49

STATE OF NEW HAMPSHIRE
DEPARTMENT OF INFORMATION TECHNOLOGY
27 Hazen Dr., Concord, NH 03301
Fax: 603-271-1516 TDD Access: 1-800-735-2964
www.nh.gov/doit

Denis Goulet
Commissioner

May 9, 2022

His Excellency, Governor Christopher T. Sununu
and the Honorable Executive Council
State House
Concord, NH 03301

REQUESTED ACTION

Authorize the Department of Information Technology (DoIT), on behalf of the Department of Labor (DOL), to enter into a contract amendment with Hyland Software Inc., (Vendor # 220511), Westlake, Ohio, increasing the price limitation by $160,000 from 1,220,182.32 to $1,380,182.32 for additional licensing services for the DOL's Electronic Document Management System (EDMS) with no change to the contract end date, effective upon Governor and Executive Council approval through June 30, 2024 . The original contract was approved by Governor and Executive Council on May 6, 2020 Item #71.

100% Other (Agency Class 27) funds: the Agency Class 027 used by the DOL to reimburse DoIT is 100% Other Funds.

Funding is available in the following account for SFY 2022 and 2023 with the authority to adjust encumbrances between fiscal years within the price limitation through the Budget Office, if needed and justified.

CAT#-DEPT#-AGENCY#- ACTIVITY#-ACCOUNTING UNIT #- DEPT NAME- AGENCY NAME -ACCOUNTING UNIT NAME CLASS- OBJECT - DESC	Activity Code	SFY 2022	SFY 2023	Total
01-03-03-030010-76260000 DoIT – IT for DOL 046-500465 IT Consult- Non-Benefit	03260017	$80,000.00	$80,000.00	$160,000.00

EXPLANATION

This contract amendment with Hyland Inc. will leverage the existing working relationship in the modernization of DOL's business processes and infrastructure. Specifically, this modification will allow for the provision of additional licensing services related to the enhancement or replacement of core components of the Department's relational database currently residing on the aging, on-premise IBM AS400 Power Server solution with Hyland's WorkView relational database solution and their OnBase Electronic Document Management System (EDMS).

The Department of Information Technology and the Department of Labor respectfully request approval of this contract modification.

Respectfully submitted,

Denis Goulet
DoIT Commissioner

Ken Merrifield
Department of Labor Commissioner

DG/ik
DoIT #2020-075A
RID: 69220

Denis Goulet
Commissioner

May 11, 2022

Ken Merrifield, Commissioner
Department of Labor
State of New Hampshire
95 Pleasant Street
Concord, NH 03301

Dear Commissioner Merrifield:

This letter represents formal notification that the Department of Information Technology (DoIT) has approved your agency's request to amend a contract with Hyland Software Inc., of Westlake, Ohio, as described below and referenced as DoIT No. 2020-075A.

This amendment will allow for the provision of additional licensing services related to the enhancement or replacement of core components of the Department's relational database currently residing on the aging on-premise IBM Power Server (aka AS400). solution with Hyland's relational database solution called WorkView and their Electronic Document Management System (EDMS) called OnBase.

The amendment will increase the Price Limitation by $160,000 from 1,220,182.32 to $1,380,182.32 and shall be effective upon Governor and Executive Council approval through June 30, 2024.

A copy of this letter will accompany DoIT's submission to Governor and Executive Council for approval.
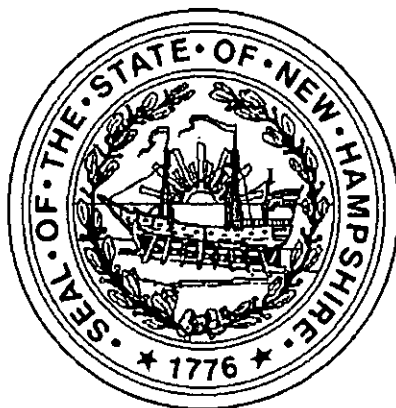
Sincerely,

Denis Goulet

DG/ik
DoIT #2020-075A

cc: Todd Allen, IT Manager, DoIT

STATE OF NEW HAMPSHIRE

Department of Information Technology - DOL

DOL Hyland Cloud Hosting Contract

DoIT – 2020-075

AMENDMENT Amend A (1)

INFORMATION TECHNOLOGY

INTRODUCTION

WHEREAS, pursuant to an Agreement approved by Governor and Council, as a result of Contract 2020-075, on May 6, 2020, Item #71 (herein after referred to as the "Agreement"), Hyland Software Inc. (herein after referred to as "Contractor") agreed to supply certain services upon the terms and conditions specified in the Agreement and in consideration of payment by the Department of Information Technology (hereinafter referred to as the "Department"), certain sums as specified therein;

WHEREAS, pursuant to the Agreement Section 17: Amendment and the provisions of the Agreement, the Agreement may be modified or amended only by a written instrument executed by the parties thereto and approved by the Governor and Executive Council;

WHEREAS, the Vendor and the Department have agreed to amend the Agreement to allow for the provision of additional licensing related to the enhancement or replacement of core components of the Department's relational database and electronic document management systems;

WHEREAS, the Vendor, in accordance with Section 4.2 of Exhibit D of the Agreement, will provide the Department with change orders for review/approval in advance of providing additional licensing.

WHEREAS, payment for the provision of additional licensing shall be made upon Departmental approval of milestones or defined deliverables as set forth in any related Change Order in accordance with Section 4.2 of Exhibit D of the Agreement;

WHEREAS, the Department and the Vendor wish to increase the Contract price by $160,000 to bring the total contract price to $1,380,182.32;

NOW THEREFORE, in consideration of the foregoing, and the covenants and conditions contained in the Agreement and set forth herein, the parties agree as follows:

The Agreement is hereby amended as follows:

1.   Amend Section 1.8 of the State of New Hampshire P-37 General Provisions by increasing the Price Limitation by $160,000 from 1.220.182.32 to $1,380,182.32.

State [ ] ntract
Date 𝓃𝐵𝐾
Cont [ ] itials

TABLE 1: CONTRACT HISTORY				
CONTRACT AND AMENDMENT NUMBER	AMENDMENT TYPE	G&C APPROVAL DATE	END DATE	CONTRACT AMOUNT
Contract 2020-075Choose an item.	Original Contract	May 6, 2020. Item #71	June 30, 2024	$1,220,182.32
			CONTRACT TOTAL	$1,220,182.32

State ⌐DS ntract
Date 𝑛ℬ𝒦
Cont⌐ itials

CONTRACTOR

Except as provided herein, all provisions of the Agreement shall remain in full force and effect. This modification shall take effect upon the approval date from the Governor and the Executive Council.

IN WITNESS WHEREOF, the parties have hereunto set their hands as of the day and year first above written.

