DATA PROCESSING AGREEMENT

This Data Processing Agreement (**"DPA"**) forms part of the Identity Automation Software (SaaS) Master Subscription Agreement, or other negotiated agreement between the Parties pursuant to which we provide Services to you, and any subsequent amendments, schedules or appendices (the **"Agreement"**) between Identity Automation Systems, LP, a Jamf company (**"Identity Automation" "we"** or **"Processor"**) and the entity identified in the Order Form as the customer (**"Customer" "you**" or **"Controller"**) each a "**Party"** and collectively the "**Parties".**

1. Overview This DPA applies to the Processing of Personal Data by Identity Automation on behalf of Customer in connection with the provision of Services under the Agreement. It is effective from the date of signature on the Order Form (the **"DPA Effective Date"**) and will terminate on the same date that the Agreement terminates (the "**Term"**).

2. Definitions. Capitalized terms not defined in the DPA will have the meanings given to them in the Agreement. Where the UK GDPR applies to the Processing of Personal Data under this DPA, references in this DPA to the GDPR and to provisions of the GDPR will be construed as references to the UK GDPR and to the corresponding provisions of the UK GDPR, and references to EU or Member State law will be construed as references to UK law. Any terms not defined in this DPA or the Agreement will have the same meaning as set out in the Standard Contractual Clauses, the CPRA or the GDPR or UK GDPR, as relevant.

a) **"Affiliate"** means any entity that directly or indirectly controls, is controlled by, or is under common control with a party, where "control" means the ownership or control of more than 50% of the voting interests of such entity.

b) **"COPPA"** means the Children's Online Privacy Protection Act, 1998.

c) "**Data Protection Laws**" means all applicable government data protection and privacy , student and education data privacy, cyber security laws, rules, and regulations of any country, including (i) the EU General Data Protection Regulation 2016/679 ("**GDPR**"), (ii) the UK General Data Protection Regulation, with the meaning given in section 3(10) (as supplemented by section 205(4)) of the Data Protection Act 2018 ("**UK GDPR**"), (iii) the Swiss Federal Data Protection Act of 1 September 2023 ("**Swiss Data Protection Act**"), (iv) data protection laws of the European Union ("**EU**"), European Economic Area ("**EEA**") member states, or the United Kingdom ("**UK**") that supplement the GDPR or UK GDPR (respectively), and (v) the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 (collectively referred to as the "**CPRA**"), (vi) FERPA; (f) COPPA; and (g) any other applicable data protection, privacy, or student data privacy law or regulation, including applicable state student privacy laws, all as amended or superseded from time to time.

d) "**Data Subject**" means the identified or identifiable individual to whom Personal Data relates.

e) **"Education Records"** means education records as defined under FERPA (20 U.S.C. § 1232g), including any personally identifiable information contained therein.

f) "**ex-EEA Transfer**" means a Processing activity whereby Customer transfers Personal Data that is Processed under the GDPR to Identity Automation outside the EEA, and such transfer is not governed by an adequacy decision made by the European Commission ("**EC**") in accordance with the relevant provisions of the GDPR.

g) "**ex-Swiss Transfer**" means a Processing activity whereby Customer transfers Personal Data that is Processed under Swiss Data Protection Laws to Identity Automation outside Switzerland, and such transfer is not governed by an adequacy decision made by the Federal Data Protection and Information Commissioner of Switzerland ("**FDPIC**") in accordance with the relevant provisions of the Swiss Federal

Data Protection Act.

h) "**ex-UK Transfer**" means a Processing activity whereby Customer transfers Personal Data that is Processed under the UK Data Protection Laws to Identity Automation outside the UK, and such transfer is not governed by an adequacy decision pursuant to Section 17A of the UK Data Protection Act 2018**.**

i) **"FERPA"** means The Family Educational Rights and Privacy Act of 1974.

j) "**Government Agency**" means a government agency or law enforcement authority, including judicial authorities.

k) "**Personal Data**" means any personal data (as defined in applicable Data Protection Laws) we or our Sub-processors Process when providing Services to you under the Agreement.

l) **"Personal Data Breach"** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data Processed by Identity Automation.

m) **"Processing"** (and "Process") means any operation or set of operations performed on Personal Data or sets of Personal Data, whether or not by automated means, as defined in Article 4(2) of the GDPR.

n) **"Restricted Transfer"** means a transfer of Personal Data from the EEA, UK, or Switzerland to a country that has not been deemed to provide an adequate level of data protection by the relevant authority.

o) **"Service"** means the services that we provide you as defined in the Agreement.

p) **"Standard Contractual Clauses"** means

(i) where the GDPR applies, the standard contractual clauses approved by the EC and annexed to the EC's Implementing Decision 2021/914 dated 4 June 2021 on standard contractual clauses for transfers of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council ("**EEA Standard Contractual Clauses**"),

