Global Data Processing Addendum

This Global Data Processing Addendum together with all appendices and addenda ("DPA") forms part of the Master Services Agreement (or similar agreement under which Services are provided to Hyland) ("Services Agreement") which incorporates this DPA by reference.

1. DEFINITIONS

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

1.1 "Adequacy Determination" means a final determination by a Regulator that the laws of a third country provide an adequate level of protection for Personal Data when that Personal Data is transferred from the jurisdiction of the governmental authority to the third country.

1.2 "Data Protection Law" means: (i) all privacy, security, data protection, direct marketing, consumer protection, and workplace privacy laws, rules, requirements and regulations of any relevant 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 DPA.

1.3 "Data Subject" means an identified or identifiable natural person as defined by applicable Data Protection Law and whose Personal Data is Processed, on Hyland's behalf, by Service Provider or its Sub-processor.

1.4 "EU SCCs" means the Commission Implementing Decision (EU) 2021/914 establishing Standard Contractual Clauses for data transfers to Third Countries.

1.5 "Hyland" means Hyland Software, Inc. located at 28500 Clemens Rd., Westlake, Ohio 44145 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 individually identifiable information related to a Data Subject and received by Service Provider from, or received or created on behalf of, Hyland. Personal Data includes Sensitive Personal Data.

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 "Regulator" means the competent supervisory authority or regulatory body under applicable Data Protection Law.

1.10 "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 as well as any other information characterized as "sensitive" under applicable Data Protection Laws.

1.11 "Sub-processor" means an entity that Processes Personal Data at the request of Service Provider.

2. SERVICE PROVIDER'S PROCESSING OF PERSONAL DATA

2.1 Instructions for Processing Personal Data. Service Provider agrees to Process Personal Data solely to provide the Services and in

accordance with the Data Processing Particulars, except where otherwise required by law. Service Provider shall inform Hyland without undue delay if, in its reasonable opinion, an instruction issued by Hyland violates applicable Data Protection law.

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

3. SERVICE PROVIDER'S SAFEGUARDS FOR PERSONAL DATA

3.1 Confidentiality Of Personal Data. Service Provider will maintain the confidentiality of all Personal Data. Service Provider will ensure that all personnel authorized to Process Personal Data have signed a confidentiality agreement or are otherwise under an appropriate statutory obligation of confidentiality.

3.2 Physical, Technical And Organizational Safeguards. Service Provider will 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 to the extent that Addenda I or II apply, such measures shall include, at a minimum, the measures set forth in **Appendix A** (Security Measures) attached hereto and incorporated herein. 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 Sensitive Personal Data, Service Provider shall apply specific restrictions and/or additional safeguards.

3.3 Reporting Personal Data Breaches. Service Provider will 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 Personal Data Breach 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 Personal Data Breach; (2) the date that the Personal Data Breach occurred; (3) the date that Service Provider became aware of the Personal Data Breach; (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 Regulator 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; (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. Service Provider will update such written report periodically as new information becomes available.

3.4 Hyland Breach Response Point of Contact. All written reports 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.

3.5 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.

3.6 Notifications Related To A Personal Data Breach. Service Provider acknowledges that as between Hyland and Service Provider, Hyland shall determine: (1) whether and when to notify any Data Subject or Regulator and which Regulator 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.

3.7 Third Party Access Requests. In the event Service Provider receives a 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 or as otherwise required by law. Where Service Provider is legally

required to disclose Personal Data in accordance with an applicable lawful process, Service Provider shall: (i) immediately notify Hyland of such order (unless prohibited by applicable law); (ii) inform the requesting third party that Service Provider is not authorized to disclose such Personal Data and that all demands shall be directed to Hyland; and (iii) to the extent that Service Provider reasonably believes the order is overly broad use reasonable efforts to challenge the scope or validity of the order.

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

4.1 Availability Of Records Of Processing. To the extent required by applicable Data Protection Law, Services Provider shall maintain a record of processing activities. Service Provider shall promptly, after a reasonable request from Hyland, make available to Hyland all information necessary to demonstrate Hyland's compliance with its 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.