Noreen B. Kilbane   Date: __May 9, 2022__ | 11:41:49 EDT

Noreen Kilbane, Chief Administrative Officer
Hyland Software, Inc.

ES   May 9, 2022 | 11:41:07 EDT

STATE OF NEW HAMPSHIRE

Date: __5/11/2022__

Denis Goulet, Commissioner
State of New Hampshire
Department of Information Technology

Date: __5/11/22__

Ken Merrifield, Commissioner
State of New Hampshire
Department of Labor

The preceding Amendment, having been reviewed by this office, is approved as to form, substance, and execution.

Approved by the Attorney General

/s/ Stacie M. Moeser   Date: __May 16, 2022__

State of New Hampshire, Department of Justice

State   ntract
Date   𝑛𝐵𝐾
Cont   itials

I hereby certify that the foregoing amendment was approved by the Governor and Executive Council of the State of New Hampshire at the Meeting on: _____ (date of meeting)

Office of the Secretary of State

_____   Date: _____

State of New Hampshire, Department of Administration

State of New Hampshire

Department of State

CERTIFICATE

I, David M. Scanlan, Secretary of State of the State of New Hampshire. do hereby certify that HYLAND SOFTWARE, INC. is a Ohio Profit Corporation registered to transact business in New Hampshire on June 26, 2009. I further certify that all fees and documents required by the Secretary of State's office have been received and is in good standing as far as this office is concerned.

Business ID: 615852

Certificate Number: 0005772122
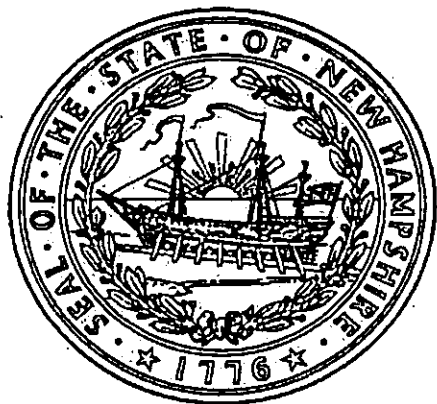
IN TESTIMONY WHEREOF,
I hereto set my hand and cause to be affixed
the Seal of the State of New Hampshire,
this 5th day of May A.D. 2022.

David M. Scanlan
Secretary of State

EU-36918-24531497

April 26, 2022

HYLAND SOFTWARE, INC.

SECRETARY'S CERTIFICATE

I, the undersigned, the duly elected and acting Secretary of Hyland Software, Inc. a corporation organized and existing under the laws of the State of Ohio (the "Corporation"), do hereby certify that Noreen Kilbane, Executive Vice President & Chief Administrative Officer, is a duly elected Officer of the Corporation and is authorized to enter into, execute, acknowledge and attest to any agreements, instruments or documents on behalf of the Corporation.

IN WITNESS WHEREOF, I have hereunto set my hand on behalf of the Corporation as of the date first written above.

HYLAND SOFTWARE, INC.

By:
_____

Date:
<u>April 26, 2022 | 17:39:12 EDT</u>

Name: Abby Moskovitz
_____

Title: Corporate Secretary
_____

<u>Hyland Legal</u>

Approved By:

Date: April 26, 2022 | 16:41:17 EDT

ACORD® CERTIFICATE OF LIABILITY INSURANCE

DATE (MM/DD/YYYY)
12/29/2021

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

IMPORTANT: If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must have ADDITIONAL INSURED provisions or be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

PRODUCER	CONTACT NAME: Mackenzie Hurd		
The James B. Oswald Company	PHONE (A/C, No, Ext): (216) 367-8787		FAX (A/C, No): (216) 241-4520
1100 Superior Avenue East	E-MAIL ADDRESS: mhurd@oswaldcompanies.com		
Suite 1500			
Cleveland OH 44114	INSURER(S) AFFORDING COVERAGE		NAIC #
	INSURER A : Federal Insurance Company		20281
INSURED	INSURER B : Great Northern Insurance Co.		20303
HSI Holdings I, Inc.	INSURER C : Pacific Indemnity Company		20346
Hyland Software, Inc.	INSURER D :		
28500 Clemens Road	INSURER E :		
Westlake OH 44145	INSURER F :		

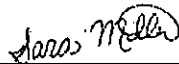COVERAGES   CERTIFICATE NUMBER: 21/22 GL/AUTO/   REVISION NUMBER:

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

INSR LTR	TYPE OF INSURANCE	ADDL INSD	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS	
A	[X] COMMERCIAL GENERAL LIABILITY	Y		3578-33-25	12/31/2021	12/31/2022	EACH OCCURRENCE	$ 1,000,000
	CLAIMS-MADE [X] OCCUR						DAMAGE TO RENTED PREMISES (Ea occurrence)	$ 1,000,000
							MED EXP (Any one person)	$ 10,000
							PERSONAL & ADV INJURY	$ 1,000,000
	GEN'L AGGREGATE LIMIT APPLIES PER:						GENERAL AGGREGATE	$ 2,000,000
	[X] POLICY [ ] PRO-JECT [ ] LOC						PRODUCTS - COMP/OP AGG	$ 2,000,000
	OTHER:							$
B	AUTOMOBILE LIABILITY [X] ANY AUTO			7352-28-83	12/31/2021	12/31/2022	COMBINED SINGLE LIMIT (Ea accident)	$ 1,000,000
							BODILY INJURY (Per person)	$
	OWNED AUTOS ONLY [ ] SCHEDULED AUTOS						BODILY INJURY (Per accident)	$
	HIRED AUTOS ONLY [ ] NON-OWNED AUTOS ONLY						PROPERTY DAMAGE (Per accident)	$
								$
A	[X] UMBRELLA LIAB [X] OCCUR			7988-20-68	12/31/2021	12/31/2022	EACH OCCURRENCE	$ 25,000,000
	EXCESS LIAB [ ] CLAIMS-MADE						AGGREGATE	$ 25,000,000
	DED [ ] RETENTION $							$
C	WORKERS COMPENSATION AND EMPLOYERS' LIABILITY Y/N ANY PROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? [ ] (Mandatory in NH) If yes, describe under DESCRIPTION OF OPERATIONS below		N/A	(22) 7171-39-93	12/31/2021	12/31/2022	[X] PER STATUTE [ ] OTH-ER	
							E.L. EACH ACCIDENT	$ 1,000,000
							E.L. DISEASE - EA EMPLOYEE	$ 1,000,000
							E.L. DISEASE - POLICY LIMIT	$ 1,000,000

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)

Contract Number: 2020-075

DOL Document Management Hosting Services is included as Additional Insured with respect to General Liability when required by written contract or agreement.

