EXHIBIT A

HYLAND CLOUD SERVICE TABLE

INITIAL COMPONENTS OF HYLAND CLOUD SERVICE
Initial Service Class Package: Gold **Initial data storage allocation:** 500 gigabytes **Initial data center location:** United States of America

1. DEFINED TERMS

All capitalized terms used in this Exhibit A shall have the meanings ascribed them in this Exhibit A.

"Customer Data" means any and all electronic data and information submitted by City or Users to the Hyland Cloud Service.

"Documentation" means: (1) to the extent available, the "Help Files" included in the Software, or (2) if no such "Help Files" are included in the Software, such other documentation published by Hyland, in each case, which relate to the functional, operational or performance characteristics of the Software.

"Host Web Site" means the web site hosted by Hyland as part of the Hyland Cloud Service on a web server included in the Hyland Cloud Platform used to access the Hyland Cloud Service.

"Hyland Cloud Service" means Hyland's provision of Software and the Hyland Cloud Platform for use by City in accordance with the Agreement.

"Hyland Cloud Service Support" means the services provided by Reseller pursuant to a Hyland Cloud Service Maintenance Agreement.

"Hosted 3rd Party Software" means all third party software products (other than third party software products bundled by Hyland as a part of the Software) provided by Hyland as part of the Hyland Cloud Service.

"Hyland Cloud Service Maintenance Agreement" means the agreement entered into by and between City and Reseller relating to maintenance and technical support to be provided by Reseller to City in connection with the Hyland Cloud Service.

"Hyland Cloud Platform" means the Physical Infrastructure and any composite software layers such as databases, operating systems, virtualization technology, Hosted 3rd Party Software, and Host Web Site, responsible for providing the Hyland Cloud Service, whether owned by Hyland or a third party.

"Physical Infrastructure" means the physical hardware and infrastructure which Hyland uses to provide the Hyland Cloud Service (which may include servers, network devices, cabling, CPU, data centers, memory, storage, switches, firewalls, routers and other network devices) whether owned by Hyland or a third party services provider.

"Reseller" means the authorized solution provider of Hyland from which City has ordered and agreed to purchase the right to use the Hyland Cloud Service under the Agreement.

"Service Class" means the service level commitment included as part of Hyland Cloud Service, as described in the Service Class Manual, and purchased by City as part of the Hyland Cloud Service.

"Service Class Manual" means the latest version of the manual describing the Service Classes, as posted by Hyland from time to time on a website designated by Hyland.

"Software" means Hyland's proprietary software products included from time to time in the Hyland Cloud Service, including third party software bundled by Hyland together with Hyland's proprietary software products as a unified product.

"Testing Environment" means a separate instance of the Hyland Cloud Service (including Customer Data) hosted by Hyland, for use by City solely with production data in a non-production environment for the limited purpose of functional and performance testing of the Software and environment and Hosted 3rd Party Software.

"Testing Lite Environment" means a separate instance of the Hyland Cloud Service (including Customer Data) hosted by Hyland, for use by City solely with production data in a non-production environment for the limited purpose of functional testing of the Software and environment and Hosted 3rd Party Software.

"Users" means City's employees that access and use the Hyland Cloud Service.

2. HYLAND CLOUD SCOPE OF SERVICES

2.1 General. During the term of the Agreement, Hyland will: (a) make the Hyland Cloud Service available to City pursuant to the Agreement, including (i) this Exhibit A, (ii) the SaaS Security Attachment, (iii) Documentation and (iv) applicable Service Class Manual; and (b) only use Customer Data to provide, develop, and improve the Hyland Cloud Service and other services, to prevent or address service or technical problems, or in accordance with City's instructions.

2.2 Service Class Manual. Prior to the date of the Agreement, Hyland has delivered a then-current copy of the Service Class Manual to City. Hyland has the right to modify the Service Class Manual (including the right to issue an entirely restated Service Class Manual) from time to time. The modifications or the revised Service Class Manual, effective thirty (30) days after Hyland provides written notice to City informing City of Hyland's posting of such modifications or revisions on the website identified in such notice. Notwithstanding the foregoing no modifications of the Service Class Manual relating to City's then-current Service Class will be effective until the next renewal of the term of the Agreement. The initial Service Class purchased by City is set forth in the initial Hyland Cloud Service Table. City may upgrade the Service Class at any time but may downgrade such Service Class only after the expiration of the Initial Term (as defined below) of the Agreement. In the event City elects to downgrade such Service Class, such downgrade will not be effective until the beginning of the next renewal of the Agreement. To modify a Service Class selection, City must submit a purchase order to Reseller indicating the new Service Class.

