Global Data Processing Addendum

This Global Data Processing Addendum together with all attachments and appendices (“DPA”) forms part of the Master Services Agreement (or similar agreement under which Services are provided to Hyland) (“Services Agreement”) between Service Provider (or similar term under the Services Agreement) and Hyland and is incorporated therein by reference.

AGREEMENT

1. DEFINITIONS

Any capitalized term not defined herein shall have the meaning given to that term under the Services Agreement.

1.1. “Controller” means the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

1.2. “Data Subject” means the subject of Personal Data.

1.3. “Data Protection Law” means: (i) all privacy, security, data protection, direct marketing, consumer protection, and workplace privacy laws, rules, requirements and regulations of any applicable jurisdiction; and (ii) all current industry standards, guidelines, and practices with respect to privacy, security, data protection, direct marketing, consumer protection, and workplace privacy, including the collection, processing, storage, protection, and disclosure of Personal Data, in each case as applicable to the processing of Personal Data in connection with this Agreement.

1.4. “EU Model Clauses” means the Commission Implementing Decision (EU) 2021/914 establishing Standard Contractual Clauses for data transfers to Third Countries. For purposes of this DPA, the applicable modules within the EU Model Clauses are MODULE TWO (Transfer Controller to Processor) and/or MODULE THREE (Transfer Processor to Processor). For the avoidance of doubt, neither MODULE ONE (Transfer Controller to Controller) nor MODULE FOUR (Transfer Processor to Controller) shall apply to this DPA.

1.5. “Hyland” means Hyland Software, Inc. on behalf of itself and its affiliates. The term affiliates shall be deemed to include any parent company, subsidiary, affiliate of, or entity controlled by (including beneficial control), controlling or under common control with Hyland.

1.6. “Personal Data” means any information received by Service Provider from, or received or created on behalf of, Hyland relating to an identified or identifiable natural person. An “identifiable natural person” is one who can be identified, directly or indirectly, in particular, by reference to an identification number, location data, an online identifier or to one or more factors specific to the physical, psychological, genetic, mental, economic, cultural or social identity of the natural person.

1.7. “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 transmitted, stored or otherwise Processed when that Personal Data is in the possession of Service Provider or its agents or subcontractors.

1.8. “Processing” means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.9. “Processor” means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of another party;

1.10. “Required By Law” means that a statute, regulation, court order, or legal process, enforceable in a court of law, mandates the conduct.

1.11. “Supervisory Authority” means the regulatory body under applicable Data Protection Law.

1.12. “Sensitive Personal Data” means Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning health, sex life, or sexual orientation, genetic data and biometric data when Processed for the purpose of uniquely identifying a natural person, and also includes information about criminal history.

1.13. “Sub-processor” means an entity that Processes Personal Data at the request of Service Provider.

1.14. “UK Model Clauses” means the UK standard contractual clauses for international transfers from controllers to processors.

2. SERVICE PROVIDER’S PROCESSING OF PERSONAL DATA

2.1. Nature and Purpose of Processing of Personal Data. Service Provider agrees to Process Personal Data solely for the specific purposes and in accordance with **Appendix A**, except where Required By Law**.** Where Service Provider is Required By Law to Process Personal Data under terms other than those of this DPA, Service Provider shall immediately notify Hyland.

2.2. Duration of Processing. Service Provider shall Process Personal Data only for the duration set out in **Appendix A**.

2.3. Violation Of Data Protection Law. Service Provider will immediately notify Hyland if Service Provider becomes aware that Service Provider’s compliance with a term or condition of this DPA has violated, violates, or will violate Service Provider’s or Hyland’s obligations under applicable law.

3. CROSS-BORDER DATA TRANSFERS

3.1. Service Provider will not transfer Personal Data outside of the jurisdiction in which the Personal Data originated, unless it has taken such measures as are necessary to ensure the transfer is in compliance with applicable Data Protection Law. Such measures may include (without limitation) transfers to any country or territory and/or sector that is at the time subject to a current finding by the relevant authority of adequate protection, to a recipient that has achieved binding corporate rules authorization in accordance with Data Protection Law, or under any derogation permitted by Data Protection Law.