4.2 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 by applicable Data Protection Laws, the Parties shall make the results of such audits available to relevant Regulators. Where applicable, Hyland may share the results of any such audit with its applicable customer(s).

4.3 Requests For Privacy Assessment Information. Service Provider shall promptly provide the information reasonably requested by Hyland to assist Hyland in conducting a data privacy assessment.

4.4 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 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 to do so.

5. SERVICE PROVIDER'S SUB-PROCESSORS

5.1 Consent To Processing By Sub-Processors. Hyland authorizes Service Provider to engage the Sub-Processors listed in the Data Processing Particulars . Service Provider shall notify Hyland at least thirty (30) days prior to authorizing any new Sub-Processor to Process Personal Data. Where such rights are granted by applicable Data Protection Law, Hyland may object to any new Sub-Processor by Service Provider. If Service Provider continues use of such Sub-Processor after Hyland's reasonable objection, then Hyland may elect to immediately (without prejudice to accrued fees or other rights under the Services Agreement) suspend or terminate the applicable Services Agreement. Service Provider will not disclose Personal Data to any third party, including Sub-processors, without Hyland's prior written consent. Service Provider shall remain fully responsible for, and remain liable to, Hyland for, the acts and omissions of its Sub-processors as if they were Service Provider's own acts and omissions.

5.2 Sub-processors' Physical, Technical And Administrative Safeguards. Service Provider shall obtain reasonable assurances, in writing, from any Sub-processor to which Service Provider discloses Personal Data or that creates or receives Personal Data on Hyland's behalf. 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 applicable 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 with applicable Data Protection Law; and (3) will notify Service Provider within 24 hours of becoming aware of any Personal Data Breach.

5.3 Sub-Processor Agreements. To the extent permitted by applicable Data Protection Law and 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 text of the agreement prior to sharing the copy.

6. JURISDICTION - SPECIFIC TERMS

6.1 The Parties acknowledge that certain jurisdictions require the Parties to provide additional protections for

Personal Data. Such additional jurisdiction-specific terms are contained in the following addenda and are incorporated by reference into this DPA. Each addendum, to the extent applicable, is binding on the Parties as follows:

6.1.1 Addendum I (EEA & Switzerland): Addendum I applies when Service Provider Processes, in a country not subject to an Adequacy Determination, Personal Data related to a Data Subject residing in the European Economic Area ("EEA") or Switzerland.

6.1.2 Addendum II (UK): Addendum II applies when Service Provider Processes Personal Data, in a country not subject to an Adequacy Determination, related to a Data Subject residing in the United Kingdom ("UK").

6.1.3 Addendum III (California, USA): Addendum III applies when Hyland is subject to the California Privacy Rights Act ("CPRA"), and Service Provider Processes Personal Data of a Data Subject residing in California.

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

7.1 Term. This DPA shall have a term commencing on the Effective Date and will terminate automatically upon the termination or expiration of the Services Agreement.

7.2 Return Or Destruction Of Personal Data. Upon termination of the Services Agreement or in response to Hyland's written request at any time, and pursuant to Hyland's written instruction, Service Provider shall return or destroy Personal Data. If Hyland directs Service Provider to destroy Personal Data, Service Provider shall (a) do so in a manner reasonably intended to prevent recovery of the Personal Data, (b) ensure that any Sub-processor that Processes Personal Data also has done so, and (c) promptly provide Hyland with a certification to the same in writing. If Hyland directs Service Provider to return Personal Data, Service Provider shall promptly return the Personal Data in its possession and in the possession of any Sub-processor and shall retain no copies thereof unless required to do so by applicable law.

7.3 Service Provider's Retention Of Personal Data. If applicable 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.

7.4 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, indemnify and hold harmless 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, judgments, 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 and (2) any Personal Data Breach caused by Service Provider's or its Sub-Processors acts or omissions.