2.3 Return of Customer Data and Deletion. Upon termination or expiration of the Agreement for any reason:

(a) Upon written request by City to Hyland sent to cloud@hyland.com, made within thirty (30) days after the effective date of any such termination or expiration, for Customer Data extraction services ("Notice of Return of Customer Data"), Hyland will either: (1) return Customer Data to City by providing: Customer Data on one (1) or more encrypted hard drives or other similar media and an export file containing the relevant keyword values and related file locations for the Customer Data, or (2) make available to City the Customer Data for extraction by City. Hyland will work with City on determining the extraction method most suitable to meet City's requirements. City acknowledges and agrees that thirty (30) days after Hyland has sent or made available to City the Customer Data, Hyland shall have no obligation to maintain or provide any Customer Data and shall thereafter, unless legally prohibited, delete all such Customer Data from all of Hyland's datacenters, including all replicated copies.

(b) Upon written request by City to Hyland sent to cloud@hyland.com, made within thirty (30) days after the effective date of any such termination or expiration, for the deletion of Customer Data ("Notice of Deletion of Customer Data"), Hyland will have no obligation to maintain or provide any Customer Data and shall thereafter, unless legally prohibited, delete all Customer Data from all of Hyland's datacenters, including all replicated copies.

(c) If City does not provide the Notice of Return of Customer Data or the Notice of Deletion of Customer Data in accordance with paragraph (a) or (b) above, City acknowledges and agrees that thirty (30) days after any termination or expiration of the Agreement, Hyland will have no obligation to maintain or provide any Customer Data and shall thereafter, unless legally prohibited, delete all Customer Data from all of Hyland's datacenters, including all replicated copies.

2.4 Data Location. Hyland shall store Customer Data at data centers located in the country(ies) indicated in the initial Hyland Cloud Service Table. Hyland may, at its expense, change the location of the Customer Data to other data centers; provided that such locations remain in that country.

2.5 City may license some Software as part of the Hyland Cloud Service, and other Software which is implemented only on the customer's premise (or a third party cloud other than the Hyland Cloud Platform), such as Hyland RPA ("On-Premise Software"). For clarity, if City licenses On-Premise Software from Hyland, Reseller or any other Hyland authorized solution provider, the Agreement does not apply to such On-Premise Software.

3. GRANT OF RIGHTS AND PROHIBITED ACTS

3.1 Hyland Cloud Service Use Grant. During the term of the Agreement, Hyland grants to City a revocable, non-exclusive, non-assignable (except as provided in the Agreement), limited right to use the Hyland Cloud Service as provided by Hyland, and the associated Documentation, solely for use by City and its Users for the internal business purposes of City, and only for capturing, storing, processing and accessing City's own data.

The Hyland Cloud Service is for use by City and its Users and may not be used for processing of third-party data as a service bureau, application service provider or otherwise. City and its Users shall not make any use of the Hyland Cloud Service in any manner not expressly permitted by the Agreement. City acknowledges that it may only access Customer Data via the Hyland Cloud Service and shall only access the Hyland Cloud Service in a manner consistent with the Agreement and the Documentation. Use of software or hardware that reduces the number of Users directly accessing or utilizing the Hyland Cloud Service (e.g. by using "multiplexing" or "pooling" software or hardware) does not reduce the number of users accessing the Hyland Cloud Services for purposes of calculating the number of users, as the required number of users would equal the number of distinct inputs to such software or hardware (e.g. to such "multiplexing" or "pooling" software or hardware). City is prohibited from using any software (including bots) other than the Software client modules or a Software application programming interface (API) to access the Hyland Cloud Service or any data stored in the Software database for any purpose other than generating reports or statistics regarding system utilization, unless Hyland has given its prior written consent to City's use of such other software and City has paid to Reseller or Hyland the fees required for such access. City further acknowledges that all components of the Hyland Cloud Service made available by Hyland, including any components downloaded or installed locally on City's or Users' systems, are solely for use with the Hyland Cloud Service and are not intended to be used on a stand-alone basis.

3.2 Volume Use Restriction. There are certain Software products Hyland makes available and which City may purchase for use as part of the Hyland Cloud Service that are volume-based may: (i) no longer function if applicable volume limits have been exceeded; (ii) require City to pay additional fees based on City's volume usage; or (iii) include functionality which monitors or tracks City usage and reports that usage. City may not circumvent or attempt to circumvent this restriction by any means, including but not limited to changing the computer calendars.

3.3 Test Environments. City may purchase limited access to Testing Environments or Testing Lite Environments, or both. Hyland agrees that the security measures described in the SaaS Security Attachment are also applied to the Testing Environment and Testing Lite Environment. Hyland reserves the right to further define the permitted use(s) and/or restrict the use(s) of the Testing Environment and Testing Lite Environment. If, at any time, City is not satisfied with the Testing Environment or Testing Lite Environment, City's sole and exclusive remedy shall be to stop using the Testing Environment or Testing Lite Environment.