(ii) where the UK GDPR applies, the "International Data Transfer Addendum to the EU Commission Standard Contractual Clauses" issued by the Information Commissioner under s.199A(1) of the UK Data Protection Act 2018 ("**UK Addendum**"), and

(iii) where the Swiss Data Protection Act applies, the applicable standard contractual clauses issued, approved, or recognized by the Swiss Data Protection Act and Information Commissioner ("**Swiss Standard Contractual Clauses**"), in each case as may be amended or updated from time to time.

q) **"Student Data"** any information directly related to a student maintained by an educational institution or party acting for it, including files, documents, and materials containing personally identifiable information such as grades, records, and disciplinary files.

r) "**Sub-processor**" means any third party engaged by Identity Automation to Process Personal Data on behalf of Customer.

3. CPRA PROCESSING OF PERSONAL DATA

To the extent that the CPRA applies to the Processing of Personal Data under the Agreement, the following provisions shall apply:

(a) Identity Automation will process Personal Data disclosed by Customer only for the limited and specified business purposes of providing the Services as set out in the Agreement.

(b) Identity Automation will comply with all applicable sections of the CPRA and shall provide the same level of privacy protection as is required of businesses under the CPRA.

(c) Identity Automation will not retain, use, or disclose Personal Data for any purpose other than performing the Services or outside the direct business relationship between Identity Automation and Customer.

(d) Identity Automation will not sell or share Personal Data for monetary or other valuable consideration, or for cross-context behavioral advertising.

(e) Identity Automation may disclose Personal Data to service providers or contractors provided that Customer is notified and such recipients are bound by equivalent CPRA protections.

(f) Identity Automation will not combine Personal Data received from Customer with personal information received from other persons or entities, or collected from Identity Automation's own interactions with data subjects, except as permitted by the CPRA.

(g) With respect to deidentified data, Identity Automation will take reasonable measures to prevent reidentification, publicly commit to maintaining the data in deidentified form, and contractually obligate any recipients to do the same.

(h) Identity Automation shall implement reasonable security procedures and practices appropriate to the nature of the Personal Data.

(i) Customer will have the right to take reasonable and appropriate steps to stop and remediate any unauthorized use of Personal Data.

(j) Identity Automation will notify Customer if it determines that it can no longer meet its obligations under the CPRA

4. PROCESSING OF PERSONAL DATA

a) Relationship of the Parties. Customer is the Controller and Identity Automation is the Processor of Personal Data processed under this DPA. Where Customer acts as a Processor on behalf of a third-party Controller, references to "Controller" shall be read accordingly, and Customer warrants that it has obtained all necessary authorizations from the relevant Controller.

b) Processing. We will Process Personal Data in accordance with the requirements of Data Protection Laws, as set out in the Agreement, or your documented instructions. Details of the Processing, including the types of Personal Data, categories of Data Subjects, and duration of Processing, are set out in Schedule 1 to this DPA. We may make reasonable amendments to Schedule 1 from time to time as reasonably necessary to reflect new product features or changing practices or processes by sending an updated or an additional Schedule 1 to you. We will inform you if we become aware that your Processing instructions infringe applicable Data Protection Laws. We will provide reasonable and timely assistance to enable you to respond to any request received from a Data Subject, regulator, or other third party in connection with the Processing of Personal Data only if we are not legally prohibited from doing so. If we expect to incur costs from this assistance, we will promptly inform you in advance and work together to agree on such costs. If a Data Subject makes a request directly to us, unless legally prohibited from doing so, we will promptly inform you and provide the related details.

c) Transfers of EEA Personal Data. The Parties agree that when the transfer of Personal Data from you (as data exporter) to us (as data importer) is an ex-EEA Transfer, such transfers will be subject to the EEA Standard Contractual Clauses (official text found here: https://commission.europa.eu/publications/publications-standard-contractual-clauses-sccs_en and will be completed as follows:

i) Module Two will apply;

ii) In clause 7, the optional docking clause will not apply (unless requested by you giving a detailed reason);

iii) In Clause 9, Option 2 will apply, and the time period for notice of Sub-processor changes will be as set out in clause 5 of this DPA;

iv) In Clause 11, the optional language will not apply;

v) In Clause 17, Option 1 will apply, and the EEA Standard Contractual Clauses will be governed by Irish law;

vi) In Clause 18 (b), disputes will be resolved before the courts of Ireland;

vii) Annex I of the EEA Standard Contractual Clauses will be deemed completed with the information set out in Schedule 1 to this DPA;

viii) Annex II of the EEA Standard Contractual Clauses will be deemed completed with the information set out in Schedule 3 to this DPA; and

ix) Annex III of the EEA Standard Contractual Clauses will be deemed completed with the information

set out in Schedule 2 to this DPA.