CERTIFICATE HOLDER	CANCELLATION
State of NH, Department of Information Technology ATTN:Chief Information Officer 27 Hazen Drive Concord NH 03301	SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS.
	AUTHORIZED REPRESENTATIVE *Jaros Miller*

STATE OF NEW HAMPSHIRE
DEPARTMENT OF INFORMATION TECHNOLOGY
27 Hazen Dr., Concord, NH 03301
Fax: 603-271-1516 TDD Access: 1-800-735-2964
www.nh.gov/doit

Denis Goulet
Commissioner

March 16, 2020

His Excellency, Governor Christopher T. Sununu
and the Honorable Executive Council
State House
Concord, NH 03301

REQUESTED ACTION

Authorize the Department of Information Technology (DoIT), on behalf of the Department of
Labor (DoL), to enter into a **Sole Source** contract with Hyland Software Inc., (Vendor #
220511), Westlake, Ohio, in the amount of $1,220,182.32 for cloud hosting services and
software related to replacing the existing electronic document management system, with the
option to renew for up to four (4) additional years, effective upon Governor and Executive
Council approval through June 30, 2024.

100% Other (Agency Class 27) funds: the Agency Class 027 used by the DoL to reimburse DoIT
is 100% Other Funds derived from the Workers' Compensation Insurance Assessments and the
Inspection Fees-Certificates-Licenses fund.

Funds are available in the following account(s) for SFY 2020 and 2021 and anticipated to be
available in SFY 2022 through SFY 2024, upon the availability and continued appropriation
of funds in the future operating budget, with the authority to adjust encumbrances between
fiscal years within the price limitation through the Budget Office, if needed and justified.

Funding is available in account: IT for Labor

Category# - Dept# - Agency # - Bur/Div Fund # - Accounting Unit# - Expenses Class# - Expense Account# - Expense Class Title	Activity Code	SFY 2020	SFY 2021	SFY 2022	SFY 2023	SFY 2024	Total
01-03-03-030010-76260000 - 046-500465 IT Consult-Non-Benefit	03260017	$549,430.32	$167,688.00	$167,688.00	$167,688.00	$167,688.00	$1,220,182.32

"Innovative Technologies Today for New Hampshire's Tomorrow"

EXPLANATION

This is a sole source request to purchase cloud hosting services and software related to Labor's Electronic Document Management System (EDMS) system upgrade. This contract works in conjunction with the ImageSoft, Inc. contract DoIT # 2018-133 which provides the integration services component of the project. These two contracts derived from a single proposal to Labor's Request for Proposal (RFP) issued in March of 2019. It was determined during contract development the State would be required to purchase the Hyland OnBase software and cloud hosting services directly from Hyland to receive the 23% government pricing discount for a savings of $365,000 through the initial term. This requirement for purchasing directly from Hyland created the unforeseen necessity for separate contracts with this one needing to be sole source.
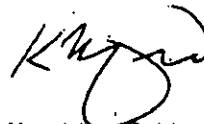
The OnBase software developed and owned by Hyland is top rated by Gartner in the Electronic Content Management sector. The Hyland cloud infrastructure provides superb security with multiple service levels of disaster recovery and continuity of operations planning. This electronic content management system using OnBase software will be flexible and configurable requiring minimal customization to accommodate the NHDOL's current and future business processes. This project will be a collaborative effort between the State, the integrator and this cloud hosting Contractor.

The Department of Information Technology and the Department of Labor request approval of this contract.

Respectfully submitted,

Denis Goulet
DoIT Commissioner

Ken Merrifield
Department of Labor Commissioner

DG/ik
DoIT #2020-075
RJD: 49406

Denis Goulet
Commissioner

March 17, 2020

Ken Merrifield, Commissioner
Department of Labor
State of New Hampshire
95 Pleasant Street
Concord, NH 03301

Dear Commissioner Merrifield:

This letter represents formal notification that the Department of Information Technology (DoIT) has approved your agency's request to enter into a contract with Hyland Software Inc., of Westlake, Ohio, as described below and referenced as DoIT No. 2020-075.

This contract will provide cloud hosting services and OnBase software for the DoL Electronic Document Management System (EDMS) system upgrade. This contract works in conjunction with the DoIT 2018-133 ImageSoft, Inc. contract. The two contracts together will provide a new, modern EDMS with up to date security for data protection. The new system will be flexible and configurable requiring minimal customization to accommodate the NHDOL's current and future business process workflows, reporting requirements, and interfaces.

The contract amount is $1,220,182.32 and shall be effective upon Governor and Executive Council approval through June 30, 2024, with an option to renew for up to four additional years.

A copy of this letter will accompany DoIT's submission to Governor and Executive Council for approval.

Sincerely,

Denis Goulet

DG/ik
DoIT #2020-075

cc: Joseph Nadeau, IT Manager, DoIT

02/19/2019 **FORM NUMBER P-37 (version 12/11/2019)**

AGREEMENT

The State of New Hampshire and the Contractor hereby mutually agree as follows:

GENERAL PROVISIONS

1. IDENTIFICATION:

1.1 State Agency Name NH Department of Information Technology in support of NH Department of Labor		1.2 State Agency Address 27 Hazen Drive Concord NH 03301	
1.3 Contractor Name Hyland Software, Inc. $\pi B K$ April 17, 2020		1.4 Contractor Address 28500 Clemens Road Westlake, Ohio 44145	
1.5 Contractor Phone Number (440) 788-5000	1.6 Account Number 01-03-03-030010-6260000 046-500465 $\overset{\Lambda}{7}$ $\mathcal{D}.G.$ 4|17|20	1.7 Completion Date 06/30/2024	1.8 Price Limitation f $1,220,182.32
1.9 Contracting Officer for State Agency Denis Goulet, Commissioner		1.10 State Agency Telephone Number 603-223-5703	
1.11 Contractor Signature *Noreen B Kilbane* Date: 03/13/2020		1.12 Name and Title of Contractor Signatory Noreen B. Kilbane – Chief Administrative Officer	
1.13 State Agency Signature Date: 3|17|2020		1.14 Name and Title of State Agency Signatory Denis Goulet, Commissioner	
1.15 Approval by the N.H. Department of Administration, Division of Personnel *(if applicable)* By: Director, On:			
1.16 Approval by the Attorney General (Form, Substance and Execution) *(if applicable)* By: On: 3/23/2020			
1.17 Approval by the Governor and Executive Council *(if applicable)* G&C Item number: G&C Meeting Date:			

HYLAND
SOFTWARE
[initials] 3-13-20
Initial Date
LEGAL

Page 1 of 32

Contractor Initials *NBK*
Date 03/13/2020

2. SERVICES TO BE PERFORMED. The State of New Hampshire, acting through the agency identified in block 1.1 ("State"), engages contractor identified in block 1.3 ("Contractor") to perform, and the Contractor shall perform, the work or sale of goods, or both, identified and more particularly described in the attached EXHIBIT B which is incorporated herein by reference ("Services").