3.2. To the extent that Service Provider transfers Personal Data outside the EU or Switzerland in connection with the Services provided under the Services Agreement, and such transfer is not covered by any measure set forth in Section 3.1, the relevant transfer shall be governed by the appropriate EU Model Clauses, which are incorporated herein by referenced into this DPA, as follows:

3.2.1. Hyland as Controller. In all such cases, MODULE TWO of the EU Model Clauses applies.

3.2.2. Hyland as Processor. In all such cases, MODULE THREE of the EU Model Clauses applies.

and the remaining details required under the EU Model Clauses being deemed completed as

appropriate with the information set out in this DPA (including without limitation the Appendix) and the Services Agreement. For the avoidance of doubt, for purposes of the EU Model Clauses, Appendix A of this DPA shall serve as Annex I and Appendix B shall serve as Annex II. In the event of any conflict or inconsistency among or between the terms and conditions of any such EU Model Clauses and this DPA and/or the Services Agreement, the terms of the EU Model Clauses shall prevail.

3.3. To the extent that Service Provider transfers Personal Data outside the United Kingdom in connection with the Services provided under the Services Agreement, and such transfer is not covered by any measure set forth in Section 3.1, the relevant transfer shall be governed by the appropriate UK Model Clauses, which are incorporated herein by reference. The remaining details required under the UK Model Clauses being deemed completed as appropriate with the information set out in this DPA (including without limitation the Appendix) and the Services Agreement. In the event of any conflict or inconsistency among or between the terms and conditions of any the UK Model Clauses and this DPA and/or the Services Agreement, the terms of the UK Model Clauses shall prevail.

3.3.1. Hyland as Controller. In all such cases, MODULE TWO of the EU Model Clauses applies.

3.3.2. Hyland as Processor. In all such cases, MODULE THREE of the EU Model Clauses applies.

and the remaining details required under the EU Model Clauses being deemed completed as appropriate with the information set out in this DPA (including without limitation the Appendix) and the Services Agreement. For the avoidance of doubt, for purposes of the EU Model Clauses, Appendix A of this DPA shall serve as Annex I and Appendix B shall serve as Annex II. In the event of any conflict or inconsistency among or between the terms and conditions of any such EU Model Clauses and this DPA and/or the Services Agreement, the terms of the EU Model Clauses shall prevail.

4. SERVICE PROVIDER'S SAFEGUARDS FOR PERSONAL DATA

4.1. Confidentiality Of Personal Data. Service Provider will maintain the confidentiality of all Personal Data. Service Provider will require employees responsible for Processing Personal Data to sign a confidentiality agreement prohibiting the disclosure of Personal Data to any third party except as permitted by this DPA or as Required By Law.

4.2. Physical, Technical And Organizational Safeguards. Service Provider shall maintain a comprehensive written information privacy and security program that includes reasonable and appropriate measures to protect against reasonably foreseeable risks to the security, confidentiality, integrity and resilience of Personal Data, which risks could result in the unauthorized disclosure, use, alteration, destruction or other compromise of the Personal Data, including a Personal Data Breach. Such program shall comply with the requirements of applicable Data Protection Laws concerning the protection of Personal Data and shall include the measures set forth in **Appendix B** (Security Measures) attached hereto and incorporated herein. Such measures shall not be materially reduced during the Term of the Services Agreement. Service Provider will regularly monitor, test, and update its information security program. Service Provider shall also maintain in accordance with good industry practice, measures to protect Personal Data from interception such as: (i) network protections intended to deny attackers the ability to intercept or access Personal Data; and (ii) anonymization or other measures to deny attackers the ability to read intelligible Personal Data, including encryption in transit between Service Provider and any third party. Service Provider will provide Hyland with such information concerning its information security program as Hyland may reasonably request from time to time. If Service Provider Processes special categories of Personal Data (as defined by applicable Data Protection Laws), Service Provider shall apply specific restrictions and/or additional safeguards.

4.3. Reporting Personal Data Breaches. Service Provider shall report to Hyland any Personal Data Breach of which it becomes aware. Service Provider will make such report orally to Hyland within 24 hours of Service Provider's becoming aware of the incident followed by a report in writing (e-mail is acceptable) within 24 hours of the initial oral report. The written report shall include, at a minimum subject to the availability of necessary information, the following: (1) a description of the incident; (2) the date that the incident occurred; (3) the date that Service Provider became aware of the incident; (4) the identity and last known mailing address of each affected Data Subject; (5) the approximate

number of affected Personal Data records involved; (6) the affected categories of Personal Data, including Sensitive Personal Data, if any, for each affected Data Subject that was affected; (7) the approximate number of Data Subjects affected; (8) an identification of any law enforcement agency or Supervisory Authority that has been contacted about the incident and contact information for the relevant official; (9) a description of the steps that have been, or will be, taken to mitigate the incident; (10) a description of the steps that have been, or will be, taken to prevent a recurrence; (11) the likely consequences of the Personal Data Breach; and (12) contact information for the person at Service Provider principally responsible for responding to the Personal Data Breach and who can provide more details about the Personal Data Breach; and (13) any other information required by applicable Data Protection Law.

