent that either Party acts as a Data Exporter ("**Data Exporter**") and transfers to the other Party as a Data Importer ("**Data Importer**") any Personal Information from the EEA, the UK, or Switzerland to countries not deemed by the European Commission, the UK Information Commissioner's Office, or Switzerland to provide an adequate level of data protection ("**Restricted Transfers**"), the SCCs will apply to any Restricted Transfers as follows:

(a) **EU Personal Information**. In respect of Personal Information that is protected by the EU GDPR, the EU SCCs will apply for any Restricted Transfers, are incorporated by reference, and are completed as follows:

(i) Module 1 applies;

(ii) in Clause 7, the optional docking clause will apply;

(iii) in Clause 11, the optional redress language will not apply;

(iv) in Clause 17, Option 2 will apply, and the EU SCCs will be governed by the law specified in the Agreement, provided that law is an EU Member State law recognizing third party beneficiary rights, otherwise, the laws of the applicable supervisory authority determined under Clause 13 of the EU SCCs shall govern;

(v) in Clause 18(b), disputes shall be resolved before the courts specified in the Agreement, provided these courts are located in an EU Member State, otherwise those courts shall be the courts of the EU Member State of the applicable supervisory authority determined under Clause 13 of the EU SCCs; and

(vi) in all cases the parties satisfy any signature requirement in "Annex 1: List of Parties" to the EU SCCs by the execution or acceptance of Partner and SailPoint to the binding Agreement effective between the parties.

(b) **UK Personal Information**. In respect of Personal Information that is protected by the UK Privacy Law, the UK SCCs will apply for any Restricted Transfers, are incorporated by reference, and are completed as follows:

(i) Table 1 of the UK SCCs is completed with the relevant information in Section 5.1(d) of the European Addendum;

(ii) Table 2 of the UK SCCs is completed with the selected modules and clauses from the EU SCCs as identified in Section 5.1(a) of the European Addendum;

(iii) Table 3 of the UK SCCs is completed with the relevant information in Sections 5.1(d) and 5.1(e) of the European Addendum;

(iv) both the importer and the exporter may terminate the UK SCCs in Table 4 of the UK SCCs in accordance with the terms of the UK SCCs; and

(v) in all cases the parties satisfy any signature requirement in UK SCCs by the execution or acceptance of Partner and SailPoint to the binding Agreement effective between the parties.

(c) **Swiss Personal Information**. In respect of Personal Information that is protected by the FADP, the EU SCCs as completed in Section 5.1(a) will apply for any Restricted Transfers, are incorporated by reference, and are amended as follows:

(i) the term "personal data" or "personal information" shall be deemed to include information relating to an identified or identifiable legal entity until the effective date of the Revised FADP;

(ii) references to (articles in) the EU General Data Protection Regulation 2016/679 shall be deemed to refer to (respective articles in) the FADP;

(iii) reference to the competent supervisory authority in Annex I. C. under Clause 13 of the SCCs shall be deemed to refer to the Federal Data Protection and Information Commissioner ("**FDPIC**");

(iv) references to Member State(s)/EU Member State(s) shall be deemed to include Switzerland;

(v) reference to the European Union in Annex I (A) shall be deemed to include Switzerland;

(vi) where the Clauses use terms that are defined in the GDPR, those terms shall be deemed to have the meaning as the equivalent terms are defined in the FADP;

(vii) the list of data subjects and categories of data indicated in Annex I. B. to the SCCs shall not be deemed to restrict the application of the SCCs to the Swiss Personal Information; and

(viii) in all cases the parties satisfy any signature requirement under the FADP by the execution or acceptance of Partner and SailPoint to the binding Agreement effective between the parties.

(d) **SCC Annex I**:

(i) In respect of Annex I, Section A of the EU SCCs, the requisite information is as follows:

(A) Partner, acting as Data Exporter when transferring Personal Information to SailPoint, and acting as Data Importer when receiving Personal Information from SailPoint:

Name: as identified in the Agreement

Address: as identified in the Agreement

Contact person's name, position and contact details: as identified in the Agreement

Activities relevant to the data transferred under these Clauses:

Promotion of each Party's business interests, customer referrals, joint marketing opportunities, executive round tables, marketing campaigns, paid media, joint webinars, joint marketing content creation

Signature and date: the parties agree that any signature requirement is satisfied by the execution or acceptance of Partner and SailPoint to the binding Agreement effective between the parties.

Role (controller/processor): Controller

(B) SailPoint, acting as Data Exporter when transferring Personal Information to Partner, and acting as Data Importer when receiving Personal Information from Partner:

Name: SailPoint Technologies, Inc.

Address: 11120 Four Points Drive, Suite 100, Austin, Texas 78726, USA

Contact person's name, position and contact details:

SailPoint's Data Protection Officer:
Dr. Felix Wittern
Partner, Fieldfisher
Hamburg, Germany
privacy@sailpoint.com

Activities relevant to the data transferred under these Clauses:

Same as listed above for Partner.