d) Transfers of UK Personal Data. The Parties agree that when the transfer of Personal Data from you (as data exporter) to us (as data importer) is an ex-UK Transfer, such transfers will be subject to the UK Addendum (official text found here: https://ico.org.uk/media2/migrated/4019539/international-data-transfer-addendum.pdf and will be completed as follows:

i) The EEA Standard Contractual Clauses, completed as set out above in clause 4 c) of this DPA, will also apply to transfers of UK Personal Data, subject to sub-clause 4 d) ii) below;

ii) Tables 1 to 3 of the UK Addendum will be completed with relevant information from the EEA Standard Contractual Clauses, completed as set out above, and the option "data importer" will be deemed checked in Table 4. The start date of the UK Addendum (as set out in Table 1) will be the date of this DPA.

e) Transfers of Swiss Personal Data. The Parties agree that when the transfer of Personal Data from you (as data exporter) to us (as data importer) is an ex-Swiss Transfer, such transfers will be subject to the Swiss Standard Contractual Clauses:
The EEA Standard Contractual Clauses, completed as set out above in clause 4 c) of this DPA, will also apply to transfers of Swiss Personal Data Subject to the modifications and amendments prescribed by the Swiss Federal Data Protection and Information Commissioner (as described here: https://www.edoeb.admin.ch/dam/en/sd-web/smvG75WY5Vsi/%C3%9Cbermittlung.

f) Further Assurance. If Data Protection Laws require Customer to execute the applicable Standard Contractual Clauses as a separate agreement, we will provide this on Customer's request. If either (i) any of the means of legitimizing transfers of Personal Data outside of the EEA or UK which are referred to in this DPA cease to be valid or (ii) any supervisory authority requires transfers of Personal Data pursuant to those means to be suspended, then we may, giving notice to you and with effect from the date set out in such notice, amend or put in place alternative arrangements for such transfers, as required by the relevant Data Protection Laws. If this DPA needs to be modified because of a change in Data Protection Laws, including a change to the Standard Contractual Clauses, then either Party may provide written notice to the other Party of the change. The Parties will discuss and negotiate, in good faith, any necessary changes to this DPA to address such changes in Data Protection Laws.

g) Supplementary measures. For any Restricted Transfer, the following applies:

i) We represent and warrant that, as of the Effective Date, we have not received any Government Agency requests for customer data, which may include Personal Data;

ii) If, after the Effective Date, we receive any Government Agency requests for your data, which may include Personal Data, we will (unless prohibited by law from doing so) inform you in writing as soon as reasonably practicable so that you, as the Controller, can work directly with the Government Agency, and together we will discuss and determine whether all or any transfers of Personal Data pursuant to this DPA should be suspended in the light of such requests; and

iii) The Parties may meet, as reasonably requested by either Party or as required under applicable Data Protection Laws, to consider whether:

1) The protection afforded to Data Subjects by the laws where we are based is sufficient to provide broadly equivalent protection to that afforded in Switzerland, the EEA and/or the UK;

2) Additional measures are reasonably necessary to enable the transfer to be compliant with the Data Protection Laws; and

3) It is still appropriate for Personal Data to be transferred to us, considering all relevant information available to the Parties, together with guidance provided by the supervisory authorities.

5. Sub-processors.

a) Approved Sub-processors. You authorize the Processing of Personal Data by the Sub-processors listed in Schedule 2 (***Approved Sub-Processors***). We will notify you of any change in Sub-processors, including the addition or replacement of Sub-processors, thereby giving you the opportunity to object to such changes. If, within 30 business days of receipt of that notice, you have not objected to the intended change, you are deemed to have authorized the intended change.

b) Contract with Sub-processor. We will impose on all Sub-processors written data protection obligations that offer the same protection of Personal Data as the data protection obligations to which we are bound in the Agreement and this DPA, including the obligation to notify us of data protection complaints in accordance with Section 6b). If a transfer of Personal Data between us and a Sub-processor constitutes a Restricted Transfer, we will enter into the relevant Standard Contractual Clauses with the Sub-processor. We will remain responsible for complying with the obligations of this DPA and for any acts or omissions of the Sub-processors that cause us to breach any of our obligations under this DPA.

