Delinea
Defining the boundaries of access

Data Processing Addendum

This Data Processing Addendum ("**DPA**") is incorporated into and forms part of the Master Subscription and License Agreement ("**MSLA**"), End User License Agreement (together with attachments thereto, "**EULA**") or other end user agreement or terms of service ("**Agreement**") by and between Delinea Inc. ("**Vendor**") and Customer (as defined in the Agreement) pursuant to which Customer purchases subscriptions to access and use Delinea Cloud Services (as defined below). This DPA sets out the requirements for processing of Personal Data by Vendor on behalf of Customer for the purposes of providing Cloud Services. For clarity, any regulatory requirements referenced herein shall apply to Customer only to the extent that Vendor's processing of Customer's Personal Data is subject to (and within the jurisdictional reach of) such regulatory requirements.

1. **Definitions**

Adequate Country	means a country or territory recognised as providing an adequate level of protection for Personal Data under an adequacy decision made, from time to time, by (as applicable) (a) the Information Commissioner's Office and/or under applicable UK law (including the UK GDPR), or (b) the European Commission under the EU GDPR, or (iii) the Swiss Federal Data Protection Authority under Swiss Data Protection Law.
Controller	has the meaning ascribed to it in the Data Protection Laws. The term "Controller" shall also include a "business" as defined in the CCPA and the CPRA and analogous terms in the applicable Data Protection Laws.
Data Protection Laws	means all data protection and privacy laws, as may be amended, superseded or replaced from time to time, that are applicable to a party and its Processing of Personal Data under the Agreement, including, where applicable, and without limitation: (a) in the European Union, the General Data Protection Regulation 2016/679 (the "**GDPR**"), (b) in the UK, the UK General Data Protection Regulation 2016/679, as implemented by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 and the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020 (the "**UK GDPR**") and the Data Protection Act 2018, (c) Swiss Data Protection Law, (d) United States federal and/or state data protection or privacy statutes, including but not limited to the California Consumer Privacy Act of 2018 ("**CCPA**") and the California Privacy Rights Act of 2020 ("**CPRA**"), and/or (e) Any other data protection and privacy laws applicable to a party and its Processing of Personal Data in connection with the Agreement.
Data Subject	has the meaning ascribed to it in the Data Protection Laws.
Data Subject Request	means a request from or on behalf of a data subject to exercise any rights in relation to their Personal Data under Data Protection Laws.
Delinea Cloud Services	refers to cloud-hosted solutions offered by Delinea for end user internal access and use in accordance with associated product documentation under

	one, two or three-year services subscriptions. Delinea Cloud Services includes the Fastpath Solutions.
EEA	means the European Economic Area.
EU Clauses	means the standard contractual clauses for international transfers of personal data to third countries set out in the European Commission's Decision 2021/914 of 4 June 2021 (at http://data.europa.eu/eli/dec_impl/2021/914/oj) incorporating Module Two for Controller to Processor transfers and which form part of this DPA in accordance with Schedule 3.
Fastpath Solutions	means those cloud services offerings for separation of duties or identity governance and administration that Vendor references as a Fastpath Solutions service in order documentation.
Personal Data	has the meaning ascribed to it in the Data Protection Laws and, for the DPA, refers to Personal Data that is uploaded into the Cloud Services or in connection with support services by Customer and accessed, stored, or otherwise processed by Vendor as a processor.
Processor	has the meaning ascribed to it in the Data Protection Laws. The term "Processor" shall also include a "service provider" as defined in the CCPA and CPRA and analogous terms in the applicable Data Protection Laws.
Security Breach	means any breach of security or other action or inaction leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data by any of Vendor's staff or sub-processors, or any other identified or unidentified third party.
Supervisory Authority	means in the UK, the Information Commissioner's Office ("**ICO**") (and, where applicable, the Secretary of State or the government), and in the EEA, an independent public authority established pursuant to the GDPR.
Swiss Data Protection Law	means the Swiss Federal Data Protection Act of 19 June 1992 and, when in force, the Swiss Federal Data Protection Act of 25 September 2020 and its corresponding ordinances as amended, superseded or replaced from time to time.
Swiss Addendum	means the addendum set out in Schedule 3.
UK	means the United Kingdom.
UK Approved Addendum	means the template Addendum B.1.0 issued by the UK's Information Commissioner's Office and laid before Parliament in accordance with s119A of the Data Protection Act 2018 of the UK on 2 February 2022, and expected to be in force on 21 March 2022.
UK Mandatory Clauses	means the Mandatory Clauses of the UK Approved Addendum, as updated from time to time and/or replaced by any final version published by the Information Commissioner's Office.
UK GDPR	means the EU GDPR as implemented into the law of the United Kingdom by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 and the Data Protection, Privacy and

Electronic Communications (Amendments etc) (EU Exit) Regulations 2020 and the Data Protection Act 2018.