3.4 No High Risk Use. The Hyland Cloud Service is not fault-tolerant and is not guaranteed to be error free or to operate uninterrupted. The Hyland Cloud Service is not designed or intended for use in any situation where failure or fault of any kind of the Hyland Cloud Service could lead to death or serious bodily injury to any person, or to severe physical or environmental damage ("High Risk Use"). City is not permitted to use the Hyland Cloud Service in, or in conjunction with, High Risk Use. High Risk Use is STRICTLY PROHIBITED. High Risk Use includes, for example, the following: aircraft or other modes of human mass transportation, nuclear or chemical facilities, life support systems, implantable medical equipment, motor vehicles, or weaponry systems. High Risk Use does not include utilization of the Hyland Cloud Service for administrative purposes, as an information resource for medical professionals, to store configuration data, engineering and/or configuration tools, or other non-control applications, the failure of which would not result in death, personal injury, or severe physical or environmental damage. These non-controlling applications may communicate with the applications that perform the control, but must not be directly or indirectly responsible for the control function. City agrees not to use, distribute, license, or grant the use of the Hyland Cloud Service in, or in connection with, any High Risk Use." City agrees to be responsible for any third-party claim arising out of City's use of the Hyland Cloud Service in connection with any High Risk Use.

3.5 Audit Rights. Upon reasonable notice to City, Hyland shall be permitted access to audit City's use of the Hyland Cloud Service in order to determine City's compliance with the grant of use, including, where applicable, to measure City's volume usage. City shall reasonably cooperate with Hyland with respect to its performance of such audit.

3.6 Third Party Services and Content. The Hyland Cloud Service may contain functionality which allows City to: (a) access, link or integrate the Hyland Cloud Service with City's applications or applications or services provided by third parties and (b) access third party websites and content. Hyland has no responsibility for such applications or services, websites or content and shall have no responsibility for any disclosure, modification or deletion of Customer Data resulting from any such access or use by such applications or services. Any activities engaged in by City or any of its Users with such third parties using the Hyland Cloud Service is solely between City and such third party and Hyland has no liability, obligation or responsibility for any such activities. Hyland does not endorse any third party web sites, applications or services that may be linked or integrated through the Hyland Cloud Service. Hyland is not responsible for any third party content, products or materials purchased, accessed or used by City or its Users using the Hyland Cloud Service.

3.7 Prohibited Conduct. City agrees not to: (a) remove copyright, trademark or other proprietary rights notices that appear during the use of the Software, Hyland Cloud Service, Documentation, or Hosted 3rd Party Software documentation; (b) sell, transfer, rent, lease or sub-license the Software, Documentation, Hyland Cloud Service, or Hosted 3rd Party Software documentation to any third party; (c) alter or modify the Software, Documentation, Hyland Cloud Service or Hosted 3rd Party Software documentation; (d) reverse engineer, disassemble, decompile or attempt to derive source code from the Software, Documentation, Hyland Cloud Service, or Hosted 3rd Party Software documentation, or prepare derivative works therefrom; or (e) use the Hyland Cloud Service or permit it to be used in violation of Hyland's Acceptable Use Policy in effect from time to time (a copy of the current form of which is attached hereto as Acceptable Use Policy Attachment) or for the purposes of evaluation, benchmarking, or other comparative analysis intended for external publication without Hyland's prior written consent.

3.8 Ownership of Customer Data. As between Hyland and City, City owns Customer Data.

3.9 City Input and Suggestions. Hyland shall have a royalty-free, worldwide, perpetual, transferable, sub-licensable, and irrevocable license to use or incorporate into any of Hyland's products or services, including the Hyland Cloud Services, any suggestions, enhancements, improvements, recommendations or any other feedback provided by City, including Users, related to the operation or use of the Hyland Cloud Service.

4. PRICING AND HYLAND CLOUD SERVICE SUPPORT

4.1 Pricing. City acknowledges and agrees that it has purchased the right to use the Hyland Cloud Service from Reseller. Accordingly, unless and until Hyland notifies City in writing to the contrary, all fees and charges with respect to the Hyland Cloud Service shall be mutually agreed upon by City and Reseller, and the Reseller will invoice City for all such fees and charges. City agrees to make any and all payments of such fees and charges to the Reseller pursuant to such mutually agreed terms.

4.2 Hyland Cloud Service Support**.** Unless and until Hyland provides written notice to City to the contrary, City shall purchase maintenance and technical support of the Software and other hardware and software components of the Hyland Cloud Service from Reseller pursuant to the terms of a Hyland Cloud Service Maintenance Agreement between City and Reseller. Hyland is not obligated under the Agreement to provide to City any maintenance or technical support with respect to the Hyland Cloud Service.

4.3 Notice from Hyland. If Hyland provides written notice as described in 4.1 and 4.2 above, Hyland and City shall use reasonable efforts to enter into a mutually agreeable amendment to the Agreement pursuant to which, among other things, City shall agree to pay applicable fees and charges relating to the Hyland Cloud Service directly to Hyland and Hyland shall agree to provide maintenance and technical support of the Hyland Cloud Service directly to City.