6. a) Data Subject Requests. Considering the nature of Processing and the information available, the Parties will assist each other to fulfill their obligations to respond to Data Subject rights requests under applicable Data Protection Laws. If you are unable to respond to a request independently, we will, on your written request, provide reasonable assistance in responding to such request under Data Protection Laws. If legally permitted, we will promptly notify you if we receive such requests and if any costs incurred in helping exceed the scope of our obligations under Data Protection Laws and/or routine customer service, the Parties will negotiate in good faith to agree such costs.

b) Data Protection Complaints. If we receive a complaint from a Data Subject that relates to the Processing of Personal Data carried out on your behalf, we will, unless legally prohibited from doing so, notify you in writing without undue delay and provide you with a copy of the complaint. We will not respond to the complainant without your prior written instructions, unless required to do so by applicable law. On your written request, we will provide reasonable assistance to enable you to investigate and respond to such complaint. If any costs we incur in providing such assistance exceed the scope of our obligations under Data Protection Laws and/or routine customer service, we will inform you in advance and the Parties will negotiate in good faith to agree such costs. We will ensure that the written data protection obligations we impose on Sub-processors pursuant to Section 5(b) include an obligation on each Sub-processor to notify us if it receives a data protection complaint relating to the Processing of Personal Data carried out on your behalf.

7. IDENTITY AUTOMATION PERSONNEL

a) Confidentiality. We will ensure that personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities, and have executed written confidentiality agreements. We will ensure that such confidentiality obligations survive the termination of the personnel engagement.

b) Limitation of Access. We will ensure that access to Personal Data is limited to personnel performing Services in accordance with the Agreement.

c) Privacy Officer. We have appointed a privacy officer, who may be reached at privacy@Jamf.com.

8. Security. We have implemented and will maintain appropriate technical and organizational measures to secure Personal Data against the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data and will comply with Data Protection Laws by taking the security measures referred to in Article 32(1) of the GDPR as appropriate, and at a minimum, meet the requirements set out in Schedule 3 to this DPA (*Security Measures*).

9. Personal Data Breach Management and Notification. We maintain security incident management policies and procedures and will notify you of any Personal Data Breach without undue delay and no later than 48 hours upon becoming aware of a Personal Data Breach. Identity Automation will include the nature of breach, categories, approximate numbers of data subjects affected, likely consequences, mitigation measures taken or proposed. If the Personal Data Breach is caused by our violation of our obligations under this DPA, we will make reasonable efforts to identify and remediate the cause of the Personal Data Breach. If a Personal Data Breach is caused by your violation of your obligations under this DPA, you will make reasonable efforts to identify and remediate the cause of the Personal Data Breach. Unless required by applicable Data Protection Laws, we will not inform any third party of any such Personal Data Breach without your prior written consent.

10. Data Protection Impact Assessments. We provide resources to assist customers with completing data protection or privacy impact assessments required under Data Protection Laws. These resources, as updated from time to time, are available in our Trust Center https://www.identityautomation.com/trust-center and https://www.jamf.com/trust-center/legal/. We will provide you with reasonable assistance to complete a data protection impact assessment or privacy impact assessment, upon reasonable written request by you. If such assistance exceeds the scope of our obligations under Data Protection Laws, and/or routine customer service, we will promptly inform you in advance and the Parties will then negotiate in good faith to agree on any additional costs.

11. Audits.

a) We allow for, cooperate with, and contribute to audits to check compliance with Data Protection Laws and this DPA, including inspections (where we are permitted to allow access) conducted by you or an external auditor you

engaged. Audits may be conducted: (i) from time to time on reasonable notice, but no more than once annually; (ii) during normal business hours and so as not to unreasonably interfere with our performance of the Services under the Agreement or unreasonably interfere with our business; and (iii) during the Term of this DPA. The notice requirement in this Section 11 a) (i) and the restrictions stated in Section 11 a) (ii) will not apply if the audit is initiated by a regulator or is requested due to a Personal Data Breach. You will cover the costs of the audit, unless it is shown that our Processing of Personal Data does not comply with Data Protection Laws, in accordance with Section 11 c) below, in which case we will bear the costs of the audit.

b) We will provide to you, your auditors, and regulators reasonable assistance to perform an audit, including (where applicable) permitting access to the premises and facilities under our control (or that we are permitted to provide access to) from which the Services will be performed; the systems (including software, networks, firewalls, and servers) used to perform the Services; and data, records, manuals, and other information relating to the Services. We will not be required to give you or auditors any access or information that may cause us to compromise our own internal, legal, or regulatory compliance obligations; is subject to confidentiality obligations with our customers, vendors, or other third parties; or is commercially sensitive (such as trade secrets).

c) If an audit shows that our Processing of Personal Data does not comply with Data Protection Laws, the Parties will discuss that finding and we will take any required corrective actions to achieve compliance to the reasonable satisfaction of the auditor.

d) Without prejudice to the rights granted in this Section 11, if the requested audit scope is addressed in a SOC, ISO, or similar audit report issued by a qualified third-party auditor within the prior 12 months and we makes such report available to you confirming there are no known material changes in the controls audited, you agree to accept the findings presented in the third-party audit report in lieu of requesting an audit of the same controls covered by the report.