3. EFFECTIVE DATE/COMPLETION OF SERVICES.
3.1 Notwithstanding any provision of this Agreement to the contrary, and subject to the approval of the Governor and Executive Council of the State of New Hampshire, if applicable, this Agreement, and all obligations of the parties hereunder, shall become effective on the date the Governor and Executive Council approve this Agreement as indicated in block 1.17, unless no such approval is required, in which case the Agreement shall become effective on the date the Agreement is signed by the State Agency as shown in block 1.13 ("Effective Date").
3.2 If the Contractor commences the Services prior to the Effective Date, all Services performed by the Contractor prior to the Effective Date shall be performed at the sole risk of the Contractor, and in the event that this Agreement does not become effective, the State shall have no liability to the Contractor, including without limitation, any obligation to pay the Contractor for any costs incurred or Services performed. Contractor must complete all Services by the Completion Date specified in block 1.7.

4. CONDITIONAL NATURE OF AGREEMENT.
Notwithstanding any provision of this Agreement to the contrary, all obligations of the State hereunder, including, without limitation, the continuance of payments hereunder, are contingent upon the availability and continued appropriation of funds affected by any state or federal legislative or executive action that reduces, eliminates or otherwise modifies the appropriation or availability of funding for this Agreement and the Scope for Services provided in EXHIBIT B, in whole or in part. In no event shall the State be liable for any payments hereunder in excess of such available appropriated funds. In the event of a reduction or termination of appropriated funds, the State shall have the right to withhold payment until such funds become available, if ever, and shall have the right to reduce or terminate the Services under this Agreement immediately upon giving the Contractor notice of such reduction or termination. The State shall not be required to transfer funds from any other account or source to the Account identified in block 1.6 in the event funds in that Account are reduced or unavailable.

5. CONTRACT PRICE/PRICE LIMITATION/ PAYMENT.
5.1 The contract price, method of payment, and terms of payment are identified and more particularly described in EXHIBIT C which is incorporated herein by reference.
5.2 The payment by the State of the contract price shall be the only and the complete reimbursement to the Contractor for all expenses, of whatever nature incurred by the Contractor in the performance hereof, and shall be the only and the complete

compensation to the Contractor for the Services. The State shall have no liability to the Contractor other than the contract price.
5.3 The State reserves the right to offset from any amounts otherwise payable to the Contractor under this Agreement those liquidated amounts required or permitted by N.H. RSA 80:7 through RSA 80:7-c or any other provision of law.
5.4 Notwithstanding any provision in this Agreement to the contrary, and notwithstanding unexpected circumstances, in no event shall the total of all payments authorized, or actually made hereunder, exceed the Price Limitation set forth in block 1.8.

6. COMPLIANCE BY CONTRACTOR WITH LAWS AND REGULATIONS/ EQUAL EMPLOYMENT OPPORTUNITY.
6.1 In connection with the performance of the Services, the Contractor shall comply with all applicable statutes, laws, regulations, and orders of federal, state, county or municipal authorities which impose any obligation or duty upon the Contractor, including, but not limited to, civil rights and equal employment opportunity laws. In addition, if this Agreement is funded in any part by monies of the United States, the Contractor shall comply with all federal executive orders, rules, regulations and statutes, and with any rules, regulations and guidelines as the State or the United States issue to implement these regulations. The Contractor shall also comply with all applicable intellectual property laws.
6.2 During the term of this Agreement, the Contractor shall not discriminate against employees or applicants for employment because of race, color, religion, creed, age, sex, handicap, sexual orientation, or national origin and will take affirmative action to prevent such discrimination.
6.3. The Contractor agrees to permit the State or United States access to any of the Contractor's books, records and accounts for the purpose of ascertaining compliance with all rules, regulations and orders, and the covenants, terms and conditions of this Agreement.

7. PERSONNEL.
7.1 The Contractor shall at its own expense provide all personnel necessary to perform the Services. The Contractor warrants that all personnel engaged in the Services shall be qualified to perform the Services, and shall be properly licensed and otherwise authorized to do so under all applicable laws.
7.2 Unless otherwise authorized in writing, during the term of this Agreement, and for a period of six (6) months after the Completion Date in block 1.7, the Contractor shall not hire, and shall not permit any subcontractor or other person, firm or corporation with whom it is engaged in a combined effort to perform the Services to hire, any person who is a State employee or official, who is materially involved in the procurement, administration or performance of this Agreement. This provision shall survive termination of this Agreement.
7.3 The Contracting Officer specified in block 1.9, or his or her successor, shall be the State's representative. In the event of any dispute concerning the interpretation of this Agreement, the Contracting Officer's decision shall be final for the State.

Contractor Initials _7ЦSP_
Date _03/13/2020_

8. EVENT OF DEFAULT/REMEDIES.

8.1 Any one or more of the following acts or omissions of the Contractor shall constitute an event of default hereunder ("Event of Default"):

8.1.1 failure to perform the Services satisfactorily or on schedule;

8.1.2 failure to submit any report required hereunder; and/or

8.1.3 failure to perform any other covenant, term or condition of this Agreement.

8.2 Upon the occurrence of any Event of Default, the State may take any one, or more, or all, of the following actions:

8.2.1 give the Contractor a written notice specifying the Event of Default and requiring it to be remedied within, in the absence of a greater or lesser specification of time, thirty (30) days from the date of the notice; and if the Event of Default is not timely cured, terminate this Agreement, effective two (2) days after giving the Contractor notice of termination;

8.2.2 give the Contractor a written notice specifying the Event of Default and suspending all payments to be made under this Agreement and ordering that the portion of the contract price which would otherwise accrue to the Contractor during the period from the date of such notice until such time as the State determines that the Contractor has cured the Event of Default shall never be paid to the Contractor;

8.2.3 give the Contractor a written notice specifying the Event of Default and set off against any other obligations the State may owe to the Contractor any damages the State suffers by reason of any Event of Default; and/or

8.2.4 give the Contractor a written notice specifying the Event of Default, treat the Agreement as breached, terminate the Agreement and pursue any of its remedies at law or in equity, or both.

8.3. No failure by the State to enforce any provisions hereof after any Event of Default shall be deemed a waiver of its rights with regard to that Event of Default, or any subsequent Event of Default. No express failure to enforce any Event of Default shall be deemed a waiver of the right of the State to enforce each and all of the provisions hereof upon any further or other Event of Default on the part of the Contractor.

9. TERMINATION.

9.1 Notwithstanding paragraph 8, the State may, at its sole discretion, terminate the Agreement for any reason, in whole or in part, by thirty (30) days written notice to the Contractor that the State is exercising its option to terminate the Agreement.