5. U.S. GOVERNMENT END USERS. To the extent applicable to City, the terms and conditions of the Agreement shall pertain to the U.S. Government's use and/or disclosure of the Hyland Cloud Service, and shall supersede any conflicting contractual terms or conditions. By accepting the terms of the Agreement and/or the delivery of the Hyland Cloud Service, the U.S. Government hereby agrees that the Software, Hosted 3rd Party Software included in the Hyland Cloud Service qualify as "commercial" computer software within the meaning of ALL U.S. federal acquisition regulation(s) applicable to this procurement and that the Software is developed exclusively at private expense. If this license fails to meet the U.S. Government's needs or is inconsistent in any respect with Federal law, the U.S. Government agrees to return this Hyland Cloud Service to Hyland. In addition to the foregoing, where DFARS is applicable, use, modification, reproduction, release, display, or disclosure of the Hyland Cloud Service, or Documentation by the U.S. Government is subject solely to the terms of the Agreement, as stated in DFARS 227.7202, and the terms of the Agreement shall supersede any conflicting contractual term or conditions.

6. SECURITY. During the term of the Agreement, Hyland shall maintain a security program which shall conform to the SaaS Security Attachment, attached hereto.

7. OWNERSHIP. Hyland and its suppliers own the Software, Documentation, and all components of the Hyland Cloud Service, including, without limitation, any and all worldwide copyrights, patents, trade secrets, trademarks and proprietary and confidential information rights in or associated with the foregoing. The Software, Documentation, and Hyland Cloud Service are protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. No ownership rights in the Software, Documentation, or Hyland Cloud Service are transferred to City. City agrees that nothing in the Agreement or associated documents gives it any right, title or interest in the Software, Documentation, or Hyland Cloud Services, except for the limited express rights granted in the Agreement. City acknowledges and agrees that, with respect to Hyland's end users generally, Hyland has the right, at any time, to change the specifications and operating characteristics of the Software and Hyland Cloud Service, and Hyland's policies respecting upgrades and enhancements (including but not limited to

its release process). THE AGREEMENT IS NOT A WORK-FOR-HIRE AGREEMENT. At no time will City file or obtain any lien or security interest in or on any components of the Software, Documentation, or Hyland Cloud Service.

8. CERTAIN RESPONSIBILITIES AND OBLIGATIONS OF CITY

8.1 City Responsibilities. In connection with the relationship established between City and Hyland under the Agreement:

(a) except as otherwise expressly permitted under the terms of the Agreement, City will not permit or authorize any third parties (such as persons or legal entities) to use the Hyland Cloud Service;

(b) City will comply with Hyland's Acceptable Use Policy, as in effect from time to time, a copy of the current form of which is attached hereto as Acceptable Use Policy Attachment.

(c) City is responsible for all Users use and all access through City and its Users of the Hyland Cloud Service and compliance with the Agreement, including, but not limited to, (i) setting-up User log-in accounts/credentials (e.g. user names, passwords, tokens, etc.) to the Hyland Cloud Service and immediately revoking User accounts/credentials when User no longer requires access to the Hyland Cloud Service, and (ii) shall not permit Users to share log-in accounts/credentials;

(d) City has sole responsibility for the accuracy, quality, content and legality of all Customer Data;

(e) City shall prohibit unauthorized access to, or use of, the Hyland Cloud Service and shall notify Hyland promptly of any such unauthorized access or use by contacting Reseller;

(f) City understands and agrees: (i) City has an independent duty to comply with any and all laws applicable to it, (ii) its use of the Hyland Cloud Service and compliance with any terms and conditions under the Agreement does not constitute compliance with any law; (iii) it shall make use of available Hyland Cloud Service security features and controls to properly transmit, store, process and provide access to Customer Data; and (iv) it shall use the tools and reporting capabilities made available in the Hyland Cloud Service to monitor and confirm Customer Data processing, such as batch processing of electronic documents uploaded to the Hyland Cloud Service.

(g) City acknowledges that Reseller or City shall designate one or more City Security Administrators to interact directly with Hyland regarding City's Hyland Cloud Service. "City Security Administrators" (also referred to as "CSA" or "CSAs") are individuals designated by Reseller or City who are authorized to submit Hyland Cloud Service configuration change requests, speak authoritatively on behalf of City's Hyland Cloud Service and shall receive and provide, as applicable, all notifications related to maintenance, security, service failures and the like. City further acknowledges that where Reseller acts on behalf of City as it relates to actions or obligations under the SaaS Security Attachment, Hyland will rely on Reseller as if Reseller were City in such instances.

(h) City may give any of its Users the rights to act as a system administrator, through the configuration tools included in the Software for the Hyland Cloud Service. Hyland has no responsibility or obligations in connection with City's internal management or administration of City's Hyland Cloud Service.

8.2 City Internet Connection. City is responsible for obtaining and maintaining all software, hardware (including without limitation network systems), telephonic or other communications circuits, and Internet Service Provider relationships that are necessary or appropriate for City to properly access and use the Hyland Cloud Service. Hyland shall have no responsibility or liability under the Agreement for any unavailability or failure of, or nonconformity or defect in, the Hyland Cloud Service that is caused by or related in any manner to any failure of City to obtain and maintain all such software, hardware, equipment and relationships.