2. **Roles & compliance with Data Protection Laws**

   a. Customer is the controller of Personal Data, and Vendor is the processor of Personal Data. Each party will comply (and will procure that its personnel comply and use commercially reasonable efforts to procure that its sub-processors comply), with Data Protection Laws applicable to such party in the processing of Personal Data. As between the parties, Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which the Personal Data was acquired.

   b. *Description of Processing*. The subject matter, nature, and specific purposes of the processing. duration, types of Personal Data and categories of Data Subject are as set out in Schedule 1.

3. **Processing by Vendor**. As a processor, Vendor will only process Personal Data (i) to provide the Cloud Services and related support services to Customer or (ii) per Customer's instructions in writing or via the Cloud Services and related support services. In providing the Cloud Services and related support services to Customer, Vendor will not process Customer Personal Data in a manner that is prohibited by applicable Data Protection laws or outside the direct business relationship between the parties. In addition, Vendor will not sell or share Customer Personal Data as the terms are defined in applicable Data Protection Laws. Vendor will notify Customer (unless prohibited by applicable law) if it is required under applicable law to process Personal Data other than pursuant to Customer's instructions. As soon as reasonably practicable upon becoming aware, Vendor will notify the Customer if, in Vendor's opinion, any instructions provided by the Customer under this Clause 3 infringe applicable Data Protection Laws, or it can no longer meet its obligations under applicable Data Protection Laws. Upon termination of the Agreement and upon written request of the Customer, Vendor will return or delete the Personal Data, unless required by law to continue to store a copy of the Personal Data.

4. **Technical and Organisational Security Measures**

   a. Vendor will implement appropriate technical and organisational measures of security appropriate to the risks that are presented by the processing of Personal Data, in particular protection against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or use of, or access to Personal Data as set out in Annex II of Schedule 4.
   b. Vendor will take reasonable steps to ensure that only authorised personnel have access to Personal Data and that any persons whom it authorises to access the Personal Data are under obligations of confidentiality.

5. **Security Breaches, Data Subject Requests & Further Assistance**

   a. *Security Breaches*. In the event of a Security Breach concerning Personal Data processed by Vendor on behalf of Customer, Vendor shall take appropriate measures to address the Security Breach, including measures to mitigate its adverse effects. Vendor will notify Customer of any Security Breach without undue delay and within forty-eight (48) hours after becoming aware of the Security Breach.
   b. *Data Subject Requests*. To the extent legally permitted, Vendor will promptly notify Customer if it receives a Data Subject Request that is identified as or determined to be related to Customer. Vendor will not respond to a Data Subject Request, provided that Customer agrees Vendor may at its discretion respond to confirm that such request relates to Customer. Customer acknowledges and agrees that the Cloud Services and related support services may include features which will allow Customer to manage Data Subject Requests directly through the Cloud Services without additional assistance from Vendor. If Customer does not have the ability to address a Data Subject Request, Vendor will, upon Customer's

written request, provide reasonable assistance to facilitate Customer's response to the Data Subject Request to the extent such assistance is consistent with applicable law.

c. *Further Assistance*. Taking into account the nature of processing and the information available to Vendor, Vendor will provide such assistance as Customer reasonably requests in relation to Customer's obligations under Data Protection Laws with respect to (i) data protection impact assessments, (ii) notifications to the Supervisory Authority under Data Protection Laws and/or communications to data subjects by the Customer in response to a Security Breach, or (iii) Customer's compliance with its obligations under Data Protection Laws (as applicable) with respect to the security of processing.