9.2 In the event of an early termination of this Agreement for any reason other than the completion of the Services, the Contractor shall, at the State's discretion, deliver to the Contracting Officer, not later than fifteen (15) days after the date of termination, a report ("Termination Report") describing in detail all Services performed, and the contract price earned, to and including the date of termination. The form, subject matter, content, and number of copies of the Termination Report shall be identical to those of any Final Report described in the attached EXHIBIT B. In addition, at the State's discretion, the Contractor

shall, within 15 days of notice of early termination, develop and submit to the State a Transition Plan for services under the Agreement.

10. DATA/ACCESS/CONFIDENTIALITY/ PRESERVATION.

10.1 As used in this Agreement, the word "data" shall mean all information and things developed or obtained during the performance of, or acquired or developed by reason of, this Agreement, including, but not limited to, all studies, reports, files, formulae, surveys, maps, charts, sound recordings, video recordings, pictorial reproductions, drawings, analyses, graphic representations, computer programs, computer printouts, notes, letters, memoranda, papers, and documents, all whether finished or unfinished.

10.2 All data and any property which has been received from the State or purchased with funds provided for that purpose under this Agreement, shall be the property of the State, and shall be returned to the State upon demand or upon termination of this Agreement for any reason.

10.3 Confidentiality of data shall be governed by N.H. RSA chapter 91-A or other existing law. Disclosure of data requires prior written approval of the State.

11. CONTRACTOR'S RELATION TO THE STATE. In the
performance of this Agreement the Contractor is in all respects an independent contractor, and is neither an agent nor an employee of the State. Neither the Contractor nor any of its officers, employees, agents or members shall have authority to bind the State or receive any benefits, workers' compensation or other emoluments provided by the State to its employees.

12. ASSIGNMENT/DELEGATION/SUBCONTRACTS.

12.1 The Contractor shall not assign, or otherwise transfer any interest in this Agreement without the prior written notice, which shall be provided to the State at least fifteen (15) days prior to the assignment, and a written consent of the State. For purposes of this paragraph, a Change of Control shall constitute assignment. "Change of Control" means (a) merger, consolidation, or a transaction or series of related transactions in which a third party, together with its affiliates, becomes the direct or indirect owner of fifty percent (50%) or more of the voting shares or similar equity interests, or combined voting power of the Contractor, or (b) the sale of all or substantially all of the assets of the Contractor.

12.2 None of the Services shall be subcontracted by the Contractor without prior written notice and consent of the State. The State is entitled to copies of all subcontracts and assignment agreements and shall not be bound by any provisions contained in a subcontract or an assignment agreement to which it is not a party.

13. INDEMNIFICATION. Unless otherwise exempted by law,
the Contractor shall indemnify and hold harmless the State, its officers and employees, from and against any and all claims, liabilities and costs for any personal injury or property damages, patent or copyright infringement, or other claims asserted against

Contractor Initials _____

Date _____

the State, its officers or employees, which arise out of (or which may be claimed to arise out of) the acts or omission of the Contractor, or subcontractors, including but not limited to the negligence, reckless or intentional conduct. The State shall not be liable for any costs incurred by the Contractor arising under this paragraph 13. Notwithstanding the foregoing, nothing herein contained shall be deemed to constitute a waiver of the sovereign immunity of the State, which immunity is hereby reserved to the State. This covenant in paragraph 13 shall survive the termination of this Agreement.

14. INSURANCE.
14.1 The Contractor shall, at its sole expense, obtain and continuously maintain in force, and shall require any subcontractor or assignee to obtain and maintain in force, the following insurance:
14.1.1 commercial general liability insurance against all claims of bodily injury, death or property damage, in amounts of not less than $1,000,000 per occurrence and $2,000,000 aggregate or excess; and
14.1.2 special cause of loss coverage form covering all property subject to subparagraph 10.2 herein, in an amount not less than 80% of the whole replacement value of the property.
14.2 The policies described in subparagraph 14.1 herein shall be on policy forms and endorsements approved for use in the State of New Hampshire by the N.H. Department of Insurance, and issued by insurers licensed in the State of New Hampshire.
14.3 The Contractor shall furnish to the Contracting Officer identified in block 1.9, or his or her successor, a certificate(s) of insurance for all insurance required under this Agreement. Contractor shall also furnish to the Contracting Officer identified in block 1.9, or his or her successor, certificate(s) of insurance for all renewal(s) of insurance required under this Agreement no later than ten (10) days prior to the expiration date of each insurance policy. The certificate(s) of insurance and any renewals thereof shall be attached and are incorporated herein by reference.

15. WORKERS' COMPENSATION.
15.1 By signing this agreement, the Contractor agrees, certifies and warrants that the Contractor is in compliance with or exempt from, the requirements of N.H. RSA chapter 281-A *("Workers' Compensation")*.
15.2 To the extent the Contractor is subject to the requirements of N.H. RSA chapter 281-A, Contractor shall maintain, and require any subcontractor or assignee to secure and maintain, payment of Workers' Compensation in connection with activities which the person proposes to undertake pursuant to this Agreement. The Contractor shall furnish the Contracting Officer identified in block 1.9, or his or her successor, proof of Workers' Compensation in the manner described in N.H. RSA chapter 281-A and any applicable renewal(s) thereof, which shall be attached and are incorporated herein by reference. The State shall not be responsible for payment of any Workers' Compensation premiums or for any other claim or benefit for Contractor, or any subcontractor or employee of Contractor, which might arise under applicable State of New Hampshire

Workers' Compensation laws in connection with the performance of the Services under this Agreement.

16. NOTICE. Any notice by a party hereto to the other party shall be deemed to have been duly delivered or given at the time of mailing by certified mail, postage prepaid, in a United States Post Office addressed to the parties at the addresses given in blocks 1.2 and 1.4, herein.

17. AMENDMENT. This Agreement may be amended, waived or discharged only by an instrument in writing signed by the parties hereto and only after approval of such amendment, waiver or discharge by the Governor and Executive Council of the State of New Hampshire unless no such approval is required under the circumstances pursuant to State law, rule or policy.

18. CHOICE OF LAW AND FORUM. This Agreement shall be governed, interpreted and construed in accordance with the laws of the State of New Hampshire, and is binding upon and inures to the benefit of the parties and their respective successors and assigns. The wording used in this Agreement is the wording chosen by the parties to express their mutual intent, and no rule of construction shall be applied against or in favor of any party. Any actions arising out of this Agreement shall be brought and maintained in New Hampshire Superior Court which shall have exclusive jurisdiction thereof.

19. CONFLICTING TERMS. In the event of a conflict between the terms of this P-37 form (as modified in EXHIBIT A) and/or attachments and amendment thereof, the terms of the P-37 (as modified in EXHIBIT A) shall control.