4.4. Service Provider will update the written report periodically as new information becomes available. All reports required by this provision shall be made to: Hyland Legal Department, Attn: Privacy Officer, 28500 Clemens Rd. Westlake, Ohio 44145, 440-788-5000, privacy@hyland.com. Service Provider acknowledges that its determination that a particular set of circumstances constitutes a Personal Data Breach shall not be binding on Hyland.

4.5. Mitigation Of Damages By Service Provider And Cooperation in Investigation. Service Provider agrees to take, at its own expense, measures reasonably necessary to mitigate any harmful effect of a Personal Data Breach. Service Provider agrees to cooperate, at its own expense, with Hyland in its investigation of any Personal Data Breach. Service Provider will reimburse Hyland for all imputed and out-of-pocket costs reasonably incurred by Hyland in connection with the Personal Data Breach, including, but not limited to, costs related to provision of notices to affected Data Subjects and to any services offered to affected Data Subjects.

4.6. Notifications Related To A Personal Data Breach. Service Provider acknowledges that Hyland shall determine (1) whether and when to notify any Controller (if applicable) or Supervisory Authority and which Supervisory Authority to notify; (2) who will provide notice to Data Subjects with respect to any Personal Data Breach; (3) the content of any such notice(s); (4) the timing for, and method of, delivery of any such notice(s); and (5) the products or services, if any, to be offered to affected Data Subjects. Service Provider shall not disclose the fact that a Personal Data Breach has occurred or any details related to a Personal Data Breach to any third party without Hyland's written consent, unless otherwise Required By Law.

4.7. Third Party Access Requests. In the event Service Provider receives a non-compulsory request from any third party, including without limitation, any law enforcement, regulatory, judicial or governmental authority, for disclosure of or access to Personal Data, Service Provider will not disclose or provide such access unless instructed to do so by Hyland. In the event Service Provider receives a compulsory order issued at the request of any third party, including without limitation any law enforcement, regulatory, judicial or governmental authority for disclosure of or access to Personal Data, Service Provider will prior to any disclosure or provision of access:

4.7.1 promptly notify Hyland of such order, unless prohibited by law, and, if so prohibited from notifying Hyland, seek to obtain the right to waive such prohibition in favor of promptly communicating to Hyland as much information as possible; and

4.7.2. inform the third party that: (i) Service Provider is a Processor of such transferred Personal Data and that Hyland has not authorised the disclosure of Personal Data to the third party; and (ii) any and all requests or demands for disclosure of or access to such transferred Personal Data should therefore be notified to or served upon Hyland; and

4.7.3. Only disclose such transferred Personal Data to the extent Service Provider is legally required to do so in accordance with an applicable lawful process, and prior to any such transfer, use reasonable efforts to challenge the scope or validity of any order that Service Provider reasonably believes to be overly broad.

4.8. Service Provider will maintain, in accordance with good industry practice, measures to protect Personal Data from interception such as: (a) network safeguards intended to deny attackers the ability to access Personal Data; and (b) other measures to deny attackers the ability to read intelligible Personal Data, including encryption in transit between Service Provider to Hyland and from Service

Provider to any Sub-Processor.

4.9. To the extent that Service Provider Processes Personal Information as that term is defined in the California Consumer Protection Act (codified at Cal. Civ. Code §1798.100 et seq.) ("CCPA"), then notwithstanding anything in this DPA, the Service Provider Agreement or any applicable Service Provider privacy policy to the contrary, Service Provider (including its vendors, agents, or subcontractors) shall not Sell (as defined in the CCPA) Personal Information. Service Provider future represents that it understands that the restrictions set forth in this DPA apply to Personal Information and agrees to comply with such obligations.