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 the Indemnification section 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 Construction. This DPA supersedes any inconsistent provisions in the Services Agreement and/or other existing agreements between Hyland and Service Provider (other than the agreements referenced in Jurisdiction Specific Terms section of this Agreement) with respect to Service Provider's obligation under this DPA.

ADDENDUM I

EEA and Switzerland

The Parties agree that transfers of Personal Data from the European Economic Area or Switzerland (collectively the "EEA") shall be governed by the EU SCCs (as supplemented by this DPA), which are incorporated herein by reference.

The Parties further agree that the EU SCCs shall be completed as follows:

- Module 2 shall apply unless Hyland is a Processor in which case Module 3 will apply.
- Clause 7, the optional docking clause will not apply.
- Clause 9(a), Option 2 will apply. Hyland authorizes Service Provider to engage Sub-Processors as set forth in Section 5 of this DPA.
- Clause 11, the optional redress language will not apply.
- Clause 17, Option 1 will apply, and the EU SCCs shall be governed by the law specified in the Services Agreement, provided that law is an EU Member State recognizing third party beneficiaries, otherwise the laws of the Netherlands shall apply.
- Under Clause 18(b), disputes will be resolved before the courts specified under the Services Agreement, provided those courts are in an EU Member State recognizing third party beneficiaries, otherwise those courts shall be the courts of the Netherlands.
- Annex I of the EU SCCs shall be deemed completed with the information set out in the Data Processing Particulars.
- Annex II of the EU SCCs shall be deemed completed with the information set out in **Appendix A.**
- Annex III of the EU SCCs shall be deemed completed with the information set out in the Data Processing Particulars**.**

In relation to Personal Data that is protected by the Swiss Federal Act on Data Protection, the EU SCCs will apply as completed herein and as adapted below:

- The Swiss Federal Data Protection and Information Commissioner ("Swiss DPA") is the exclusive supervisory authority, and each reference to a "supervisory authority" shall be understood to be a reference to the Swiss DPA.
- The term "member state" will not be interpreted in such a way as to exclude Data Subjects in Switzerland from the possibility of enforcing their rights in their place of habitual residence (Switzerland) in accordance with Clause 18 and the choice of law in Clause 17 shall be the applicable Swiss law.
- References to the GDPR and EU SCCs shall include equivalent provisions of the Swiss Federal Act on Data Protection.

Signatures to the Services Agreement shall constitute all necessary signatures to the EU SCCs, including the Annexes attached thereto.

ADDENDUM II

United Kingdom

Part 1: Tables

TABLE 1: Parties		
Start date	Effective Date as defined in the Services Agreement.	
The Parties	Exporter (who sends the Restricted Transfer)	Importer (who receives the Restricted Transfer)
Parties' details	Full legal name: Hyland on behalf of	Full legal name: Service Provider, as

	its affiliates located in the United Kingdom, including the following: Hyland UK Operations Limited Hyland UK Holdings Limited Hyland Software UK Ltd. Hyland Software Solutions UK Ltd. Nuxeo Group Limited Nuxeo Limited Trading name (if different): n/a Main address (if a company registered address): As specified in the Services Agreement Official registration number (if any) (company number of similar identifier):	set forth in the Services Agreement. Trading name (if different): Main address (if a company registered address): As specified in the Services Agreement Official registration number (if any) (company number of similar identifier):
Key Contact	Full Name (optional): Job Title: Global Privacy Officer Contact Details including email: privacy@hyland.com	Full Name (optional): Job Title: Contact Details including email: As set forth in the Data Processing Particulars
Signature (if required for purposes of Section 2)	Signatures to the Services Agreement shall constitute all necessary signatures to this Addendum II.	Signatures to the Services Agreement shall constitute all necessary signatures to this Addendum II.

TABLE 2: Selected SCCs, Modules, and Selected Clauses	
Addendum EU SCCs	The version of the Approved EU SCCs which this Addendum is appended, including the Appendix Information.