9. CONFIDENTIAL INFORMATION

9.1 "Confidential Information" shall mean Customer Data and such information that is marked "Proprietary" or "Confidential," that is known by the recipient to be confidential or that is of such a nature as customarily would be confidential between business parties, except as provided in the next sentence. Confidential Information shall not include information that: (a) is or becomes generally known to the public without breach of the Agreement by the recipient, or (b) is demonstrated by the recipient to have been in the recipient's possession prior to its disclosure by the disclosing party, or (c) is received by the recipient from a third party that is not bound by restrictions, obligations or duties of non-disclosure to the disclosing party, or (d) is demonstrated by recipient to have been independently developed by recipient without reference to the other party's information.

9.2 Each party agrees that, with respect to the Confidential Information of the other party, or its affiliates, such party as a recipient shall use the same degree of care to protect the other party's Confidential Information that such party uses to protect its

own confidential information, but in any event not less than reasonable care; and not use or disclose to any third party any such Confidential Information, except as may be required by law or court order or as provided under the Agreement. City agrees to take all reasonable steps to protect all Software, Hyland Cloud Services, and any related Documentation, delivered by Hyland to City under the Agreement from unauthorized copying or use. Each party shall be liable and responsible for any breach of this Section 9 committed by any of such party's employees, agents, consultants, contractors or representatives.

10. LIMITED WARRANTIES; WARRANTY DISCLAIMER

10.1 Hyland Cloud Service Limited Warranty. Hyland warrants to City that, during the term of the Agreement, the Hyland Cloud Service will function in all material respects as described in the Documentation. The terms of this warranty shall not apply to, and Hyland shall have no liability for any non-conformity related to, the Hyland Cloud Service if: (a) any component of the Hyland Cloud Service has been modified, misused or abused by City or a third party, (ii) any such non-conformity arises from or is related to problems within or impacting City's computing environment, including any City third party software applications, hardware, network or internet connectivity, or (iii) if the Hyland Cloud Service is used in combination with equipment or software other than that which is provided by Hyland or is consistent with the Documentation.

10.2 Hyland Cloud Service Warranty Remedy. Hyland's sole obligation, and City's sole and exclusive remedy for a non-conformities to the express limited warranties under Section 10.1 shall be as follows: provided that City notifies Hyland in writing of the non-conformity, Hyland will either: (a) correct the non-conforming component of the Hyland Cloud Service, which may include the delivery of a reasonable workaround for the non-conformity; or (b) if Hyland determines that correction of the non-conformity is not commercially practicable, then terminate the Agreement, in which event Hyland will cause to be refunded to City the "unused portion of pre-paid subscription fees" (as defined below) related to the non-conforming component of the Hyland Cloud Service which have been paid by City to Reseller prior to the time of such termination. The "unused portion of the prepaid subscription" shall mean an amount equal to the total usage fees paid by City to Reseller for the non-conforming portion of the Hyland Cloud Service for the then current term (or applicable twelve-month period within the Initial Term) during which such removal occurs, multiplied by a fraction, the numerator of which shall be the number of full calendar months remaining during the term (or applicable twelve-month period within the Initial Term) during which such removal occurs, and the denominator of which shall be twelve (12).

10.3 City Limited Warranty. City represents and warrants to Hyland that: (a) City and its Users are the legal custodian of the Customer Data and it has the right and authority to use the Hyland Cloud Service in connection with all Customer Data and other materials hereunder; (b) City will use reasonable efforts to ensure that any Customer Data submitted to Hyland via electronic media will be free of viruses; and (c) any User submitting Customer Data to Hyland for use in connection with the Hyland Cloud Service has the legal authority to do so, either through ownership of the Customer Data or by obtaining appropriate authorizations therefor, and that submission of Customer Data does not violate any contracts, agreements, or any applicable law. City is responsible for all Customer Data that is submitted to Hyland for use in connection with the Hyland Cloud Service.

10.4 EXCEPT FOR THE WARRANTIES PROVIDED BY A PARTY AS EXPRESSLY SET FORTH IN THIS SECTION 11 EACH PARTY (AND, IN THE CASE OF HYLAND, ITS SUPPLIERS) MAKE NO WARRANTIES OR REPRESENTATIONS REGARDING ANY SOFTWARE, HYLAND CLOUD SERVICE (INCLUDING ANY HARDWARE OR SOFTWARE) OR ANY INFORMATION PROVIDED UNDER THE AGREEMENT. EACH PARTY (AND, IN THE CASE OF HYLAND, ITS SUPPLIERS) DISCLAIM AND EXCLUDE ANY AND ALL OTHER EXPRESS, IMPLIED AND STATUTORY WARRANTIES, INCLUDING, WITHOUT LIMITATION, WARRANTIES OF GOOD TITLE, WARRANTIES AGAINST INFRINGEMENT, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AND WARRANTIES THAT MAY ARISE OR BE DEEMED TO ARISE FROM ANY COURSE OF PERFORMANCE, COURSE OF DEALING OR USAGE OF TRADE. HYLAND AND ITS SUPPLIERS DO NOT WARRANT THAT ANY SOFTWARE OR HYLAND CLOUD SERVICE PROVIDED UNDER THE AGREEMENT WILL BE UNINTERRUPTED. EXCEPT AS EXPRESSLY STATED IN THE AGREEMENT, HYLAND DOES NOT ASSUME ANY LIABILITY WHATSOEVER WITH RESPECT TO ANY THIRD PARTY HARDWARE, FIRMWARE, SOFTWARE OR SERVICES (OTHER THAN "HOSTED 3RD PARTY SOFTWARE").