12. Obligations upon Termination. Upon termination or expiration of the Agreement and this DPA, and, upon your written request, we will return the Personal Data and all copies to you in machine readable format and/or will securely delete the Personal Data and all existing copies in accordance with the Agreement, except if continued storage is required and permitted under Data Protection Laws. In such case, we will inform you of such legal obligation and keep the Personal Data confidential.

13. LIMITATION OF LIABILITY. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, AND EXCEPT AS SPECIFICALLY PROVIDED IN THE STANDARD CONTRACTUAL CLAUSES AS APPLICABLE, THE TOTAL AGGREGATE LIABILITY OF EACH PARTY AND ITS AFFILIATES ARISING OUT OF OR RELATED TO THIS DPA, IS SUBJECT TO THE LIMITATION OF LIABILITY SECTION OF THE AGREEMENT, AND ANY REFERENCE IN SUCH SECTION TO THE LIABILITY OF A PARTY MEANS THE AGGREGATE LIABILITY OF THAT PARTY AND ALL OF ITS AFFILIATES UNDER THE AGREEMENT AND DPA TOGETHER. FOR THE AVOIDANCE OF DOUBT, THIS LIMITATION DOES NOT APPLY TO DATA SUBJECT RIGHTS PROVIDED FOR UNDER APPLICABLE DATA PROTECTION LAWS.

14. GENERAL PROVISIONS

a) Governing Law; Venue; Jurisdiction. Without prejudice to the provisions of the relevant Standard Contractual Clauses addressing the law that governs them, this DPA will be governed by and construed in accordance with the laws that govern the Agreement. The venue and dispute resolution provisions under the Agreement will also apply to disputes and claims under this DPA.

b) Entire Agreement/Order of Precedence. This DPA constitutes the entire agreement between the Parties with respect to its subject matter and supersedes all prior understandings regarding such subject matter, whether written or oral. If a conflict exists between this DPA and the Agreement regarding the subject matter of this DPA, the terms of this DPA will govern. If a conflict exists between this DPA and the Standard Contractual Clauses regarding the subject matter of this DPA, the applicable Standard Contractual Clauses will govern.

c) Amendment. No amendment or modification of this DPA will be binding unless in writing and signed by the Parties.

d) Waiver. Any waiver by a Party of a breach of any provision of this DPA will not operate as or be construed as a waiver of any further or subsequent breach.

e) Survival. Provisions of this DPA that by their nature are to be performed or enforced following any termination of this DPA will survive such termination.

f) Assignment. We may assign this DPA to an Affiliate or in connection with a merger, acquisition, sale, or

other transfer of substantially all our assets, including to Jamf Software LLC or any Jamf Affiliate.

g) Binding Effect. This DPA will be binding upon and inure to the benefit of the Parties, their successors, and permitted assigns.

h) Unenforceability and Severability. If for any reason, a court of competent jurisdiction or duly appointed arbitrator finds any provision or portion of this DPA to be unenforceable, the remainder of this DPA will continue in full force and effect.

i) Translations. If this DPA is translated into languages other than English, the English version will control.

j) Headings. The headings are for convenience only and do not affect the interpretation of this DPA.

k) Counterparts. This DPA may be executed by electronic signature and in counterparts, which together constitute one binding agreement.

l) Third-party Rights. Except to the extent expressly provided by any of the Standard Contractual Clauses with respect to Data Subjects, this DPA does not give rise to any rights for third parties to enforce any term of this DPA.

SCHEDULE 1: DETAILS OF PROCESSING

This Schedule forms part of the DPA and provides the details required by Article 28(3) of the GDPR and Annex I to the Standard Contractual Clauses.

A. List of Parties

(1) **Data exporter(s)**: Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union:

Name: _____ or as set out in the Agreement/ Order Form.

Address: _____or as set out in the Agreement/Order Form.

Contact person's name, position, and contact details: _____or as set out in the Agreement/Order Form.

Activities relevant to the data transferred under these Clauses: Use of Identity

Automation Services.

Signature and date: _____or as accepted in the Agreement/Order Form.

Role (controller/processor): Controller

(2) **Data importer**:

Name: Identity Automation Systems, LP (a Jamf company)

Address: 100 Washington Ave, Suite 900
Minneapolis, MN 55401

Contact person's name, position, and contact details: Justin Francis, Vice President, Enterprise Risk & Compliance; privacy@jamf.com; +1 612-605-6625

Activities relevant to the data transferred under these Clauses: Identity Automation's provision of Services under the Agreement

Signature and date: _____ 06-01-2025

Role (controller/processor): Processor

B. Description of Transfer

Item	Description
Subject matter	Provision of Services to Customer under the Agreement
Duration	For the term of the Agreement plus the data retention period specified in Section 12 of the Agreement.
Nature and purpose	Processing of Personal Data as necessary to provide identity lifecycle management, access governance, authentication (including SSO and MFA), rostering, student-teacher portal, threat detection and response, and related Services
Frequency	Continuous, related to the nature of the Services
Categories of Data Subjects	Any individual whose data is managed by the Customer, including but not limited to employees, contractors, students and their parents or guardians of Customer, as applicable.