20. THIRD PARTIES. The parties hereto do not intend to benefit any third parties and this Agreement shall not be construed to confer any such benefit.

21. HEADINGS. The headings throughout the Agreement are for reference purposes only, and the words contained therein shall in no way be held to explain, modify, amplify or aid in the interpretation, construction or meaning of the provisions of this Agreement.

22. SPECIAL PROVISIONS. Additional or modifying provisions set forth in the attached EXHIBIT A are incorporated herein by reference.

23. SEVERABILITY. In the event any of the provisions of this Agreement are held by a court of competent jurisdiction to be contrary to any state or federal law, the remaining provisions of this Agreement will remain in full force and effect.

24. ENTIRE AGREEMENT. This Agreement, which may be executed in a number of counterparts, each of which shall be deemed an original, constitutes the entire agreement and understanding between the parties, and supersedes all prior agreements and understandings with respect to the subject matter hereof.

Contractor Initials *NBC*

Date *03/13/2020*

EXHIBIT A
SPECIAL TERMS

The terms outlined in the General Provisions Form P37 are modified as set forth below:

1. The following language is added to Provision 3, Effective Date/Completion of Services, as sub-provision 3.3:

   3.3 The Contract and all obligations of the parties hereunder shall become effective on the Effective Date and extend for four (4) years ("Initial Term"). The Initial Term may be extended up to four (4) years ("Extended Term") at the sole option of the State, subject to the parties' prior·written agreement and governmental approvals.

2. The following language is added to 7.1.2 in Provision 7, Personnel

   During the term of this Agreement for a period of six (6) months after termination or expiration of this Agreement, the State shall not hire, and shall not solicit, hire or employ as an employee or independent contractor any Contractor employee.

3. Provision 8 is deleted in its entirety.

4. Provision 13, Indemnification, is deleted in its entirety and replaced with the following:

   Unless otherwise exempted by law, and except as provided in Exhibit F, Section 8, the Contractor shall indemnify and hold harmless the State, its officers and employees, from and against any and all claims, liabilities and costs for any third party claim for damages resulting from personal injury or death or damages to tangible personal property or real property, , which arise out of (or which may be claimed to arise out of) the acts or omission of the Contractor, or subcontractors, including but not limited to the negligence, reckless or intentional conduct. The State shall not be liable for any costs incurred by the Contractor arising under this paragraph 13. Notwithstanding the foregoing, nothing herein contained shall be deemed to constitute a waiver of the sovereign immunity of the State, which immunity is hereby reserved to the State. This covenant in paragraph 13 shall survive the termination of this Agreement.

5. Provision 14.1.1, Insurance, is partially modified as following:

   14.1.1. Commercial general liability insurance against all claims of bodily injury, death or property damage, in amounts of $1,000,000 per occurrence and $2,000,000 aggregate or excess; and

6. Provision 14.1.3, Insurance, is modified as following:

   14.1.3 The Contractor shall furnish to the Contracting Officer identified in block 1.9, or his or her successor, a certificate(s) of insurance for all insurance required under this Agreement. Contractor shall also furnish to the Contracting Officer identified in block 1.9, or his or her successor, certificate(s) of insurance for all renewal(s) of insurance required under this Agreement no later than five (5) days after the expiration date of each insurance policy. The certificate(s) of insurance and any renewals thereof shall be attached and are incorporated herein by reference.

7. The following language is added to Provision 19, Conflicting Terms:

Contractor Initials _NBC_
Date _03/13/2020_

In the event of conflict or ambiguity among any of the text of the Contract Documents, the following Order of Precedence shall govern:

I. Form P-37, General Provisions as modified in Exhibit A;
II. Exhibit C, Price and Payment Schedule;
III. Exhibit D, Software License Schedule – Perpetual ;
IV. Exhibit E, Maintenance Schedule;
V. Exhibit F, Hosting Schedule;
VI. Exhibit B, Scope of Work;
VII. Attachments
    a. State of NH Hosting and Software Technical Requirements Spreadsheet with Hyland responses dated February 14, 2020
    b. Hyland Service Class Manual Version 2017.2 dated December 1, 2017
    c. Hyland Cloud Customer Process Manual Version 2017.1.

8. Provision 20, Third Parties, is modified as following:

20. Except as provided in Section 8.15 of General Terms Schedule below, the parties hereto do not intend to benefit any third parties and this Agreement shall not be construed to confer any such benefit.

The following General Terms Schedule provisions are added to P-37:

1. TERM; TERMINATION; SURVIVAL OF PROVISIONS AFTER EXPIRATION OR TERMINATION.

1.1 *Term.* This Agreement shall have a term commencing on the Effective Date, and will continue until all Schedules have been terminated in accordance with the terms in this Agreement.

1.2 *Termination.*

1.2.1 *Intentionally omitted.*

1.2.2 *By Either Party.* Either party may terminate this Agreement in its entirety or any Schedule, effective immediately upon written notice to the other party, if the other party has committed a breach of a material provision of this Agreement or any Schedule and has failed to cure the breach within thirty (30) days after the receipt of written notice of the breach given by the non-breaching party.

1.3 *Certain Effects or Consequences of Termination: Survival of Certain Provisions.*

1.3.1 *Generally.* Any termination of this Agreement or any Schedule will not discharge or otherwise affect any pre-termination obligations of either party existing under this Agreement at the time of termination, including Customer's obligation to pay to Hyland all fees and charges accrued or due for any period or event occurring on or prior to the effective date of termination or expiration of this Agreement or the applicable Schedule; and all liabilities which have accrued prior to the date of termination shall survive.

1.3.2 *Survival of Certain Obligations.* All provisions of this Agreement or of an applicable Schedule, which by their nature extend beyond the expiration or termination of this Agreement will survive and remain in effect until all obligations are satisfied, including, but not limited to all sections of these General Terms (except Section 8.12).

1.3.3. *Termination of a Schedule.* If a Software License Schedule - Perpetual or a Software License and Maintenance Schedule – Subscription or a SaaS Schedule is terminated in accordance with its terms, then this entire Agreement will terminate with respect to the Software licensed under such Schedule. Otherwise, termination of a Schedule will not affect the remaining Schedules.

2. PAYMENT TERMS.

Contractor Initials *TLBL*
Date *03/13/2020*

2.1   *Intentionally omitted.*

2.2   *Intentionally Omitted.*

2.3   *Intentionally Omitted .*

2.5   <u>Resolution of Invoice Disputes</u>. If, prior to the due date for payment under any invoice, Customer notifies Hyland in writing that it disputes all or any portion of an amount invoiced, both parties will use reasonable efforts to resolve the dispute within thirty (30) calendar days of Hyland's receipt of the notice. If any amount remains disputed in good faith after such 30-day period, either party may escalate the disputed items to the parties' respective executive management to attempt to resolve the dispute. The parties agree that at least one of each of their respective executives will meet (which may be by telephone or other similarly effective means of remote communication) within ten (10) calendar days of any such escalation to attempt to resolve the dispute. If the parties' executive managers are unable to resolve the dispute within ten (10) calendar days of such meeting, either party thereafter may file litigation in a court of competent jurisdiction to seek resolution of the dispute.