6. **Sub-processing**

a. Customer grants a general authorisation to Vendor (i) to appoint one or more of its Affiliates as sub-processors and (ii) to appoint third party data center operators, outsourced support providers, and/or third-party technology providers as sub-processors to support the performance of the Cloud Services and support services, subject to the terms herein. As used herein, the term "**Affiliate**" means any person or entity directly or indirectly controlling, controlled by, or under common control with Vendor.

b. Vendor will maintain a list of sub-processors at the following URL: https://delinea.com/sub-processors/, and will add the names of new and replacement sub-processors to the list prior to their starting sub-processing of Personal Data. Customer can subscribe to updates as instructed at https://delinea.com/privacy-notifications. If the Customer has a reasonable legal objection to any new or replacement sub-processor, it shall notify Vendor of such objections in writing setting forth the legal requirements that form the basis of the objection within ten (10) days of Vendor's notice of any new or replacement sub-processor and the parties will seek to resolve the matter in good faith. If Vendor is able to provide Cloud Services and support services to Customer in accordance with the Agreement and applicable legal requirements and decides in its discretion to do so, then Customer will have no further rights under this Clause 6.b in respect of the proposed use of the sub-processor.

c. Sub-processors engaged by Vendor to process Personal Data in connection with the Cloud Services or support services must have entered into contractual terms which impose on such sub-processor terms substantially no less protective of Personal Data than those imposed on Vendor in this DPA, and Vendor shall remain responsible and liable for such sub-processor's processing of Personal Data in accordance with such terms.

7. **International Transfers**

a. Customer agrees that its use of the Cloud Services and related support services will involve the transfer of Personal Data to, and processing of Personal Data in, the countries in which Vendor and Vendor's sub-processors are based. Vendor may process and permit the processing of Personal Data in another country outside the EEA or the UK (except if in an Adequate Country) in conformity with this Section 7.

b. *UK transfers:*

(i) To the extent Personal Data is transferred to Vendor and processed by or on behalf of Vendor outside the UK (except if in an Adequate Country) in circumstances where such transfer would be prohibited by UK GDPR in the absence of a transfer mechanism, the parties agree that the EU Clauses subject to the UK Approved Addendum will apply. The UK Approved Addendum is incorporated into this DPA.

(ii) Schedule 2 references the information required by Tables 1 to 4 inclusive of the UK Approved Addendum.

c. *EU transfers:*

(i) To the extent Personal Data is transferred to Vendor and processed by or on behalf of Vendor outside the EEA (except if in an Adequate Country) in circumstances where such transfer would be prohibited by EU GDPR in the absence of a transfer mechanism, the parties agree that the EU Clauses will apply in respect of that processing and are incorporated into this DPA in accordance with Schedule 3.

(ii) Schedule 3 contains the information required by the EU Clauses.

d. *Swiss transfers*

(i) To the extent Personal Data is transferred to Vendor and processed by or on behalf of Vendor outside Switzerland (except if in an Adequate Country) in circumstances where such transfer would be prohibited by Swiss Data Protection Laws in the absence of a transfer mechanism, the parties agree that the EU Clauses subject to the Swiss Addendum will apply in respect of that processing. The Swiss Addendum is incorporated into this DPA.

(ii) Schedule 3 contains the information required by the EU Clauses, including for the purposes of transfers to which this clause 7.d applies.

e. Vendor may (i) replace the EU Clauses, the Swiss Addendum and/or the UK Approved Addendum generally or in respect of the EEA, Switzerland and/or the UK (as appropriate) with any alternative or replacement transfer mechanism in compliance with applicable Data Protection Laws, including any further or alternative standard contractual clauses approved from time to time and (ii) make reasonably necessary changes to this DPA for new or revised transfer mechanisms or new standard contractual clauses, provided their content is in compliance with the Data Protection Laws. Customer may subscribe to notifications of such changes by following the instructions at https://delinea.com/privacy-notifications.

8. **Audit and Records**

a. Customer may take reasonable and appropriate steps to verify Vendor's compliance with applicable Data Protection Laws and this DPA as described in this Clause 8. Vendor shall maintain such business records and information in Vendor's possession or control with a view to demonstrating Vendor's compliance with the obligations of data processors under applicable Data Protection Law in relation to its processing of Personal Data. Whenever required by an audit or inspection request of any Supervisory Authority or otherwise under applicable Data Protection Laws (an "**Audit Request**"), Vendor shall make available those business records and information reasonably determined by Vendor to be legally required and necessary to meet the Audit Request. Customer shall ensure Vendor receives reasonable prior notice of at least thirty (30) days as to any Audit Request and provide Vendor with all relevant excerpts of the formal Audit Request that may be relevant to the records Vendor may be required to produce. Vendor shall be entitled to make legal objections to Audit Requests to protect sensitive materials and may exercise all available legal rights to protect its business records and information in connection with any Audit Request, including without limitation to redact records, require confidential treatment, require non-disclosure agreements, require verification of audit requirements and limit access to records. Vendor will take reasonable and appropriate steps to remediate findings of non-compliance of applicable Data Protection Law or this DPA.

