HYLAND EXPERIENCE SECURITY

For Hyland Experience, Hyland maintains and manages a comprehensive written security program that is 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. Such program includes the following:

1 Risk Management

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

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

2 Information Security Program

2.1 Maintaining a documented comprehensive information security program that includes policies and procedures based on industry standard practices, which may include ISO 27001/27002, or other equivalent standards. Such information security program shall include, as applicable: (a) adequate physical and cyber security where Customer Data will be processed and/or stored; and (b) reasonable precautions taken with respect to Hyland personnel employment.

2.2 Reviewing and updating such policies annually.

3 Organization of Information Security. Assigning security responsibilities to appropriate individuals or groups to facilitate protection of Hyland Experience and associated assets.

4 Human Resources Security

4.1 Requiring all Hyland employees to undergo a comprehensive screening during the hiring process.

4.2 Performing background checks and reference validation to determine whether candidate qualifications are appropriate for the proposed position.

4.3 Subject to any restrictions imposed by applicable law and based on jurisdiction, conducting criminal background checks, employment validation, and education verification as applicable.

4.4 Ensuring all Hyland employees are subject to confidentiality and non-disclosure commitments before access is provisioned to Hyland Experience or Customer Data.

4.5 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.

4.6 Upon Hyland employee separation or change in roles, ensuring any Hyland employee’s access to Hyland Experience is revoked in a timely manner and all applicable Hyland assets, both information and physical, are returned.

5 Asset Management

5.1 Ensuring Customer Data is encrypted and stored in a secure location subject to strict physical access controls.

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

5.3 Note: Hyland Experience 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, including media handling and decommissioning. AWS Device Management Controls can be found here: https://aws.amazon.com/compliance/data-center/controls/#Device_Management

6 Access Controls

6.1 Maintaining an access policy and corresponding procedures. The access procedures will define the request, approval, and access provisioning process for Hyland personnel. The 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.

6.2 Documenting procedures for: (a)onboarding and offboarding Hyland personnel users in a timely manner; and (b) Hyland personnel user inactivity threshold leading to account suspension and removal threshold.

6.3 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. For such Hyland employees, Hyland shall utilize the principle of "least privilege" and the concept of "minimum necessary." Hyland shall require strong passwords subject to complexity requirements and periodic rotation and the use of multi-factor authentication.

6.4 Ensuring access controls are in place for Customer Data access by Hyland. Note: Customer controls its: user's access, user's permissions, and Customer Data retention to the extent such controls are available to Customer.

7 System Boundaries

7.1 Note: Hyland is not responsible for any system components that are not within Hyland Experience, including network devices, network connectivity, workstations, servers, and software owned and operated by the Customer or other third parties.

7.2 Note: The processes executed within Hyland Experience 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.

7.3 Note: Certain business processes may cross these boundaries, meaning one or more tasks are executed outside of Hyland's established system boundaries for Hyland Experience, 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. Examples of business processes that cross these boundaries include, but are not limited to, Hyland Experience configuration changes, processing that occurs within Hyland Experience, user authorization, and file transfers.

8 Encryption

8.1 Ensuring Customer Data shall only be uploaded to Hyland Experience in a supported encrypted format such as TLS or other equivalent method.

8.2 Encrypting Customer Data at rest and in transit over public networks.

8.3 Note: Where use of encryption functionality may be controlled or modified by Customer and Customer elects to modify its use of or turn off any encryption functionality, Customer does so at its own risk.

9 Operations Security

9.1 Maintaining change management controls to ensure changes made by Hyland to production systems are properly authorized and reviewed prior to implementation. Note: Customer is responsible for testing all configuration changes, authentication changes and upgrades implemented by Customer or Hyland. If Customer requests Hyland to implement changes on its behalf, such request must be in writing and submitted by Customer's designated Authorized Customer Administrators via a support case or set forth in a separate agreement.

9.2 Making scheduled configuration changes that are expected to impact Customer access to Hyland Experience during a planned maintenance window. Note: Hyland may make configuration changes that are not expected to impact Customer during normal business hours.

9.3 Utilizing technologies that are configured to meet common industry standards designed to protect the Customer Data within Hyland Experience from virus infections or similar malicious payloads.

9.4 Implementing disaster recovery and business continuity procedures in accordance with the applicable Service Level purchased by Customer.

9.5 Maintaining security logs for one year.

9.6 Maintaining system hardening requirements and configuration standards for components deployed within Hyland Experience.

9.7 Conducting vulnerability scans on a regular basis and remediating in a timely manner. In the event any security patch would materially adversely affect Hyland Experience, then Hyland will use reasonable efforts to implement compensating controls until a security patch is available that would not materially adversely affect Hyland Experience. Upon written request, Hyland will provide an executive summary report of its most recent external vulnerability scan.

9.8 Conducting external penetration tests at least annually against an instance of Hyland Experience that is representative of the configuration used by Customers generally and making an executive summary of the most recent penetration test to Customer upon request.