2.6   <u>Certain Remedies For Non-Payment or For Late Payment</u>. At the election of Hyland, exercisable by written notice to Customer, any past due amounts (except those amounts properly disputed in accordance with Section 2.5 of these General Terms), which default continues unremedied for at least thirty (30) calendar days after the due date of such payment, Hyland shall provide written notice to Customer regarding such past due amounts and if after thirty (days) following such notice, such past-due amounts remain unremitted, Hyland shall have the right to suspend or cease the provision of any services under this Agreement or any Services Proposal, including the delivery of any Upgrades and Enhancements to Customer, unless and until such default shall have been cured.

2.7   <u>U.S. Dollars; Delivery of Hasps and CDs</u>. All fees, costs and expenses under this Agreement shall be determined and invoiced in, and all payments required to be made in connection with this Agreement shall be made in, U.S. dollars. Delivery of CDs, if any, shall be F.O.B. Hyland's offices in Westlake, Ohio, USA.

2.8   <u>Training</u>. Hyland offers training courses to Customer and its employees as described on Hyland's training web portal (currently. https://training.onbase.com). Training fees for such courses shall be determined at Hyland's retail prices in effect at the time Customer registers for training. Hyland shall invoice Customer for applicable training fees upon Customer's registration for each training course and such invoice shall be due and payable in accordance with Section 2.3 above. In the event that Customer prepays for training, then such prepaid training shall expire twelve (12) months from the date Hyland accepts Customer's purchase order for such training.

3.   CONFIDENTIAL INFORMATION.

3.1   "Confidential Information" shall be 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 this 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.

3.2   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 (except in performance of this Agreement) or disclose to any third party any such Confidential Information, except as may be required by law or court order. Each party shall be liable and responsible for any breach of this Section 3 committed by any of such party's employees, agents, consultants, contractors or representatives.

3.3   Notwithstanding the foregoing, Hyland acknowledges that Customer is subject to State and federal laws governing disclosure of information including, but not limited to, RSA Chapter 91-A. Customer will maintain confidentiality of Confidential Information insofar as it is consistent with applicable State and federal laws or regulations, including but not limited to, RSA Chapter 91-A. In the event the State receives a request for Hyland's information, the State shall notify Hyland and specify the date the State will be releasing the requested information. At the request of the State, Hyland shall cooperate and assist the State with the collection and review of the Contractor's information, at no additional expense to the State. Any effort to prohibit or enjoin the release of the information shall be the Contractor's sole responsibility and at Hyland sole expense. If Hyland fails to obtain a court order enjoining the disclosure, Hyland shall release the information on the date specified in the State's notice to Hyland, without any liability to Hyland.

4.   OWNERSHIP AND PROHIBITED CONDUCT.

4.1   <u>Ownership</u>. Hyland and its suppliers own the Software, Work Products, Documentation and Innovations, 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 Work Products are protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. No ownership rights in the Software, Innovations or Work Products are transferred to Customer. Customer agrees to take all reasonable steps to protect all Work Products and Innovations, and any related Documentation, delivered by Hyland to Customer under this Agreement from unauthorized copying or use. Customer agrees that nothing in this Agreement or associated documents gives it any right, title or

Contractor Initials *NBL*
Date *03/13/2020*

interest in the Software or Work Products, except for the limited express rights granted in a Software License Schedule – Perpetual or a Software License and Maintenance Schedule – Subscription or a SaaS Schedule. Customer 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's policies respecting Upgrades and Enhancements (including but not limited to its release process). THIS AGREEMENT IS NOT A WORK-FOR-HIRE AGREEMENT.

4.2 . Prohibited Conduct. Customer agrees not to: (a) remove copyright, trademark or other proprietary rights notices that appear on or during the use of the Software, Work Products, Documentation or Third Party Software; (b) sell, transfer, rent, lease or sub-license the Software, Work Products, Documentation, Third Party Software, or Third Party Software documentation to any third party; (c) except as expressly permitted with respect to Work Products, alter or modify the Software, Work Products, Documentation or Third Party Software; or (d) reverse engineer, disassemble, decompile or attempt to derive source code from the Software, Work Products, Documentation or Third Party Software, or prepare derivative works therefrom.

5. DISCLAIMER OF WARRANTIES.

5.1 EXCEPT FOR THE WARRANTIES PROVIDED BY HYLAND AS EXPRESSLY SET FORTH IN THE SCHEDULES MADE PART OF THIS AGREEMENT, HYLAND AND ITS SUPPLIERS MAKE NO WARRANTIES OR REPRESENTATIONS REGARDING ANY SOFTWARE, HOSTED SOLUTION (INCLUDING ANY SOFTWARE OR HARDWARE), WORK PRODUCTS, INNOVATIONS, INFORMATION, MAINTENANCE AND SUPPORT, HOSTING SERVICES, PROFESSIONAL SERVICES OR ANY OTHER SERVICES PROVIDED UNDER THIS AGREEMENT OR ANY SERVICES PROPOSAL. HYLAND AND 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 MAINTENANCE AND SUPPORT, HOSTING SERVICES, PROFESSIONAL SERVICES, SOFTWARE OR WORK PRODUCTS PROVIDED WILL SATISFY CUSTOMER'S REQUIREMENTS OR ARE WITHOUT DEFECT OR ERROR, OR THAT THE OPERATION OF ANY SOFTWARE OR ANY WORK PRODUCTS PROVIDED UNDER THIS AGREEMENT WILL BE UNINTERRUPTED. EXCEPT AS EXPRESSLY STATED IN A HOSTING SCHEDULE, HYLAND DOES NOT ASSUME ANY LIABILITY WHATSOEVER WITH RESPECT TO ANY THIRD PARTY HARDWARE, FIRMWARE, SOFTWARE OR SERVICES.

5.2 CUSTOMER SPECIFICALLY ASSUMES RESPONSIBILITY FOR THE SELECTION OF THE SOFTWARE, WORK PRODUCTS, MAINTENANCE AND SUPPORT, HOSTING SERVICES AND PROFESSIONAL SERVICES TO ACHIEVE ITS BUSINESS OBJECTIVES.

5.3 HYLAND MAKES NO WARRANTIES WITH RESPECT TO ANY SOFTWARE OR WORK PRODUCTS USED IN ANY NON-PRODUCTION SYSTEM AND PROVIDES ANY SUCH SOFTWARE AND WORK PRODUCTS "AS IS."