9. **General**

a. *Effective Date.* This DPA is effective as of the later of November 25, 2024 or the effective date of the Agreement.

b. *Incorporation of Updates to DPA.* This DPA may from time to time be updated by Vendor to reflect regulatory and compliance changes, Vendor process enhancements, and similar changes ("**DPA Updates**") that Vendor deems necessary and advisable. DPA Updates shall be deemed automatically

incorporated into and made a part of this DPA upon Vendor's publication of this DPA on its website (https://delinea.com/dpa) incorporating the DPA Update. Customer shall not dispute any DPA Updates which Vendor reasonably deems are necessary or advisable to comply with applicable law; provided, no DPA Update that will materially adversely impact Customer's rights under this DPA shall become effective as to Customer without an opportunity for Customer to review and discuss such DPA Update with Vendor. Customer can subscribe to DPA Updates at https://delinea.com/privacy-notifications. Upon request of Customer, Vendor and Customer will execute a written amendment reflecting the DPA Updates.

c. *Conflicts*. This DPA is without prejudice to the rights and obligations of the parties under the Agreement which shall continue to have full force and effect. In the event of any conflict between the terms of this DPA and the terms of the Agreement, the terms (including definitions) of this DPA shall prevail so far as the subject matter concerns the processing of Personal Data; provided, however, in the event Customer and Vendor have a separate executed data processing addendum effective prior to November 18, 2024, such other data processing addendum shall prevail to the extent of any provision that directly conflicts with this DPA. This DPA sets out all terms and conditions that have been agreed between the parties in relation to the subjects covered by it.

d. *Limitation of Liability*. Vendor's maximum aggregate liability to Customer under or in connection with this DPA shall not under any circumstances exceed the maximum aggregate liability of Vendor to the Customer as set out in the Agreement. Nothing in this DPA will limit Vendor's liability in respect of personal injury or death in negligence or for any other liability or loss which may not be limited by agreement under applicable law.

e. *Governing Law; Venue*. Without prejudice to the provisions of the EU Clauses, Swiss Addendum and the UK Approved Addendum addressing the law which governs them, this DPA shall be governed by and construed in accordance with the laws which govern the Agreement and the venue and dispute resolution provisions under the Agreement shall also apply to disputes and claims under this DPA.

[Schedules to DPA Follow]

Delinea
Defining the boundaries of access

SCHEDULE 1

Data Processing Details

For the purposes of Clause 3 of the DPA and Schedules 2 and 3 to the DPA, the parties set out below a description of the Personal Data being processed by Vendor under the Agreement and further details required pursuant to the Data Protection Laws.

Delinea Cloud Services (excluding Fastpath Solutions)

Subject Matter of the Processing	Vendor's provision of the Cloud Services and related support services to Customer.
Nature and purpose of Processing	The collection and storage of Personal Data pursuant to providing the Cloud Services and related support services to Customer.
Types of Personal Data	Personal Data that Customer in its discretion uploads into the Cloud Services and submits in using the support services, consisting of the following types at Customer's discretion: • Username, account passwords, old passwords, old password hashes, user display name, one-time passcode for multi-factor authentication; and • Universal second factor security keys, hashed passwords; and • The history of when passwords are checked out and used; and • Name, email, and phone numbers; and • Device IP address, device UDID and system generated unique user-ID; and • User security question/answer; and • User login time history, login geographical location history, login success/failure/failure reason history; and • Session recordings elected by Customer in connection with Cloud Services or support services; and • Device serial number, IMEI, MAC address, SIM ICCID number; and • Derived credentials.
Sensitive Personal Data and applied restrictions	None
Categories of Data Subject	Data Subjects may include any end users (including without limitation Customer's employees, contractors, or other personnel) about whom Personal Data is provided to Vendor via the Cloud Services and related support services by, or at the direction of, Customer.
Duration of Processing	For the duration of the Agreement, or until the processing is no longer necessary for the purposes.

Fastpath Solutions:

Subject Matter of the Processing	Vendor's provision of the Fastpath Solutions and related support services to Customer.