9.9 Permitting Customer to, on an annual basis (but no more than once during any 12-month period), conduct a penetration test against a Hyland Experience website, setup by Hyland, that is authorized for penetration testing , provided: (1) Customer submits a Penetration Testing Authorization form in advance; (2) prior to conducting such testing, Hyland and Customer mutually agree upon the timing, scope, and price, (3) such testing is at Customer's sole cost and expense; and (4) if Customer engages a third-party to assist with such testing, the third-party must first be cleared by Hyland and enter into a Non-Disclosure Agreement directly with Hyland. Note: Any testing performed without mutual agreement regarding timing, scope, and criteria may be considered a hostile attack, which may trigger automated and manual responses, including reporting the activity to local and federal law enforcement agencies as well as immediate suspension of Customer's access to or use of Hyland Experience; and Customer is prohibited from distributing or publishing the results of such penetration testing without Hyland's prior written approval.

9.10 Maintaining a 24/7 security operations center.

10 Supplier Relationships. Maintaining a Vendor Management Program for its critical vendors and evaluating critical vendors on an annual basis.

11 Security Incident Response

11.1 Employing incident response standards that are based upon applicable industry standards, such as ISO 27001 and National Institute for Standards and Technology ("NIST"), to maintain the information security components of Hyland Experience environment.

11.2 Responses to these incidents follow the Hyland documented incident response sequence. This sequence includes the incident trigger phase, evaluation phase, escalation phase, response phase, recovery phase, de-escalation phase, and post-incident review phase.

11.3 If Hyland has determined Customer's instance of Hyland Experience has been negatively impacted by a security incident, delivering a root cause analysis summary. Such notice will not be unreasonably delayed but will occur after initial corrective actions have been taken to contain the security threat or stabilize Hyland Experience.

11.4 The root cause analysis will include the duration of the event, resolution, technical summary, outstanding issues, and follow-up, including steps Customer needs to take to prevent further issues. Hyland Experience information including data elements that require additional confidentiality and security measures (including that of other customers impacted in the event) will not be publicly disclosed. If Customer needs additional details of an incident, a request to the applicable Hyland Cloud support team must be submitted and handled on a case-by-case basis to protect the confidentiality and security of the requested information.

11.5 Notifying Customer of a Security Incident within 48 hours. 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.

12 Information Security Aspects of Business Continuity Management

12.1 Maintaining a business continuity and disaster recovery plan.

12.2 Reviewing and testing the business continuity and disaster recovery processes annually.

13 Audits and Assessments

13.1 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.

13.2 Maintaining a periodic external audit program. Completed attestations are provided to Customer upon written request.

13.3 Permitting Customer to, on an annual basis (but no more than once during any 12-month period), conduct audits (which includes assessments, questionnaires, guided reviews or other requests to validate Hyland's security controls) of Hyland's operations that participate in the ongoing delivery and support of Hyland Experience (each, a "Security Inquiry"), provided, that:

(a) the proposed Security Inquiry does not overlap with, or otherwise cover the same or similar information as, or scope of: (1) any controls already provided for by an external audit or assessment already performed by Hyland, such as a SOC 2 report, ISO 27001 or other similar audit or assessment that is made available to Customer upon Customer's request; or (2) any content already provided by Hyland through its completed SIG, CAIQ or similar questionnaire that is made available to Customer upon request.

(b) Hyland and Customer mutually agree upon the timing, scope, fees (if any), and criteria of such Security Inquiry;

(c) confidential and restricted documentation, such as Hyland internal policies, practices, and procedures, including any documentation requested by Customer that cannot be removed from Hyland's premises as a result of physical limitations or policy restrictions will not be provided externally or removed from Hyland's premises and such reviews must either (at Hyland's election) be conducted onsite at Hyland's corporate headquarters in Ohio or through a secure screenshare which may be arranged by Hyland to prohibit any type of copying or screen shots;

(d) Hyland will not permit access to internal systems or devices used to host or support Hyland's offerings; and

(e) to the extent Customer desires to engage a third party to perform such Security Inquiry: (1) Hyland must approve of such third party in writing in advance, (2) Customer shall cause such third party to: (A) enter into a Non-Disclosure Agreement with Hyland and (B) agree to abide by Hyland's security standards, and (3) Customer shall manage the engagement with the third party and ensure the third party understands the scope of the Security Inquiry as mutually agreed upon between Hyland and Customer and how Customer utilizes the Hyland Cloud Service.

Where necessary, Hyland will provide private and reasonable accommodation at Hyland's corporate headquarters in Ohio for data analysis and meetings. Upon reasonable advance written request, Hyland and Customer may mutually agree to make necessary employees or contractors available for interviews in person or on the phone during such Security Inquiry at Customer's cost and expense. Customer is prohibited, , and Customer shall prohibit each third-party engaged to perform a Security Inquiry from distributing or publishing the results of such Security Inquiry without Hyland's prior written approval. Notwithstanding anything to the contrary within this Agreement, nothing in this Agreement (including this section) will require Hyland or any of its affiliates to disclose information that is subject to attorney-client privilege.

[This version shall be in effect as of 11:59 p.m. ET of the date stamped on such online version.]