10.5 CITY SPECIFICALLY ASSUMES RESPONSIBILITY FOR THE SELECTION OF THE SOFTWARE AND HYLAND CLOUD SERVICE TO ACHIEVE ITS BUSINESS OBJECTIVES.

10.6 HYLAND MAKES NO WARRANTIES WITH RESPECT TO ANY SOFTWARE OR HYLAND CLOUD SERVICES USED IN ANY NON-PRODUCTION SYSTEM AND PROVIDES ANY SUCH SOFTWARE AND HYLAND CLOUD SERVICE "AS IS."

11.7 No oral or written information given by Hyland, its agents, or employees shall create any additional warranty. No modification or addition to the limited warranties set forth in the Agreement is authorized unless it is set forth in writing, references the Agreement, and is signed on behalf of Hyland by a corporate officer.

12. LIMITATIONS OF LIABILITY

12.1 EXCEPT TO THE EXTENT PROHIBITED BY LAW, IN NO EVENT SHALL HYLAND'S (INCLUDING ITS AFFILIATES' AND DIRECT OR INDIRECT SUPPLIERS') AGGREGATE LIABILITY ARISING OUT OF OR IN CONNECTION WITH THE AGREEMENT OR IN CONNECTION OR ANY USE OR INABILITY TO USE THE SOFTWARE OR HYLAND CLOUD SERVICE EXCEED THE AMOUNT OF THE FEES AND CHARGES ACTUALLY PAID BY CITY TO THE RESELLER OR HYLAND UNDER THE AGREEMENT DURING THE 24- MONTH PERIOD IMMEDIATELY PRECEDING THE EVENT GIVING RISE TO SUCH LIABILITY. IN NO EVENT WILL HYLAND (OR ITS AFFILIATES, DIRECT OR INDIRECT SUPPLIERS) BE LIABLE FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL OR PUNITIVE DAMAGES OR OTHER PECUNIARY LOSS INCLUDING, WITHOUT LIMITATION, LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF DATA OR INFORMATION, THE COST OF RECOVERING SUCH DATA OR INFORMATION, THE COST OF SUBSTITUTE SOFTWARE, HARDWARE OR SERVICES, OR CLAIMS BY THIRD PARTIES, ARISING OUT OF OR IN CONNECTION WITH THE AGREEMENT OR ANY USE OR INABILITY TO USE THE SOFTWARE OR HYLAND CLOUD SERVICE, EVEN IF HYLAND OR SUCH AFFILIATES OR SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITIES OF SUCH DAMAGES.

12.2 IF CITY USES THE SOFTWARE IN A CLINICAL SETTING, CITY ACKNOWLEDGES THAT THE SOFTWARE DOES NOT OFFER MEDICAL INTERPRETATIONS OF DATA, DIAGNOSE PATIENTS, OR RECOMMEND THERAPY OR TREATMENT; THE SOFTWARE IS AN INFORMATION RESOURCE AND IS NOT A SUBSTITUTE FOR THE SKILL, JUDGMENT AND KNOWLEDGE OF THE CITY'S USERS OF THE SOFTWARE IN THE PROVISION OF HEALTHCARE SERVICES. IN ADDITION TO THE LIMITATIONS OF LIABILITY PROVIDED HEREIN, HYLAND SHALL NOT HAVE ANY LIABILITY FOR ANY ASPECT OF CITY'S SERVICES PROVIDED IN CONJUNCTION WITH ITS USE OF THE SOFTWARE.

ACCEPTABLE USE POLICY ATTACHMENT

1. INTRODUCTION.

This Acceptable Use Policy (this "AUP") applies to all persons and entities (collectively referred to herein as "User") who use the services and software products provided by Hyland Software, Inc. or its affiliates ("Hyland") in connection with Hyland Cloud Service. This AUP is designed to protect the security, integrity, reliability and privacy of Hyland's network and the Hyland Cloud Services Hyland hosts for its hosting customers.

User's use of the Hyland Cloud Service constitutes User's acceptance of the terms and conditions of this AUP in effect at the time of such use. Hyland reserves the right to modify this policy at any time effective immediately upon Hyland's posting of the modification or revised AUP on Hyland's website: https://www.hyland.com/community.

2. USER OBLIGATIONS.

2.1 Misuse. User is responsible for any misuse of a Hyland Cloud Service. Therefore, User must take all reasonable precautions to protect access and use of any Hyland Cloud Service that it uses.

