PAAS SECURITY ATTACHMENT

Introduction: Hyland maintains and manages a comprehensive written security program that covers the Hyland Cloud Service designed to protect: (a) the security and integrity of Customer Data; (b) against threats and hazards that may negatively impact Customer Data; and (c) against unauthorized access to Customer Data, which such program includes the following:

I. Risk Management.

a. Conducting an annual risk assessment designed to identify threats and vulnerabilities in the administrative, physical, legal, regulatory, and technical safeguards used to protect the Hyland Cloud Service.

b. Maintaining a documented risk remediation process to assign ownership of identified risks, establish remediation plans and timeframes, and provide for periodic monitoring of progress.

II. Information Security Program.

a. Maintaining a documented comprehensive information security program that covers Hyland Cloud Service. This program will include policies and procedures based on industry standard practices, which may include ISO 27001/27002, or other equivalent standards.

b. Such information security program shall include, as applicable: (i) adequate physical and cyber security where Customer Data will be processed and/or stored; and (ii) reasonable precautions taken with respect to Hyland personnel employment.

c. These policies will be reviewed and updated by Hyland management annually.

III. Organization of Information Security. Assigning security responsibilities to appropriate Hyland individuals or groups to facilitate protection of the Hyland Cloud Service and associated assets.

IV. Human Resources Security.

a. Hyland employees undergo comprehensive screening during the hiring process. Background checks and reference validation will be performed to determine whether candidate qualifications are appropriate for the proposed position. Subject to any restrictions imposed by applicable law and based on jurisdiction, these background checks include criminal background checks, employment validation, and education verification as applicable.

b. Ensuring all Hyland employees are subject to confidentiality and non-disclosure commitments before access is provisioned to the Hyland Cloud Service or Customer Data.

c. Ensuring applicable Hyland employees receive security awareness training designed to provide such employees with information security knowledge to provide for the security, availability, and confidentiality of Customer Data.

d. Upon Hyland employee separation or change in roles, Hyland shall ensure any Hyland employee access to the Hyland Cloud Service is revoked in a timely manner and all applicable Hyland assets, both information and physical, are returned.

V. Asset Management.

a. Maintaining asset and information management policies and procedures. This includes ownership of assets, an inventory of assets, classification guidelines, and handling standards pertaining to Hyland assets.

b. The Hyland Cloud Service is hosted in the Amazon Web Services (AWS) Cloud where security and compliance are shared responsibilities between AWS and Hyland. AWS is responsible for protecting the infrastructure that runs all the services offered in the AWS Cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run AWS Cloud services. AWS operates, manages, and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the service operates. AWS Device Management Controls can be found here: https://aws.amazon.com/compliance/data-

center/controls/#Device_Management

VI. Access Controls.

a. Maintaining a logical access policy and corresponding procedures. The logical access procedures will define the request, approval and access provisioning process for Hyland personnel. The logical access process will restrict Hyland user (local and remote) access based on Hyland user job function (role/profile based, appropriate access) for applications and databases. Hyland user access recertification to determine access and privileges will be performed periodically. Procedures for onboarding and offboarding Hyland personnel users in a timely manner will be documented. Procedures for Hyland personnel user inactivity threshold leading to account suspension and removal threshold will be documented.

b. Limiting Hyland's access to Customer Data to its personnel who have a need to access Customer Data as a condition to Hyland's performance of the services under this Agreement. Hyland shall utilize the principle of "least privilege" and the concept of "minimum necessary" when determining the level of access for all Hyland users to Customer Data. Hyland shall require strong passwords subject to complexity requirements and periodic rotation and the use of multi-factor authentication.

c. Ensuring access controls are in place for Customer Data access by Hyland. Customer administrators control its user access, user permissions, and Customer Data retention to the extent such controls are available to Customer with respect to the Hyland Cloud Service.

VII. System Boundaries.

a. Hyland is not responsible for any system components that are not within the Hyland Cloud Service, including network devices, network connectivity, workstations, servers, and software owned and operated by the Customer or other third parties. Hyland may provide support for these components at its reasonable discretion.

b. The processes executed within the Hyland Cloud Service are limited to those that are executed by a Hyland employee (or Hyland authorized third party) or processes that are executed within Hyland's established system boundaries, in whole.

c. Certain business processes may cross these boundaries, meaning one or more tasks are executed outside of Hyland's established system boundaries for the Hyland Cloud Service, one or more tasks are executed by individuals who are not Hyland personnel (or authorized third-parties), or one or more tasks are executed based on written requests placed by Customer. In such event, Hyland will provide support for such processes to the extent they occur within Hyland's established system boundaries, but Hyland is not responsible for providing support for such processes to the extent they occur outside of such established system boundaries. At its reasonable discretion, Hyland may provide limited support for processes that occur outside such established system boundaries for the Hyland Cloud Service. Examples of business processes that cross these boundaries include, but are not limited to, Hyland Cloud Service configuration changes, processing that occurs within the Hyland Cloud Service, user authorization, and file transfers.

VIII. Encryption.

a. Customer Data shall only be uploaded to the Hyland Cloud Services in an encrypted format such as TLS/SSL, or other equivalent method.

b. Customer Data shall be encrypted at rest and in transit.

c. Where use of encryption functionality may be controlled or modified by Customer, in the event Customer elects to modify the use of or turn off any encryption functionality, Customer does so at its own risk.