5. SERVICE PROVIDER'S ASSISTANCE WITH AUDITS AND DATA SUBJECT REQUESTS

5.1. Availability Of Records Of Processing. To the extent required by applicable Data Protection Law, Services Provider shall maintain a record of processing activities and Service Provider shall promptly, after a reasonable request from Hyland, make available to Hyland all information necessary to demonstrate the Controller's compliance with such obligations established under applicable Data Protection Laws. Service Provider shall notify Hyland without undue delay if it becomes aware that the Personal Data it is Processing on Hyland's behalf is inaccurate or has become outdated.

5.2. Information Technology Audits. Service Provider will permit Hyland, directly or through a contractor, to conduct site audits of the information technology and information security controls for all facilities used to Process Personal Data so that Hyland can ensure that Service Provider provides the appropriate level of security for the Personal Data. Where required to do so, the Parties shall make the results of such audits available to the competent Supervisory Authority/ies.

5.3. Requests For Impact Assessment Information. Service Provider shall promptly provide the information requested by Hyland to assist in conducting a data protection impact assessment pursuant to applicable Data Protection Law, including with respect to related consultations of the applicable Supervisory Authority.

5.4. Requests Directed to Service Provider. Service Provider agrees to assist Hyland in responding to a request from a Data Subject to exercise any of his/her rights as provided for under applicable Data Privacy Laws. In the event a Data Subject submits such a request to Hyland with respect to the Data Subject's Personal Data processed by Service Provider, Service Provider agrees to comply with the request within 5 business days of receiving the request from Hyland. Service Provider will immediately provide Hyland with any requests concerning Personal Data that are sent directly to Service Provider from parties other than Hyland. Service Provider shall not respond to the request itself, unless authorized by Hyland.

6. SERVICE PROVIDER'S SUB-PROCESSORS

6.1. Consent To Processing By Sub-Processors. Service Provider will not disclose Personal Data to any third party without Hyland's prior written consent. In the event that Hyland consents to Service Provider's disclosure of Personal Data to a Sub-processor, Service Provider shall remain fully responsible for, and remain liable to, Hyland for, the acts and omissions of such Sub-processor as if they were Service Provider's own acts and omissions.

6.2. Sub-processors' Physical, Technical And Administrative Safeguards. Service Provider shall obtain reasonable assurances, in writing, from any Sub-processor to whom Service Provider discloses Personal Data. Such assurances shall include at least the following: that the Sub-processor (1) will comply with substantially the same restrictions and conditions on Processing of Personal Data that this DPA imposes on Service Provider, including the restrictions on cross-border data transfers; (2) will implement reasonable and appropriate physical, technical and organizational safeguards to protect Personal Data at least in compliance applicable Data Protection Law; and (3) will notify Service Provider within 24 hours of becoming aware of any Personal Data Breach involving Personal Data.

6.3. Sub-Processor Agreements. At Hyland's request, Service Provider shall provide a copy of all Sub-processor agreements and any subsequent amendments. To the extent necessary to protect business secret or other confidential information, including Personal Data, the Service Provider may redact the text of the agreement prior to sharing the copy.

7. SERVICE PROVIDER'S OBLIGATIONS UPON TERMINATION OF THE SERVICE AGREEMENT

7.1. Return Or Destruction Of Personal Data. Upon Hyland's written instruction, Service Provider shall return or destroy Personal Data. If Hyland directs Service Provider to destroy the Personal Data, Service Provider shall do so in a manner reasonably intended to prevent recovery of the Personal Data and shall certify to the same in writing.

7.2. Service Provider's Retention Of Personal Data. If local law requires Service Provider to retain a copy of any Personal Data, then Service Provider shall (1) notify Hyland of such requirement, (2) extend the protections of this DPA to the retained Personal Data and (3) limit further Processing of the retained Personal Data to those purposes Required By Law for as long as Service Provider maintains the Personal Data.

7.3 Survival. Service Provider's obligations and duties under this DPA with respect to Personal Data shall survive the termination of the Services Agreement and of this DPA and shall continue for as long as the Personal Data remains in the possession of Service Provider or of its Sub-processors.

8. MISCELLANEOUS TERMS

8.1. Indemnification. Service Provider shall defend and indemnify Hyland, its parent and subsidiary corporations, officers, directors, employees and agents for any and all claims, charges, inquiries, investigations, costs, reasonable attorneys' fees, monetary penalties, and damages incurred by Hyland and/or its parent or subsidiary corporations, officers, directors, employees and agents resulting from (1) any Processing of Personal Data not permitted by the Services Agreement and this DPA, (2) any Personal Data Breach involving Personal Data in the possession, custody or control of Service Provider or its sub-processors, in the event such Personal Data Breach results in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data.