2.2 Restriction on Use. User shall not use a Hyland Cloud Service in any manner in violation of applicable law including, but not limited to, by:

(a) Infringing or misappropriating intellectual property rights, including copyrights, trademarks, service marks, software, patents and trade secrets;

(b) Engaging in the promotion, sale, production, fulfillment or delivery of illegal drugs, illegal gambling, obscene materials or other products and services prohibited by law. Similarly, soliciting illegal activities is prohibited even if such activities are not actually performed;

(c) Displaying, transmitting, storing or making available child pornography materials;

(d) Transmitting, distributing or storing any material that is unlawful, including encryption software in violation of U.S. export control laws, or that presents a material risk of civil liability to Hyland;

(e) Displaying, transmitting, storing or publishing information that constitutes libel, slander, defamation, harassment, obscenity, or otherwise violates the privacy or personal rights of any person;

(f) Displaying or transmitting obscene, threatening, abusive or harassing messages; or

(g) Promoting, offering or implementing fraudulent financial schemes including pyramids, illegitimate funds transfers and charges to credit cards.

2.3 Prohibited Acts. User shall not use a Hyland Cloud Service to engage in any of the following:

(a) Interfering with, gaining unauthorized access to or otherwise violating the security of Hyland's or another party's server, network, personal computer, network access or control devices, software or data, or other system, or to attempt to do any of the foregoing, including, but not limited to, use in the development, distribution or execution of Internet viruses, worms, denial of service attacks, network flooding or other malicious activities intended to disrupt computer services or destroy data;

(b) Interfering with Hyland's network or the use and enjoyment of Hyland Cloud Services received by other authorized Users;

(c) Promoting or distributing software, services or address lists that have the purpose of facilitating spam;

(d) Providing false or misleading information in message headers or other content, using non-existent domain names or deceptive addressing, or hiding or obscuring information identifying a message's point of origin or transmission path;

(e) Violating personal privacy rights, except as permitted by law;

(f) Sending and collecting responses to spam, unsolicited electronic messages or chain mail; and

(g) Engaging in any activities that Hyland believes, in its sole discretion, might be harmful to Hyland's operations, public image or reputation.

3. ENFORCEMENT. If a User violates this AUP, Hyland may, depending on the nature and severity of the violation, suspend the hosting of any Hyland Cloud Service that such User accesses for so long as necessary for steps to be taken that, in Hyland's reasonable judgment, will prevent the violation from continuing or reoccurring.

4. NOTICE. Unless prohibited by law, Hyland shall provide User with written notice via e-mail or otherwise of a violation of this AUP so that such violation may be corrected without impact on the hosting of Hyland Cloud Services; Hyland shall also provide User with a deadline for User to come into compliance with this AUP. Hyland reserves the right, however, to act immediately and without notice to suspend the Hyland Cloud Service in response to a court order or government notice that certain conduct of User must be stopped or when Hyland reasonably determines: (1) that it may be exposed to sanction, civil liability or prosecution; (2) that such violation may cause harm to or interfere with the integrity or normal operations or security of Hyland's network or networks with which Hyland is interconnected or interfere with another of Hyland's customer's use of Hyland Cloud Services, other services or software products; or (3) that such violation otherwise presents imminent risk of harm to Hyland or other of Hyland's customers or their respective employees. In other situations, Hyland will use reasonable efforts to provide User with at least seven (7) calendar days' notice before suspending the Hyland Cloud Service. User is responsible for all charges or fees due to Hyland up to the point of suspension by Hyland, pursuant to the agreement in place between User and Hyland or Reseller related to the Hyland Cloud Services.

5. DISCLAIMER. Hyland disclaims any responsibility for damages sustained by User as a result of Hyland's response to User's violation of this AUP. User is solely responsible for the content and messages transmitted or made available by User using a Hyland Cloud Service. By using a Hyland Cloud Service, User acknowledges that Hyland has no obligation to monitor any activities or content for violations of applicable law or this AUP, but it reserves the right to do so. Hyland disclaims any responsibility for inappropriate use of a Hyland Cloud Service by User and any liability for any other third party's violation of this AUP or applicable law.

6. RESPONSIBILITY. User agrees to be responsible for liabilities, obligations, losses and damages, plus costs and expenses, including reasonable attorney's fees, arising out of any claim, damage, loss, liability, suit or action brought against Hyland by a third party as a result of the conduct of User that violates this AUP.

7. WAIVER. No failure or delay in exercising or enforcing this policy shall constitute a waiver of the policy or of any other right or remedy. If any provision of this policy is deemed unenforceable due to law or change in law, such a provision shall be disregarded and the balance of the policy shall remain in effect.

8. QUESTIONS. If you are unsure of whether any contemplated use or action is permitted, please contact Hyland, at 440-788-5000.

SAAS 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 Hyland Cloud Service information security program. 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. Maintaining media handling procedures to ensure media containing Customer Data as part of the Hyland Cloud Service is encrypted and stored in a secure location subject to strict physical access controls.
   c. When a Hyland Cloud Service storage device has reached the end of its useful life, procedures include a decommissioning process that is designed to prevent Customer Data from being exposed to unauthorized individuals using the techniques recommended by NIST to destroy data as part of the decommissioning process.
   d. If a Hyland storage device is unable to be decommissioned using these procedures, the device will be virtually shredded, degaussed, purged/wiped, or physically destroyed in accordance with industry-standard practices.