Signature and date: the parties agree that any signature requirement is satisfied by the execution or acceptance of Partner and SailPoint to the binding Agreement effective between the parties.

Role (controller/processor): Controller

(ii) In respect of Annex I, Section B of the EU SCCs, the requisite information is as follows:

(A) Please see Section 4.3 (Details of Data Processing) of the DPA for details of transfer(s);

(B) For transfers to (sub-) processors, each party as separate controllers will independently determine the subject matter, nature, and duration of processing by their (sub-) processors.

(iii) In respect of Annex I, Section C of the EU SCCs, the competent supervisory authority shall be the applicable supervisory authority determined under Clause 13 of the EU SCCs.

(e) **SCC Annex II**:

(i) In respect of Annex II of the EU SCCs, the requisite information is as follows:

(A) Description of the technical and organisational measures implemented by the data importer(s)

Please see Exhibit A of this Addendum, which describes the basic technical and organizational security measures to be implemented by each party.

(B) For transfers to (sub-) processors, each party as separate controllers will independently determine that their (sub-) processors shall ensure that they have appropriate technical and organisational measures to protect against and report a personal data breach, appropriate to the harm that might result from such personal data breach, having regard to the state of technological development and the cost of implementing any measures.

5.2. The parties agree that the data export solution identified in Section 5.1 (Standard Contractual Clauses) will not apply if and to the extent that SailPoint adopts an alternative data export solution for the lawful transfer of Personal Information (as recognised under applicable Data Protection Laws) outside of the EEA, the UK, or Switzerland in which event, Partner shall take any action (which may include execution of documents) required to give effect to such solution and the alternative transfer mechanism will apply instead (but only to the extent such alternative transfer mechanism extends to the jurisdictions to which Personal Information is transferred).

6. Sub-processing

6.1. **Sub-processor Obligations**. If and to the extent either Controller transfers any Personal Information to any third-party data processor, such Controller shall first enter into contractual arrangements with such third party data processors obligating such processor to Process the Personal Information in accordance with the requirements under the applicable Data Protection Laws.

7. Security

7.1. **Security Measures**. Taking into account the nature of the Processing, each Controller shall implement and maintain reasonable technical and organisational security measures to protect Personal Information from Security Incidents and to preserve the security and confidentiality of the Personal Information. SailPoint shall implement security measures in accordance with the security standards described in **Schedule A** ("**Security Measures**"), and Partner shall implement substantially similar security measures. In the event that either Party suffers a Security Incident connected to Personal Information received from the other Party, the Party suffering the Security Incident shall notify the other Party without undue delay and the Parties shall reasonably cooperate with each other in taking such measures as may be necessary to notify affected Data Subjects, comply with each Party's obligations under applicable Data Protection Laws, and to mitigate or remedy the effects of such Security Incident.

8. Cooperation

8.1. Taking into account the nature of the Processing, each Party shall provide reasonable cooperation to assist in response to any requests from data subjects in relation to their data subject rights under applicable Data Protection Laws or applicable regulatory authorities relating to the Processing of Personal Information under the Agreement.

8.2. If, after the date of this DPA, the Data Importer receives any Government Agency Requests concerning the Personal Information of the Data Exporter, Data Importer shall attempt to redirect the law enforcement or government agency to request that data directly from Data Exporter. As part of this effort, Data Importer may provide Data Exporter's basic contact information to the government agency. If compelled to disclose Data Importer's Personal Information to a law enforcement or government agency, Data Importer shall give Data Exporter reasonable notice of the demand and cooperate to allow Data Exporter to seek a protective order or other appropriate remedy unless Data Importer is legally prohibited from doing so. Data Importer shall not voluntarily disclose Personal Information to any law enforcement or government agency. Data Exporter and Data Importer shall (as soon as reasonably practicable) discuss and determine whether all or any transfers of Personal Information pursuant to this Addendum should be suspended in the light of the such Government Agency Requests.

9. Relationship with the Agreement

9.1. Except for the changes made by this DPA, the Agreement remains unchanged and in full force and effect. If there is any conflict between this DPA and the Agreement, this DPA shall prevail to the extent of that conflict in connection with the Processing of Personal Information.

9.2. Notwithstanding anything to the contrary in the Agreement or this DPA, the liability of each party and each party's Affiliates under this DPA shall be subject to the exclusions and limitations of liability set out in the Agreement. Without limiting either of the parties' obligations under the Agreement, Partner agrees that any regulatory penalties incurred by SailPoint that arise as a result of, or in connection with, Partner's failure to comply with its obligations under this DPA or any applicable Data Protection Laws shall count toward and reduce SailPoint's liability under the Agreement as if it were liability to the Partner under the Agreement.