Nature and purpose of Processing	The collection and storage of Personal Data pursuant to providing the Fastpath Solutions and related support services to Customer.
Types of Personal Data	Personal Data that Customer in its discretion uploads into the Fastpath Solutions and submits in using the support services, consisting of the following types at Customer's discretion: • User name • System ID and device data • Email address • Phone number and business address • Job title • Descriptions associated with job title • Other personal data types uploaded or designated by Customer for use of the Fastpath Solutions.
Sensitive Personal Data and applied restrictions	None
Categories of Data Subject	Data Subjects may include any end users (including without limitation Customer's employees, contractors, or other personnel) about whom Personal Data is provided to Vendor via the Fastpath Solutions and related support services by, or at the direction of, Customer.
Duration of Processing	For the duration of the Agreement, or until the processing is no longer necessary for the purposes.

Delinea
Defining the boundaries of access

SCHEDULE 2

UK Transfers

For the purposes of the UK Approved Addendum,

1. the information required for Table 1 is contained in Schedule 1 of this DPA and the start date shall be deemed dated the same date as the EU Clauses;

2. in relation to Table 2, the version of the EU Clauses to which the UK Approved Addendum applies is Module Two for Controller to Processor;

3. in relation to Table 3, the list of parties and description of the transfer are as set out in Annex I of Schedule 4 of this DPA, Vendor's technical and organisational measures are set in Annex II of Schedule 4 of this DPA, and the list of Vendor's sub-processors shall be provided pursuant to Clause 6 of this DPA; and

4. in relation to Table 4, neither party will be entitled to terminate the UK Approved Addendum in accordance with clause 19 of the UK Mandatory Clauses.

SCHEDULE 3

Swiss Addendum

In respect of transfers otherwise prohibited by Swiss Personal Data:

1. The FDPIC will be the competent supervisory authority;
2. Data subjects in Switzerland may enforce their rights in Switzerland under clause 18c of the EU SCCs, and
3. References in the EU SCCs to the EU GDPR should be understood as references to Swiss Data Protection Law insofar as the data transfers are subject to Swiss Data Protection Law.

Delinea
Defining the boundaries of access

SCHEDULE 4

EU Clauses

1. For the purposes of this Schedule 4, the EU Clauses (Module II), available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32021D0914&from=EN, shall be incorporated by reference to this Schedule 4 and the DPA and shall be considered an integral part thereof, and the parties' signatures in the Agreement (to which this DPA is attached as an Exhibit) shall be construed as the parties' signature to the EU Clauses. In the event of an inconsistency between the DPA and the EU Clauses, the latter will prevail.

2. For the purposes of the EU Clauses, the following shall apply:

   - Customer is the exporter and Vendor is the importer. Each party agrees to be bound by and comply with its obligations in its role as exporter and importer respectively as set out in the EU Clauses.
   - Clause 7 (Docking clause) shall be deemed as included.
   - Clause 9 (Use of sub-processors): OPTION 2 – GENERAL WRITTEN AUTHORISATION shall apply. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors as set out in Clause 6 of the DPA.
   - Clause 11 (Redress): optional clause (optional redress mechanism before an independent dispute resolution body) shall be deemed as not included.
   - Clause 13 (a) (Supervision).

   Competent Supervisory Authority

   Where Customer is established in an EU Member State, the supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer shall act as competent supervisory authority.

   Where Customer is not established in an EU Member State but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679, the supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established shall act as competent supervisory authority.

   Where Customer is not established in an EU Member State but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679, the supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behavior is monitored, are located, shall act as competent supervisory authority.

   - Clause 17 (Governing law): These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The parties agree that this shall be the law of Ireland.
   - Clause 18 (b) (Choice of forum and jurisdiction): The parties agree that any dispute between them arising from the EU Clauses shall be resolved by the courts of Ireland.

3. Any provision in the EU Clauses relating to liability of the parties with respect to each other shall be subject to the limitations and exclusions of the Agreement.

4. Any provision in the EU Clauses relating to the right to audit shall be interpreted in accordance with Clause 8 of the DPA and the Agreement.

Delinea
Defining the boundaries of access

ANNEX I to Schedule 4

A. LIST OF PARTIES

Data exporter(s):

Name: Customer name as set forth in the preamble of the Agreement.

Address: Customer address as set forth in the preamble of the Agreement.

Contact person's name, position and contact details: Customer privacy contact details as notified to Vendor at **dpo@delinea.com** or in accordance with the "Notices" provision of the Agreement, or if no privacy contact is so notified, the Customer name for general notices, as set forth under "Notices" in the Agreement.

Activities relevant to the data transferred under these Clauses: Data exporter will transfer Personal Data to the data importer as required for the provision of Cloud Services and related support services by the data importer under the Agreement and as set out in the DPA.

Signature and date: The Effective Date of the DPA (Clause 9.a.)