TABLE 3: Appendix Information	
“Appendix Information” means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in.	
Annex 1A: List of Parties:	As described in the Data Processing Particulars
Annex 1B: Description of Transfer:	As described in the Data Processing Particulars
Annex II: Technical and organizational measures including technical and organizational measures to ensure the security of the data:	As described in the DPA, Appendix A
Annex III: List of Sub processors (Modules 2 and 3 only):	As described in the Data Processing Particulars

TABLE 4: Ending this Addendum when the Approved Addendum Changes	

Ending this Addendum when the Approved Addendum Changes	Which Parties may end this Addendum as set out in Section 19: Importer Exporter

Part 2: Mandatory Clauses

Mandatory Clauses	Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.

ADDENDUM III

California, USA

The following additional provisions apply to Service Providers 's Processing of the Personal Information that is subject to the CCPA and/or CPRA, as applicable.

a. Definitions: Unless otherwise indicated in this DPA, the capitalized terms used in this section shall have the meaning assigned to them in the California Privacy Rights Act ("CPRA" or the "Act"), codified at Cal. Civ. Code §1798.100 *et seq.*, effective January 1, 2023.

i. "Business Purpose(s)" means Processing Personal Information on behalf of Hyland for the following purposes: (i) to provide the Services as specifically defined in the Services Agreement; (ii) to detect security incidents or protect the Personal Information against malicious, deceptive, fraudulent or illegal activity; or (iii) otherwise as expressly permitted by the CPRA or the CPRA Regulations.

ii. "CCPA" means Title 1.81.5 California Consumer Privacy Act of 2018 (California Civil Code §§ 1798.100–1798.199), as amended or superseded from time to time.

iii. "Consumer" means a California resident (a) who is a natural person, and (b) whose Personal Information is Processed by Service Provider on Hyland's behalf for the purposes stated in the Services Agreement and this DPA.

iv. "CPRA Regulations" means final regulations implementing the CPRA after those regulations go into effect.

v. "Personal Information" shall have the meaning set forth in the CPRA but shall be limited to Personal Information of California Consumers which Service Provider Processes on Hyland's behalf pursuant to the Services Agreement and this DPA.

b. Processing Of Personal Information: Hyland is a Business and appoints Service Provider as its Service Provider (as defined under the CPRA) to Process Personal Information only for the Business Purposes. Service Provider shall comply with all applicable sections of the CPRA and/or the CPRA Regulations, including providing the same level of protection for Personal Information as the CPRA requires Hyland, as a Business, to provide. Service Provider grants Hyland the right to take reasonable and appropriate steps to help ensure that Service Provider uses Personal Information consistent with the CPRA and to stop and remediate unauthorized use of Personal Information.

c. Restrictions On Processing Personal Information: Service Provider is prohibited from: (i) Processing Personal Information for any purposes but for the Business Purposes; (ii) Processing Personal information for any additional commercial purpose (other than the Business Purposes) including in the servicing of a different business, unless otherwise expressly permitted by the CPRA or the CPRA Regulations; (iii) Processing Personal Information outside the direct business relationship between Hyland and Service Provider unless otherwise expressly permitted by the CPRA or the CPRA Regulations; (iv) Selling or Sharing Personal Information; (v) combining Personal Information with personal information that it receives from, or on behalf of, another person or persons, or Collects from its own interaction with a Consumer (except as permitted by the CPRA Regulations); or (vi) Processing the Personal Information for any other purpose except as permitted by this DPA.

d. Inability To Comply With CPRA: Service Provider shall, within 5 business days, notify Hyland after Service Provider determines that it no longer can meet its obligations under this Addendum, the CPRA or the CPRA Regulations. In the event of Service Provider's inability

to meet its obligations, Hyland may, in its discretion, (i) take reasonable and appropriate steps to stop and remediate any unauthorized use of Personal Information, or (ii) terminate the Service Agreement.

APPENDIX A

Security 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 those measures set forth in the Services Agreement and the DPA, including, 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 commitments and understand their obligations and responsibilities in relation to the Service Provider's 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 complexity, 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 and securely 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;
- An external audit program, tested at least annually; and
- Completed attestations, such as SOC 2 reports, shall be provided to Hyland upon written request.