Types of Personal Data	Names, user identifier, IP addresses, telephone numbers, computer names, job titles and functions, email addresses, group and role membership, authentication credentials, entity identifier, grade level, class assignments, and other contact information and other education-related data as determined by Customer's configuration of the Services.
Sensitive data / special categories	Not Processed by default. Depending on Customer's use and configuration of the Services, Personal Data may include special categories of data as defined under Article 9 GDPR determined by Customer's deployment.
Retention post-termination	90 days. Then return or deletion per Section 7.6 of the Agreement.
Competent supervisory authority	Per Clause 13(a) of the EEA SCCs

SCHEDULE 2: AUTHORISED SUB-PROCESSORS

Rapid Identity Cloud Identity and Access Management (IAM) platform uses the following Sub-processors for the Services provided under the Agreement:

https://www.identityautomation.com/hubfs/PDFs/IA.Sub-processors.pdf?hsLang=en

SCHEDULE 3: TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES

This Schedule describes the minimum technical and organizational security measures implemented by Identity Automation in connection with the processing of Personal Data. These measures also serve as Annex II to the Standard Contractual Clauses.

We will take all reasonable measures required to ensure Processing of Personal Data is done in accordance with applicable Data Protection Laws and will have the required technical and organizational measures in place to ensure this. Considering the state of technological development and the cost of implementing such measures, we will ensure a level of security appropriate to the harm that might result from unauthorized or unlawful Processing or accidental loss, destruction, or damage, considering the nature of the Personal Data to be protected.

We will implement the following measures:

1. **Information Security Policies and Measures.**

   a) Policies. We will document information security policies and senior management will approve them.

   b) Review of the Policies. We will review information security policies at least annually, or promptly after we make any material changes to them to confirm applicability and effectiveness. We will not make changes to the policies that would materially degrade our security obligations.

   c) Information Security Reviews. We will independently review our approach to managing information security and its implementation (i.e., control objectives, controls, policies, processes, and procedures for information security) at planned intervals or when significant changes occur.

   d) Disaster Recovery. During the Term of the Agreement, we will maintain a disaster recovery (DR) or high availability (HA) solution and related plan that is consistent with industry standards for the Services we provide to you. We will test the DR or HA solution and related plan at least once annually. In addition, the solution and related plan will ensure:

      i) that we can restore installed systems used to provide Services in case of interruption;

      ii) that we can restore the availability and access to Customer Content in a timely manner if there is a physical or technical incident; and

      iii) the ongoing confidentiality, integrity, availability, and resilience of systems we use to provide Services.

   e) Testing. We will maintain a process for regularly testing the effectiveness of the technical and organizational measures for ensuring the security of the Processing of Customer Content.

2. **Information Security Framework.**

   a) Security Accountability. We will assign one or more security officers who will be responsible for coordinating and monitoring all information security functions, policies, and procedures.

   b) Security Roles and Responsibility. We will have confidentiality agreements with our personnel, contractors and agents who provide Services under the Agreement.

   c) Risk Management. We will perform appropriate information security risk assessments as part of an ongoing risk governance program with the following objectives (i) recognize risk, (ii) assess the impact of risk, and (iii) where risk reduction or mitigation strategies are identified and implemented, effectively manage the risk with recognition that the threat landscape constantly changes.

3. **Human Resource Security.**

   a) Security Training. We will provide appropriate security awareness, education, and training to all our personnel and contractors with access to the Services we provide to you.

   b) Background Screening. We will perform background checks on our personnel who are part of teams managing our hosting infrastructure and on personnel or agents who will provide Services at your premises, if applicable. We will perform background checks in accordance with applicable law and our

background screening policies and procedures. We will only permit individuals who have passed background checks to provide Services at your premises or manage our hosted infrastructure.