Role (controller/processor):

☒ Controller

☐ Processor

Data importer(s):

Name: Delinea Inc.

Address: 221 Main Street, Suite 1300, San Francisco, CA, 94105, United States

Contact person's name, position and contact details: Legal Department, Attention: DPO, Delinea Europe Ltd., 5 New Street Square, London, EC4A 3TW, United Kingdom; dpo@delinea.com.

Activities relevant to the data transferred under these Clauses: data importer will process personal data as required for the provision of Cloud Services and related support services under the Agreement and as set out in the DPA.

Signature and date: The Effective Date of the DPA (Clause 9.a.)

Role (controller/processor):

☐ Controller

☒ Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

See Schedule 1 to the DPA

Categories of personal data transferred

See Schedule 1 to the DPA

Sensitive data transferred (if applicable) and applied restrictions or safeguards

See Schedule 1 to the DPA

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

Transfers will occur from time to time as required during the course of the performance of the Cloud Services and related support services under the Agreement.

Nature of the processing

See Schedule 1 to the DPA

Purpose(s) of the data transfer and further processing

See Schedule 1 to the DPA

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

See Schedule 1 to the DPA

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

See Schedule 1 to the DPA

C. COMPETENT SUPERVISORY AUTHORITY

See Schedule 4 to the DPA

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL

See Schedule 4 to the DPA

ANNEX III – LIST OF SUB-PROCESSORS

See URL https://delinea.com/sub-processors/

Delinea
Defining the boundaries of access

Annex II of Schedule 4

Security Measures

This Annex II describes Vendor's security measures for delivery of Delinea Cloud Services (excluding Fastpath Solutions), including technical and organisational controls designed to: 1) protect Customer Data, including Personal Data, from unauthorised use, access, disclosure, or theft; and 2) maintain the confidentiality, integrity, and availability of Delinea Cloud Services and Customer Data, including Personal Data. Vendor's security measures for Delinea Cloud Services are subject to annual ISO 27001 and SOC 2 assessments and may be updated or modified from time to time, provided that such updates and modifications do not degrade or diminish the overall security of Delinea Cloud Services for Customer or Customer Data, including Personal Data.

Security Program Framework & Oversight

- Vendor maintains an Information Security Program ("ISP") utilizing industry recognized frameworks (*e.g.,* NIST, SOC 2, ISO 27001). Vendor's ISP leverages the Secure Controls Framework (SCF), a widely adopted overarching security and privacy framework enabling organizations to comply with multiple statutory, regulatory, and contractual requirements.

- Vendor's Security Steering Committee is primarily responsible for cyber risk management activities and oversight of the ISP and related security controls. The Security Steering Committee is chaired at the executive level by our Chief Information Officer (CIO)/Chief Information Security Officer (CISO) and is comprised of a cross-section of key functional leaders.

- ISP policies are reviewed annually by the Security Steering Committee. The security measures summarized in this Annex II are subject to annual ISO 27001 and SOC 2 assessments.

Shared Responsibility Model for SaaS

- Security in cloud computing is achieved through what is known as "shared responsibility." Vendor employs a "Shared Responsibility Model," which outlines the responsibilities of Vendor, Vendor's Cloud Service Providers (CSPs), and Vendor's customers as we work together to keep the platform reliable and secure.

  CSP: Security of the infrastructure (i.e., datacenter hardware and software, networking, and the datacenter's physical security.)

  Vendor: Security of the application portfolio (i.e., security of the software, data management, performing operations, and maintenance of assets in the cloud in accordance with Vendor policy and procedure.)

  Customer: Operating Delinea Cloud Services in accordance with the customer's own policies and procedures and within the terms of the Master Service Agreement with Vendor.

Identification & Authentication

- The customer governs the master encryption key and controls access to their tenant. Vendor does not require access to customer tenants in order to provide the Cloud Services.

- Vendor implements Role-Based Access Controls (RBAC) over Vendor personnel and resources.

- Authorised access by Vendor users to the Cloud Services environment requires two separate approvals, including management approval and forced use of Multi-Factor Authentication (MFA). Vendor does not permit default or guest user accounts.

- Vendor conducts periodic access reviews to ensure active accounts are valid and staff members possess access and permissions commensurate with their role.

- Vendor's password policy includes length, case, character type, and history requirements. Passwords must be changed every 90 days. Vendor also uses MFA, Single Sign-On (SSO), and VPN as further methods to control and protect access to the Cloud Services environment.