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 the 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 strict access controls are in place for Customer Data access by Hyland. City administrators control its user access, user permissions, and Customer Data retention to the extent such controls are available to City 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 Platform, including network devices, network connectivity, workstations, servers, and software owned and operated by the City or other third parties. Hyland may provide support for these components at its reasonable discretion.

b. The processes executed within the Hyland Cloud Platform 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. This includes, but is not limited to, hardware installation, software installation, data replication, data security, and authentication processes.

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 Platform, 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 City. 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 Platform. 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 via SFTP, TLS/SSL, or other equivalent method.

b. If City purchases the applicable encryption service, applicable Customer Data shall be encrypted at rest.

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

IX. Physical and Environment Security.

a. The Hyland Cloud Platform uses data centers or 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 Platform.

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

X. Operations Security.

a. Maintaining documented Hyland cloud operating procedures.

b. Maintaining change management controls to ensure changes to Hyland Cloud Service production systems made by Hyland are properly authorized and reviewed prior to implementation. City is responsible for testing all configuration changes, authentication changes and upgrades implemented by City or implemented by Hyland at the request of City prior to production use of the Hyland Cloud Service. In cases where the City 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 City's designated City Security Administrators ("CSAs") or set forth in a Services Proposal. Hyland will make scheduled configuration changes that are expected to impact City access to their Hyland Cloud Service during a planned maintenance window. Hyland may make configuration changes that are not expected to impact City during normal business hours.

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

d. Utilizing virus and malware protection technologies, which are configured to meet industry best practices designed to protect the Customer Data and equipment located within the Hyland Cloud Platform from virus infections, malware, ransomware, or similar malicious payloads.

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

f. Maintaining a system and security logging process to capture system logs deemed critical by Hyland. These logs shall be maintained for at least six months and reviewed on a periodic basis.

g. Maintaining system hardening requirements and configuration standards for components deployed within the Hyland Cloud Platform. Ensuring servers, operating systems, and supporting software used in the Hyland Cloud Platform receive all Critical and High 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.

h. Conducting Hyland Cloud Platform vulnerability scans or analysis on at least a quarterly basis and remediate all critical and high vulnerabilities identified in accordance with its patch management procedures.

i. Conducting Hyland Cloud Platform penetration tests at least annually.

XI. Communications Security.

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

b. When supported, upon implementation and once annually thereafter, City may request Hyland limit access to City'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 Incident.

a. Employing incident response standards that are based upon applicable industry standards, such as ISO 27001:2013 and National Institute for Standards and Technology ("NIST"), to maintain the information security components of the Hyland Cloud Service environment.

b. 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.

c. If Hyland has determined City's Hyland Cloud Service has been negatively impacted by a security incident, Hyland will deliver 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 the Hyland Cloud Service.

d. The root cause analysis will include the duration of the event, resolution, technical summary, outstanding issues, and follow-up, including steps City needs to take in order to prevent further issues. Hyland Cloud Service 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 City needs additional details of an incident, a request to the Hyland GCS Support team must be submitted and handled on a case by case basis. The release of information process may require an on-site review to protect the confidentiality and security of the requested information.

e. Hyland will notify City 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.

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 City 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. Audit and Security Testing.

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 City upon written request.

c. City may conduct audits of Hyland's operations that participate in the ongoing delivery and support of the Hyland Cloud Service purchased by City on an annual basis; provided City provides Hyland written notice of its desire to conduct such audit and the following criteria are met: (a) Hyland and City mutually agree upon the timing, scope, and criteria of such audit, which may include the completion of questionnaires supplied by City and guided review of policies, practices, procedures, Hyland Cloud Service configurations, invoices, or application logs, and (b) City 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 City 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 City cannot be removed from Hyland's facilities as a result of physical limitations or policy restrictions, Hyland will allow City'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 City mutually agree to make necessary employees or contractors available for interviews in person or on the phone during such audit at City's cost and expense. City is prohibited from distributing or publishing the results of such audit to any third party without Hyland's prior written approval.

d. City may conduct penetration testing against the public URL used to access the Hyland Cloud Service on an annual basis; provided City provides Hyland with written notice of its desire to conduct such testing and the following criteria are met: (a) Hyland and City mutually agree upon the timing, scope, and criteria of such testing, which may include common social engineering, application, and network testing techniques used to identify or exploit common vulnerabilities including buffer overflows, cross site scripting, SQL injection, and man in the middle attacks, and (b) such testing is at City's cost and expense and City pays to Hyland fees (at Hyland's standard rates) for the Professional Services that are required or requested of Hyland in connection with such testing. Prior to any such testing, any third party engaged by City to assist with such testing, must be cleared by Hyland and enter into a Non-Disclosure Agreement directly with Hyland. City acknowledges and agrees that any such 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 City's access to or use of the Hyland Cloud Service. City is prohibited from distributing or publishing the results of such penetration testing to any third party without Hyland's prior written approval.