4. Asset Management

a) Asset Inventory

i) We will maintain an asset inventory of all media and equipment where Customer Content is stored. We will restrict access to such media and equipment to authorized personnel of Identity Automation. We will prevent the unauthorized reading, copying, modification, or removal of data media.

ii) We will classify Customer Content so that it is properly identified and will appropriately restrict access to Customer Content. Specifically, we will ensure that no person we appoint to Process Customer Content will do so unless that person:

1) has a need to access Customer Content for the purpose of performing our obligations under the Agreement;

2) has been authorized by us in a manner consistent with our information security policies;

3) has been fully instructed by us in the procedures relevant to the performance of our obligations under the Agreement, in particular the limited purpose of Processing Customer Content; and

4) is aware that they are prohibited from copying any Customer Content you transmit to us, provided, however, that we may retain copies of Customer Content in our servers for backup and archive purposes until completion of the Agreement.

iii) We will further maintain measures to ensure that the persons we appoint to Process Customer Content will prevent the unauthorized input of Customer Content and the unauthorized inspection, modification, or deletion of stored Customer Content.

iv) We will maintain an appropriate approval process whereby approval is provided to personnel, contractors, and agents prior to storing Customer Content on portable devices or remotely accessing Customer Content. All approvals will be subject to measures designed to prevent the unauthorized reading, copying, modification, or deletion of Customer Content during transfers of such content or during transportation of data media. If remote access is approved and granted, our personnel, agents, and contractors will use multi-factor authentication. Multi-factor authentication may include techniques such as the use of cryptographic certificates, one-time password ("**OTP**") tokens, or biometrics.

b) Security of Components. We agree to appropriately inventory all Software components (including open-source software) used with our Software and Services. We will assess whether any such software components have any security defects and/or vulnerabilities that could lead to unauthorized disclosure of Customer Content. We will perform such assessment prior to delivery of, or providing you access to, the Software and Services and on an on-going basis thereafter during the term of the Agreement. We agree to remediate any security defect or vulnerability we detect in a timely manner.

5. Access Control.

a) Policy.

i) We will maintain an appropriate access control policy that is designed to restrict access to Customer Content and Identity Automation assets to authorized personnel, agents, and contractors. To ensure clarity, all references to user accounts and passwords in this Section 5 relate only to our users, user accounts, and passwords. This Section 5 does not apply to your access to and use of the Software and Services, your user accounts, or your passwords.

b) Authorization.

i) We will maintain user account creation and deletion procedures for granting and revoking access to all assets, Customer Content, and all Identity Automation internal applications while providing

Software and Services under the Agreement. We will assign an appropriate authority to approve creation of user accounts or elevated levels of access for existing accounts.

ii) We will maintain and update records of employees and contractors who are authorized to access systems that are involved in providing Software and Services to you and review such records at least quarterly. Administrative and technical support personnel, agents, or contractors will only be permitted to have access to such data when required; provided such personnel, agents, or contractors comply with our applicable technical and organizational measures.

iii) We will ensure the uniqueness of user accounts and passwords for everyone. Individual user accounts will not be shared.

iv) We will remove access rights of personnel and contractors to assets that store Customer Content upon termination of their employment, contract, or agreement within 24 hours, or adjust access upon change of personnel role.

c) Authentication.

i) We will use industry standard capabilities to identify and authenticate personnel, agents, and contractors who attempt to access information systems and assets.

ii) We will maintain industry standard practices to deactivate passwords that have been corrupted or disclosed.

iii) We will monitor for repeated access attempts to information systems and assets.

iv) We will maintain industry standard password protection practices that are designed to maintain the confidentiality and integrity of passwords generated, assigned, distributed, and stored in any form.

v) We will use multi-factor authentication for all administrative access, including domain and cloud portal administrative access. Multi-factor authentication may include techniques such as the use of cryptographic certificates, OTP tokens, or biometrics.

d) Data-processing Equipment.

i) We will deny unauthorized persons access to systems and equipment used for processing Customer Content ("**Data-Processing Equipment**").

ii) We will prevent the use of automated Data-Processing Equipment by unauthorized persons using data communication equipment.

iii) We will ensure that persons authorized to use an automated Data-Processing Equipment only have access to the Customer Content covered by their access authorization.

iv) We will ensure that it is subsequently possible to verify and establish which Customer Content has been put into automated Data-Processing Equipment, when it was added, and by whom the input was made.

6. **Cryptography**. We will maintain policies and standards regarding the use of cryptographic controls that we implement to protect Customer Content. Such protections will include the pseudonymization and encryption of Personal Data, as further detailed below in Section 9. We will implement industry standard key management policies and practices designed to protect encryption keys for their entire lifetime.

7. Physical and Environmental Security.

a) Physical Access to Facilities. We will limit access to facilities where systems that are involved in providing the Services are located to identified personnel, agents, and contractors.

b) Protection from Disruptions. We will use reasonable efforts, and, to the best of our ability and to the extent within our control, protect equipment from power failures and other disruptions caused by failures in supporting utilities.

c) Secure Disposal or Reuse of Equipment. We will verify that all Customer Content has been deleted or securely overwritten from equipment containing storage media using industry standard processes prior to disposal or reuse.