Endpoint Security

- Vendor ensures that endpoint devices connected to the Cloud Services are known, authorised, and appropriately protected from security threats.

- Endpoint controls include antimalware technologies to detect and eradicate malicious code, Data Loss Prevention (DLP) to ensure data does not leave the Cloud Services, and Mobile Device Management (MDM) to prevent unauthorised connections.

- Vendor utilizes current antivirus where feasible across compute and processing endpoints, including automated, multiple daily signature updates and centralized administration.

Cloud Security and Configuration Management

- Vendor operates a multitenant architecture and Customer Data processed on behalf of the Customer is kept logically and/or physically separated from other customers.

- Vendor ensures the security and resilience of Internet-accessible technologies through secure configuration management practices and monitoring for anomalous activity. Vendor addresses the risks associated with Internet-accessible technologies by hardening devices, monitoring system file integrity, enabling auditing, and monitoring for malicious activities.

Third-Party Management

- Vendor's third-party risk management program focuses on identifying, assessing, and mitigating cybersecurity and data protection risks associated with Third-Party Service Providers (TSP). TSP risk management activities include conducting annual due diligence on the subprocessors that support provision of the Cloud Services, including annual Transfer Impact Assessments where required.

- Vendor utilizes industry-leading cloud service providers Microsoft Azure (MS Azure) and Amazon Web Services (AWS) to host the Cloud Services.

- MS Azure and AWS are SOC 2 compliant and maintain various certifications that include controls and requirements related to physical security, environmental security, system availability, identity and access management, data isolation, encryption, virtualized redundancy, and continuous monitoring and testing. Additional information on appropriate security controls is available at:

  Microsoft Azure https://docs.microsoft.com/en-us/azure/compliance/

  Amazon Web Services (AWS) https://aws.amazon.com/compliance/programs/

Cryptographic Protections

- Vendor's SaaS communications are encrypted with AES-256 and SSL encryption. Vendor supports TLS version 1.2 or higher. SSH/port 22 and HTTPS/port 443 communication protocols are used for secure transmission. As TLS is initiated on the client side, the version of TLS in use is controlled by the customer's endpoint configurations.

- Databases that store Customer Data in Amazon Web Services (AWS) and Microsoft Azure are encrypted using AES-256 or a similar industry-accepted encryption standard (*e.g.,* TDE). The encryption controls for data at rest are based on the classification level of the Customer Data and Vendor's internal policies.

- Vendor uses private encryption keys for each customer, with Cloud Service Provider (CSP) key management support such as AWS Key Management Service (KMS), or Azure Key Vault. CSPs' keys are maintained in their proprietary vaulting solution, which is hardened separately from the rest of the cloud environment, tamper-resistant, and isolated from the host. The CSP-maintained keys are rotated automatically.

Network Security

- Vendor's network defense strategy for the Cloud Services environment involves multiple layers of defense designed to protect against unauthorised access to identities, devices, applications, data, and systems (e.g., servers, workstations, endpoints).

- Cloud network defense tooling includes monitoring of the network environment, Distributed Denial-of-Service (DDoS) protection, network firewalls or cloud services which emulate a firewall (e.g., Security Groups), Web Application Firewall (WAF) protection, and vulnerability scanners.

- Communication between the public internet and Cloud Service components is secured using HTTPS or SSH.

- Vendor employs Network Intrusion Detection / Prevention Systems (NIDS/NIPS) designed to detect and prevent intrusions into the Cloud Services and utilizes Bot and DDoS protection designed to detect and defend against denial-of-service threats.

Vulnerability & Patch Management

- Vendor's Cloud Service assets are continuously scanned and monitored for vulnerabilities. If a vulnerability is found, Vendor's standards for responding to vulnerabilities are maintained in the Support Portal.

- Vendor performs independent third party penetration testing annually for all SaaS applications in the portfolio.

- Vendor's patch management policy outlines maintenance controls which are the requirements and best practices for ensuring Vendor assets and endpoints have up-to-date operating systems and have security patches installed to protect them from known vulnerabilities.

- As a part of the shared responsibility model, Vendor patches its assets at a minimum on a monthly basis and as needed based on criticality. Cloud-provided assets are automatically updated by the cloud service provider (CSP). Vendor's standards for patching vulnerabilities are maintained in Support Portal.

Continuous Monitoring

- Customer-level/tenant logging is stored in the individual customer tenant's database.