8.2. Indemnification Process. The foregoing indemnification obligations are conditioned upon Hyland: (1) notifying Service Provider promptly in writing of any claim, charge, inquiry, or investigation as described in Section 8.1 above; (2) reasonably cooperating and assisting in defense of such claim, charge, inquiry, or investigation; and (3) giving sole control of the defense and any related settlement negotiations to Service Provider with the understanding that Service Provider may not settle any claim in a manner that admits guilt or otherwise prejudices Hyland, without Hyland's consent.

8.3. Third Party Beneficiaries. If: (i) Hyland has factually disappeared, ceased to exist in law or has become insolvent; and (ii) MODULE THREE of the EU Model Clauses applies to the Services provided by Service Provider, then Service Provider agrees that any applicable data exporter shall have the right to terminate this DPA solely as to such data exporter and to instruct Service Provider regarding the return or erasure of the applicable Personal Data.

8.4. Construction. This DPA supersedes any inconsistent provisions in the Services Agreement and/or other existing agreements between the Hyland and Service Provider with respect to Service Provider's obligation to safeguard Personal Data.

8.5. Signatures. The Parties agree that signature to this Services Agreement constitutes all necessary signatures to the EU Model Clauses or UK Model Clauses, including the appendices attached thereto (where applicable).

APPENDIX A

Subject Matter and During of the Processing	The subject matter of the Processing is Service Providers provision of Services under the Services Agreement. The duration of the Processing is the term of the Services Agreement, and any exit period, if applicable.
Categories of Data Subjects whose	Employees, Vendors, Website visitors, Hyland Customers or End-Users

Personal Data is Processed	
Nature and Purpose of the Processing	The purpose of the Processing is to provide the Services as set forth in the Services Agreement. The nature of the Processing may include, but is not limited to, collection, recording, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Type of Personal Data Processed	The Personal Data transferred may concern the following categories of Data Subjects: ***Employees*** - Past, potential, present and future staff of Hyland (including job candidates, volunteers, agents, independent contractors, interns, temporary and casual workers). ***Vendors*** - Past, present and potential advisors, consultants, vendors, contractors, subcontractors and other professionals engaged by Hyland and related staff. ***Website visitors*** – Individuals who visit any Hyland owned or operated website. ***Hyland Customers or End Users (collectively, "Customers")*** – (a) Past, present and potential Customers of Hyland, and (b) data subjects whose Personal Data is uploaded or provided by Customers to Hyland during use of Hyland's services or products.
Categories of Personal Data Processed	The Personal Data transferred may concern the following categories: ***Employees*** Identification data: civil/marital status; first and last name; photograph; date and place of birth; nationality; corporate identifier; gender. Contact details: address; telephone number (fixed and mobile); email address; fax number; emergency contact information. Employment details: job title; company name; grade, occupation code; geographic location; employee performance and evaluation data; employee discipline information; information regarding previous roles and employment; employee benefits information such as election decisions, leave requests, authorization/declination, health insurance company. National identifiers: national ID/passport number; tax ID; government identification number; driver's license, visa or immigration status. Academic and professional qualifications: degrees; titles; skills; language proficiency; training information; employment history; CV/résumé. Financial data: bank account number; IBAN number; bank details including bank name, bank code, sort code; salary and compensation data; bonuses; pension qualification information; payroll data; tax class; tax office name.

	IT related data: computer ID; user ID and password; domain name; IP address; log files; software and hardware inventory; software usage pattern tracking information (i.e., cookies and information recorded for operation and training purposes). Lifestyle: hobbies; social activities; holiday preferences. ***Vendors*** Identification data: first and last name; date of birth; place of birth; nationality; photograph; vendor ID. Contact details: address; professional email address; professional telephone number (including mobile telephone number). Professional details: job title; employer; academic and professional qualifications; data related to transactions involving goods and services. National identifiers: tax ID; government identification number. Financial data: bank account number; bank details. ***Website visitors*** IT-related data: unique device identifiers, dynamic and static Internet Protocol addresses, as well as other information, such as browser characteristics, language preferences, operating system details, referring URLs, length of visits, and pages viewed. ***Customers, potential Customers and/or their staff, each as applicable*** Contact information (including name, physical address, e-mail and telephone numbers); Employer; Job title; Login credentials; Account profile, including interests and photograph; Applications for Hyland's educational opportunities, including name, contact information, references, programming experience, and application essays; Dietary preferences and restrictions; Order information for trainings courses; Training records including courses taken, certifications completed, and scores and grades; Questions, feedback, comments and other postings, including through https://community.hyland.com; Other information the Customer chooses to provide; Information provided by third parties: data relating to the Customer, potential Customer or staff having clicked on a Hyland advertisement posted on a third party website; Information provided by third parties, where a Customer attends a Hyland event sponsored by a third party: including name, e-mail address, and phone number; Versions of Hyland Group company software used and how the software is being used (what functions, how often etc.); bank account number; bank details; credit card details; purchasing history; return history; cancellation history; and Personal Data submitted by a Customer in the course of the Customer's use of Hyland's Services or during the performance of Services under the Service Agreement.