IX. Physical and Environment Security.

a. The Hyland Cloud Service uses third party service providers who have demonstrated compliance with one or more of the following standards (or a reasonable equivalent): International Organization for Standardization ("ISO") 27001 and/or American Institute of Certified Public Accountants ("AICPA") Service Organization Controls ("SOC") Reports for Services Organizations. These providers provide Internet connectivity, physical security, power, and environmental systems and other services for the Hyland Cloud Service.

b. Hyland uses architecture and technologies designed to promote both security and high availability.

X. Operations Security.

a. Maintaining change management controls to ensure changes to Hyland Cloud Service production systems made by Hyland are properly authorized and reviewed prior to implementation. Customer is responsible for testing all configuration changes, authentication changes and upgrades implemented by Customer or implemented by Hyland at the request of Customer prior to production use of the Hyland Cloud Service. In cases where the Customer relies upon Hyland to implement changes on its behalf, a written request describing the change must be submitted (e.g. an e-mail, or another method provided by Hyland) by Customer's designated Customer Security Administrators ("CSAs") or set forth in a Services Proposal. Hyland will make scheduled configuration changes in accordance with the process set forth in the applicable PaaS Specification. Hyland may make configuration changes that are not expected to impact Customer during normal business hours.

b. Monitoring usage and capacity levels within the Hyland Cloud Service to adequately and proactively plan for future growth.

c. Utilizing virus and malware protection technologies, which are configured to meet common industry standards designed to protect the Customer Data and equipment located within the Hyland Cloud Service from virus infections or similar malicious payloads.

d. Implementing disaster recovery and business continuity procedures. These will include replication of Customer Data to a secondary location.

e. Maintaining a system and security logging process to capture system logs deemed critical by Hyland. These logs shall be maintained in accordance with the process set forth in the applicable PaaS Specification.

f. Maintaining system hardening requirements and configuration standards for components deployed within the Hyland Cloud Service. Ensuring servers, operating systems, and supporting software used in the Hyland Cloud Service receive all Critical and High (CVE score) security patches within a timely manner, but in no event more than 90 days after release, subject to the next sentence. In the event any such security patch would materially adversely affect the Hyland Cloud Service, then Hyland will use reasonable efforts to implement compensating controls until a security patch is available that would not materially adversely affect the Hyland Cloud Service.

g. Conducting vulnerability scans or analysis on at least a quarterly basis.

h. Conducting penetration tests on Hyland Cloud Service at least annually.

XI. Communications Security

a. Implementing security controls to protect information resources within the Hyland Cloud Service.

b. When supported, upon implementation and once annually thereafter, Customer may request Hyland limit access to Customer's Hyland Cloud Service to a list of pre-defined IP addresses at no additional cost.

XII. Supplier Relationships. Maintaining a Vendor Management Program for its critical vendors. This program will ensure critical vendors are evaluated on an annual basis.

XIII. Security Incidents are managed in accordance with the terms set forth in the applicable PaaS Specification. For purposes of this PaaS Security Attachment and as used within the applicable PaaS Specification, a "Security Incident" means a determination by Hyland of an actual disclosure of unencrypted Customer Data to an unauthorized person or entity that compromises the security, confidentiality, or integrity of the Customer Data.

XIV. Information Security Aspects of Business Continuity Management.

a. Maintaining a business continuity and disaster recovery plan.

b. Reviewing and testing this plan annually.

XV. Aggregated Data.

a. Hyland owns all Customer and User registration and billing data collected and used by Hyland that is required for user set-up, use and billing for the Hyland Cloud Service ("Account Information") and all aggregated, anonymized and statistical data derived from the use and operation of the Hyland Cloud Service, including without limitation, the number of records in the Hyland Cloud Service, the number and types of transactions, configurations, and reports

processed as part of the Hyland Cloud Service and the performance results of the Hyland Cloud Service (the "Aggregated Data").

b. Hyland may utilize the Account Information and Aggregated Data for purposes of operating Hyland's business. For clarity, Account Information and Aggregated Data does not include Customer Data.

XVI. Security Inquiries.

a. Monitoring its compliance with its information security program. This includes periodic internal reviews. Results are shared with Hyland leadership and deviations tracked through to remediation.

b. Maintaining a periodic external audit program. Completed attestations, such as available SOC 2 reports, are provided to Customer upon written request.

c. Customer may conduct audits of Hyland's operations that participate in the ongoing delivery and support of the Hyland Cloud Service purchased by Customer on an annual basis; provided Customer provides Hyland written notice of its desire to conduct such audit and the following criteria are met: (a) Hyland and Customer mutually agree upon the timing, scope, and criteria of such audit, which may include the completion of questionnaires supplied by Customer and guided review of policies, practices, procedures, Hyland Cloud Service configurations, invoices, or application logs, and (b) Customer agrees to pay Hyland fees (at Hyland's standard rates) for the Professional Services that are required or requested of Hyland in connection with such audit. Prior to any such audit, any third party engaged by Customer to assist with such audit, must be cleared by Hyland and enter into a Non-Disclosure Agreement directly with Hyland. If any documentation requested by Customer cannot be removed from Hyland's facilities as a result of physical limitations or policy restrictions, Hyland will allow Customer's auditors access to such documentation at Hyland's corporate headquarters in Ohio and may prohibit any type of copying or the taking of screen shots. Where necessary, Hyland will provide private and reasonable accommodation at Hyland's corporate headquarters in Ohio for data analysis and meetings. Upon reasonable notice, Hyland and Customer mutually agree to make necessary employees or contractors available for interviews in person or on the phone during such audit at Customer's cost and expense. Customer is prohibited from distributing or publishing the results of such audit to any third party without Hyland's prior written approval.