- Application audit logs record types of events including, but not limited to, access attempts, authentications, secret access, and approvals for secret access. Azure logs contain but are not limited to accessed resources, authentications, application logs, privilege escalation logs, and Web Application Firewall (WAF) logs.

- Vendor uses a Platform as a Service (PaaS) system for accessing the application and web tiers. As part of the shared responsibility model, the CSP manages OS and server logs. Audit logs are read-only to Vendor, which prevents tampering.

- Vendor has deployed solutions for continuous intrusion detection and vulnerability monitoring for Cloud Service environment.

- Activity performed by Vendor personnel within the Cloud Services environment is logged and monitored.

Technology Development & Acquisition and Project & Resource Management

- Vendor's Software Development Life Cycle (SDLC) specifies Vendor's approach to creating software securely. The source code is encrypted at rest and only accessible from the corporate network by authorised end-points. Identity and Access Management (IAM) provides access only for those authorised to work with the source code.

- Vendor uses third-party libraries documented for commercial/open source. Reasonable efforts are made to use the most current version of a library at development time. Open source code is subject to the same security controls as Vendor -authored code. Open-source libraries are also checked for vulnerabilities. A Software Composition Analysis (SCA) tool scans the source code throughout the development lifecycle.

Business Continuity & Disaster Recovery and Incident Response

- Vendor's Business Continuity & Disaster Recovery (BC/DR) plans define the practices designed to ensure critical operations can continue in the event of an unexpected interruption or disaster, including natural, technological, or human-made. BC/DR plans are reviewed and updated annually or when appropriate to accommodate material changes.

- Vendor's incident response program provides a centralized process to evaluate security events and initiate an appropriate response. Vendor uses a Security Information and Event Management (SIEM) solution to identify events in information systems, and employee-reported security events. Vendor maintains processes and procedures for the activation of a Cyber Incident Response Team (CIRT) as needed for incidents.

- The Microsoft Azure and AWS data centres are in geographically diverse regions with multiple isolated locations to ensure service continuity. Vendor utilizes geo-replication, which asynchronously replicates data from a primary region to a geographically separated secondary region. Using multiple availability zones provides redundancy and automated failover capability to limit service disruptions and protect against geographic and environmental risks.

- Vendor leverages Azure's native continual backup functionality for stateful data within each customer's database. Continual Azure SQL backups are taken and stored in geo-redundant storage, which can be restored within the past 30 days. The cloud operations team can restore these in the event of an emergency or disruption.

- Databases are also replicated to a hot copy in an alternate data center. If system monitoring indicates a problem with the primary server, the system automatically switches to the alternate.

- Application servers have redundant deployment in a different physical location. If the primary data centre for a region goes down, Vendor can switch to the alternate application servers and begin serving data from the alternate location.

Human Resources Security and Security Awareness & Training

- Vendor conducts background checks to verify education, employment history, professional experience, and technical competence in accordance with applicable local laws. We also conduct criminal checks, in accordance with job responsibilities, access levels, and applicable local laws.

- Vendor implements a multi-tiered security and privacy awareness program for employees, including security and privacy awareness training upon hire, and annually thereafter, specialized training for key functional areas, security awareness bulletins, and just in time awareness training through phishing simulations.

- Vendor requires advanced security training (e.g., OWASP) annually for relevant personnel (e.g., SDEs, SREs).

With respect to Personal Data processed by Vendor in delivery of Fastpath Solutions:

- Vendor maintains an information security program (ISP) to maintain confidentiality, integrity, and availability of Personal Data within the Fastpath Solution. Vendor maintains SOC1 and SOC2 reports for the Fastpath Solutions.

- Vendor has annual examinations conducted to review the suitability of the design and the operating effectiveness of the controls in place around personnel security, system resiliency, system monitoring, information security, application change control, and data communications. Controls include:

    - Use of firewalls and monitoring;
    - Secure configuration of hardware, devices, and software.
    - Corporate policies and training ensure requirements are communicated throughout organization.
    - Control and segregation of access to data and services.
    - Change control and monitoring, including testing.
    - Malware and virus protection.
    - Maintenance and update of software, hardware, and related systems.
    - Regular backups of data.

- Vendor utilizes Microsoft Azure and Amazon Web Services to host the software solution and Customer Data. Vendor reviews annual Microsoft Azure and Amazon Web Services SOC1 and SOC2 reports to ensure controls in place around personal security, system resiliency, system monitoring, information security, application change control, and data communications are operating as designed.

- Vendor has an incident response policy and program in place to address personal data breaches.

* * * * * *