Categories of Sensitive Personal Data Processed	No collection of any sensitive data by a Service Provider is anticipated other than employee data required to provide Services in connection with valid employment purposes or to the extent required by applicable law. Such collection will only concern limited sensitive data, for example, health-related information for the purpose of managing employee absences, or disabilities in order to provide access to our premises.
FOR USE ONLY WITH THE EU MODEL CLAUSES	
Data Exporter (including country of establishment)	Hyland, as defined in this DPA.
Data Importer (including country of establishment)	Service Provider, as defined in the Service Provider Agreement.
Frequency of the Transfer	Continuous basis
Retention Period	The Personal Data transferred may be stored in an identifiable form for no longer than necessary for the purposes for which the Personal Data was transferred and, in no event, longer than permitted under the laws of the country of the Data Exporter.
Governing Law	MODULE TWO: EU Member State in which the data exporter (i.e., applicable Hyland entity) is established. MODULE THREE: EU Member State in which the data exporter (i.e., applicable customer entity) is established.
Choice of Forum and Jurisdiction	The Parties agree that any disputes arising from the EU Model Clauses shall be resolves by the courts of the Netherlands.
Sub-processors	Data importer may use Sub-processors as set forth by Section 6 of this DPA.
Competent Supervisory Authority	The competent supervisory authority is the supervisory authority of the EU/EEA Member State where the Data Exporter is established.

Appendix B
Technical and organizational measures

Taking into account

- the state of the art,

- the costs of implementation and

- the nature, scope, context and

- the purpose of processing as well as

- the risk of varying likelihood and severity for the rights and freedoms of natural persons,

Service Provider shall maintain a comprehensive written information privacy and security program that

includes reasonable and appropriate measures to protect against reasonably foreseeable risks to the security, confidentiality, integrity and resilience of Personal Data. Such program shall include, at a minimum, the following:

Administrative Controls

- A person or committee responsible for Service Provider's information security and privacy program;
- Policies and procedures to investigate, mitigate, and provide notice of a Personal Data Breach;
- Vulnerability management program to identity, prioritize and remediate security vulnerabilities;
- Employees that are subject to confidentiality and non-disclosure commitments and understand their obligations and responsibilities in relation to the Service Providers information privacy and security program;
- A security awareness training program, which includes periodic security reminders and updates;
- A password policy, requiring complex passwords, a maximum password age, a minimum password age, account lockout policies and other logon restrictions; and
- Disaster recovery and business continuity procedures.

Physical Controls

- Policies and procedures to safeguard the facilities and equipment that house Personal Data against unauthorized physical access, theft or destruction;
- Procedures to control and validate access to facilities that house Personal Data based on role/function, including visitor control;
- Physical safeguards for all workstations that access Personal Data to restrict access from authorized users; and
- Permanently destroying or removing Personal Data from hardware prior to final disposition.

Technical Controls

- Policies and procedures to limit access rights based on the principle of least privilege;
- User access controls that address timely provisioning and de-provisioning of user accounts;
- Workstations that are set to lock automatically after a set period of inactivity;
- Encryption at rest and in transit of Personal Data;
- Industry standard anti-malware software used on all endpoints with behavioral based protection against ransomware and other exploits;
- Procedures to ensure that all security patches are applied in a timely manner;
- Operating system and application patches and updates pushed regularly;
- Network segregation including but not limited to the separation of all Hyland Personal Data stored by Service Provider; and
- Service Providers that store Hyland Personal Data shall also maintain an external audit program, tested at least annually.
- Completed attestations, such as SOC 2 reports, shall be provided to Hyland upon written request.