8. Operations Security

a) Operations Policy. We will maintain appropriate operational and security operating procedures and such procedures will be made available to all our personnel who require them.

b) Protections from Malware. We will maintain anti-malware controls that are designed to protect systems from malicious software, including malicious software that originates from public networks.

c) Configuration Management. We will have policies that govern the installation of software and utilities by personnel.

d) Change Management. We will maintain and implement procedures to ensure that only approved and secure versions of the code, configurations, systems, and applications will be deployed in the production environment(s).

e) Encryption of Data. We will deploy encryption solutions with no less than 256-bit Advanced Encryption Standard ("**AES**") encryption.

f) Systems. We will ensure that the functions of the systems used to provide Services perform, that the appearance of faults in the functions is reported, and that stored Customer Content cannot be corrupted by means of a malfunctioning of such systems.

9. Communications Security.

a) Information Transfer.

i) With respect to Hosted Services, Customer Content is encrypted in-transit to the Hosted Services and maintained in encrypted storage. We will use industry standard encryption to encrypt Customer Content.

ii) We will restrict access through encryption to Customer Content stored on media that is physically transported from our facilities.

iii) We will ensure that it is possible to verify and establish the extent to which Customer Content has been or may be transmitted or made available using data communication equipment.

b) Security of Network Services.

i) We will ensure that industry standard security controls and procedures for all network services and components are implemented whether such services are provided in-house or outsourced.

c) Intrusion Detection.

i) We will deploy intrusion detection or intrusion prevention systems for all systems used to provide Services to you to provide continuous surveillance for intercepting and responding to security events as they are identified and update the signature database as soon as new releases become available for commercial distribution.

d) Firewalls.

i) We will have appropriate firewalls in place which will only allow documented and approved ports and services to be used. All other ports will be in a deny-all mode.

10. System Acquisition, Development, and Maintenance.

a) Workstation Encryption. We will require hard disk encryption of at least 256-bit AES encryption on all workstations and/or laptops used by personnel, contractors, and agents where such personnel are Processing Customer Content.

b) Application Hardening.

i) We will maintain and implement secure application development policies, procedures, and standards that are aligned to Industry Standard practices such as the SANS Top 25 Security Development Techniques or the OWASP Top Ten project.

ii) All personnel responsible for secure application design, development, configuration, testing, and deployment will be qualified to perform the Services and receive appropriate training regarding our secure application development practices.

c) System Hardening.

i) We will establish and ensure the use of standard secure configurations of operating systems. Images should represent hardened versions of the underlying operating system and the applications installed on the system. Hardening includes removal of unnecessary accounts (including service accounts), disabling or removal of unnecessary services, applying patches, closing open and unused network ports, and implementing intrusion detection systems and/or intrusion prevention systems. These images should be validated on a regular basis to update their security configuration as appropriate.

ii) We will perform periodic (at least quarterly) access reviews for system administrators for all supporting systems requiring access control.

iii) We will implement patching tools and processes for both applications and operating system software. When outdated systems can no longer be patched, we will update to the latest version of application software. We will remove outdated, unsupported, and unused software from the system.

iv) We will limit administrative privileges to only those personnel who have both the knowledge necessary to administer the operating system and a business need to modify the configuration of the underlying operating system.

d) Infrastructure Vulnerability Scanning. We will scan our internal environment (e.g., servers, network devices, etc.) related to the Services monthly and external environment related to the Services on a weekly basis. We will have a defined process to address any findings but will ensure that any high-risk vulnerabilities are addressed no later than 30 days after discovery.

e) Application Vulnerability Assessment. We will perform an application security vulnerability assessment prior to any new public release. We will have a defined process to address any findings but will ensure that any high-risk vulnerabilities are addressed within 30 days of discovery.

f) Penetration Tests and Security Evaluations of Websites. We will perform a comprehensive penetration test and security evaluation of all systems and websites involved in providing Services on a recurring basis at least once annually. Additionally, we will have an industry-recognized independent third party perform an annual test. We will have a defined process to address any findings but will ensure that any high-risk vulnerabilities are addressed within 30 days of discovery. Upon your written request, but no more than once per year, we will provide an assertion statement to validate the completion of the independent third-party penetration test and attest to the fact that we maintain a process to address findings.

11. Identity Automation Relationships.

a) If we must use a third-party application or service to provide the Services, our contract with that third-party vendor must clearly outline security requirements for the third-party vendor consistent with the security requirements of this Schedule 3. In addition, service level agreements with the third party must be clearly defined.

b) Any third-party gaining access to our systems must be covered by a signed agreement containing confidentiality and security provisions consistent with the confidentiality and security requirements of the Agreement and this Schedule 3.

c) Identity Automation will perform quality control and security management oversight of outsourced software development.