9.3. Any claims against SailPoint or its Affiliates under this DPA shall only be brought by the Partner entity that is a party to the Agreement against the SailPoint entity that is a party to the Agreement. In no event shall this DPA or any party to this DPA restrict or limit the rights of any data subject or of any competent supervisory authority.

9.4. This DPA will be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement, unless required otherwise by applicable Data Protection Laws.

9.5. This DPA will terminate automatically with the termination or expiry of the Agreement, subject to additional provisions in any Addenda attached hereto.

Schedule A – Security Measures

SailPoint Data Security Program

SailPoint has implemented and shall maintain a commercially reasonable security program in accordance with industry best practices, which shall include technical and organisational measures to ensure an appropriate level of security for Personal Information taking into account the risks presented by the Processing, in particular from accidental or unlawful destruction, loss, alteration, or unauthorised disclosure of, or access to Personal Information, and the nature of the Personal Information to be protected having regard to the state of the art and the cost of implementation. The security program shall include the following measures:

1. Security Program

a. **ISO27001-based Information Security Management System (ISMS)**: SailPoint shall maintain an ISMS risk-based security program to systematically manage and protect the organisation's business information and the information of its customers and partners.

b. **Security Governance Committee**: SailPoint shall maintain a security committee comprised of leaders across all 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.

c. **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 categorisations and (2) establish remediation and mitigation actions for events, including artifact and evidence collection procedures and defined remediation steps.

d. **Policy maintenance**: All security and privacy related policies shall be documented, reviewed, updated and approved by management at least annually to ensure they remain consistent with best practices, legal and regulatory requirements and industry standards.

e. **Communication and commitment**: Security and privacy policies and procedures shall be published and effectively communicated to all personnel and relevant 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

a. **Background screening**: Personnel who have access to Personal Information or the equipment on which it is stored shall be subject to background screening (as allowed by local laws and regulations) 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.

b. **Confidentiality obligations**: Personnel who have access to Personal Information shall be subject to a binding contractual obligation with SailPoint to keep the Personal Information confidential.

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

d. **Code of conduct**: SailPoint shall maintain a code of business conduct policy and compliance program to ensure ethical behavior and compliance with applicable laws and regulations.

3. Third-Party Security

a. **Screening**: SailPoint shall maintain policies and procedures to ensure that all new suppliers, 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.

b. **Contractual obligations**: SailPoint shall ensure that contractual agreements with suppliers 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.

c. **Monitoring**: SailPoint shall periodically review existing third-party suppliers to ensure the supplier complies with contractual terms, including any security and availability requirements. The monitoring program shall review suppliers at least annually (regardless of length of contractual term) to confirm that the supplier/solution is still meeting the company's objectives and the supplier'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

a. **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.

b. **Corporate data center security**: Systems installed on SailPoint's premises and used to Process Personal Information shall be protected in such a manner that unauthorised logical or physical access is effectively prevented; equipment used to Process Personal Information cannot be moved, removed, upgraded or reconfigured without appropriate authorisation and protection of the information; and, when equipment Processing Personal Information is decommissioned, Personal Information shall be disposed of securely in a manner that would prevent its reconstruction.

5. Operational Security

a. Access controls: SailPoint shall maintain policies, procedures, and logical controls to establish access authorisations for employees and third parties to limit access to properly authorised personnel and to prevent unauthorised access. Such controls shall include:

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

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

iii. communicating passwords separately from user IDs;

iv. ensuring that user passwords are (1) changed at regular intervals; (2) of sufficient length and complexity; (3) stored in an encrypted format; (4) subject to reuse limitations; and (5) not assigned to other users, even at a different time; and

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

b. **Least privilege**: SailPoint shall ensure that personnel only have access to systems and data as required for the performance of their roles; only authorised personnel have physical access to infrastructure and equipment; and access rights are reviewed and certified at least annually to ensure access is appropriate.

c. **Malware**: SailPoint shall utilise industry-standard measures to detect and remediate malware, viruses, ransomware, spyware, and other intentionally harmful programs that may be used to gain unauthorised access to information or systems.

d. **Encryption**: SailPoint shall use industry-standard strong 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 Personal Information is stored shall be encrypted.

e. **Business continuity and disaster recovery (BCDR)**: SailPoint shall maintain formal BCDR plans that are regularly reviewed and updated to ensure SailPoint's systems and services remain resilient in the event of a failure, including natural disasters or system failures.

f. **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 strong encryption in transit and at rest.

g. **Change management**: SailPoint shall maintain change management policies and procedures to plan, test, schedule, communicate, and execute changes to infrastructure, systems, networks, and applications.

h. **Network security**: SailPoint shall implement industry standard technologies and controls 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.

End of SailPoint General Partner Data Processing Addendum