5.4 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 this Agreement is authorized unless it is set forth in writing, references this Agreement, and is signed on behalf of Hyland by a corporate officer.

6. LIMITATIONS OF LIABILITY.

6.1 EXCEPT AS PROVIDED IN SECTION 6.3 BELOW, AND EXCEPT TO THE EXTENT PROHIBITED BY APPLICABLE LAW, IN NO EVENT SHALL EITHER PARTY (INCLUDING IN THE CASE OF HYLAND, ITS SUPPLIERS) BE LIABLE FOR ANY INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL OR PUNITIVE DAMAGES, OR ANY TYPE OF CLAIM FOR LOST PROFITS, LOST SAVINGS, BUSINESS INTERRUPTION DAMAGES OR EXPENSES, THE COSTS OF SUBSTITUTE SOFTWARE WORK PRODUCTS OR SERVICES, OR LOSSES RESULTING FROM ERASURE, DAMAGE, DESTRUCTION OR OTHER LOSS OF FILES, DATA OR PROGRAMS OR THE COST OF RECOVERING SUCH INFORMATION, EVEN IF SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, LOSSES, EXPENSES OR COSTS.

6.2 EXCEPT AS PROVIDED IN SECTION 6.3 BELOW, AND EXCEPT TO THE EXTENT PROHIBITED BY APPLICABLE LAW, HYLAND AND ITS SUPPLIERS' MAXIMUM LIABILITY ARISING UNDER THIS AGREEMENT SHALL NOT EXCEED: (A) WITH RESPECT TO ALL CLAIMS ARISING OUT OF A CUSTOMER DATA INCIDENT (AS DEFINED WITH RESPECT TO A HOSTING SCHEDULE – PERPETUAL OR SOFTWARE-AS-A-SERVICE SCHEDULE), SIX (6) TIMES ALL FEES AND CHARGES ACTUALLY PAID BY CUSTOMER TO HYLAND AS DESCRIBED IN THIS AGREEMENT DURING THE YEAR IN WHICH SUCH CUSTOMER DATA INCIDENT OCCURRED; AND (B) WITH RESPECT TO CLAIMS BASED UPON ALL OTHER MATTERS, THE AMOUNT OF FEES AND CHARGES ACTUALLY PAID BY CUSTOMER TO HYLAND AS DESCRIBED IN THIS AGREEMENT DURING THE TWELVE (12) MONTH PERIOD IMMEDIATELY PRECEDING THE OCCURRENCE OF THE EVENT GIVING RISE TO SUCH LIABILITY. NOTWITHSTANDING ANY OF THE FOREGOING, IN NO EVENT SHALL MICROSOFT, AS A SUPPLIER TO HYLAND OF THIRD PARTY SOFTWARE BUNDLED WITH THE SOFTWARE LICENSED UNDER THIS AGREEMENT, BE LIABLE FOR ANY DIRECT DAMAGES IN EXCESS OF FIVE DOLLARS ($5.00).

6.3 NOTWITHSTANDING ANYTHING TO THE CONTRARY, THE LIMITATIONS OF SECTIONS 6.1 AND 6.2(B) ABOVE, AS APPLICABLE, SHALL NOT APPLY WITH RESPECT TO: (1) ANY CLAIMS, LOSSES OR DAMAGES OF THIRD PARTIES THAT ARE SUBJECT TO HYLAND'S INDEMNIFICATION OBLIGATIONS UNDER THIS AGREEMENT; (2) ANY CLAIMS, LOSSES OR DAMAGES ARISING OUT OF THE RESPONSIBLE PARTY'S BREACH OF SECTION 3 (CONFIDENTIAL INFORMATION) (EXCEPT WITH RESPECT

Contractor Initials _HSL_
Date _03/13/2020_

TO CUSTOMER DATA AS DEFINED FOR A HOSTING SCHEDULE – PERPETUAL OR SOFTWARE-AS-A-SERVICE SCHEDULE); OR (3) ANY CLAIMS, LOSSES OR DAMAGES ARISING OUT OF CUSTOMER'S OR CONTRACTOR'S PROHIBITED ACTS.

7.   **FORCE MAJEURE.** No failure, delay or default in performance of any obligation of a party to this Agreement (except the payment of money) shall constitute a default or breach to the extent that such failure to perform, delay or default arises out of a cause, existing or future, beyond the control (including, but not limited to: action or inaction of governmental, civil or military authority; fire; strike, lockout or other labor dispute; flood; war; riot; theft; earthquake; natural disaster or acts of God; national emergencies; unavailability of materials or utilities; sabotage; viruses; or the act, negligence or default of the other party) and without negligence or willful misconduct of the party otherwise chargeable with failure, delay or default. Either party desiring to rely upon any of the foregoing as an excuse for failure, default or delay in performance shall, when the cause arises, give to the other party prompt notice in writing of the facts which constitute such cause; and, when the cause ceases to exist, give prompt notice of that fact to the other party. This Section 7 shall in no way limit the right of either party to make any claim against third parties for any damages suffered due to said causes: If any performance date by a party under this Agreement is postponed or extended pursuant to this Section 7 for longer than ninety (90) calendar days, the other party, by written notice given during the postponement or extension, and at least thirty (30) days prior to the effective date of termination, may terminate this Agreement.

8.   **GENERAL PROVISIONS.**

8.1   Intentionally omitted.

8.2   Interpretation. The headings used in this Agreement are for reference and convenience purposes only and shall not in any way limit or affect the meaning or interpretation of any of the terms hereof. All defined terms in this Agreement shall be deemed to refer to the masculine, feminine, neuter, singular or plural, in each instance as the context or particular facts may require. Use of the terms "hereunder," "herein," "hereby" and similar terms refer to this Agreement.

8.3   Waiver. No waiver of any right or remedy on one occasion by either party shall be deemed a waiver of such right or remedy on any other occasion.

8.4   Integration. This Agreement, including any and all exhibits and schedules referred to herein, set forth the entire agreement and understanding between the parties pertaining to the subject matter and merges and supersedes all prior agreements, negotiations and discussions between them on the same subject matter. This Agreement shall not be supplemented or modified by any course of performance, course of dealing or trade usage. Customer and Hyland specifically acknowledge and agree that any other terms varying from or adding to the terms of this Agreement, whether contained in any purchase order or other electronic, written or oral communication made from Customer to Hyland are rejected and shall be null and void and of no force or effect, unless expressly agreed to in writing by both parties.

8.5   Intentionally omitted.

8.6   Binding Effect; No Assignment. This Agreement shall be binding upon and shall inure to the benefit of the parties and their respective successors and permitted assigns.

8.7   Intentionally omitted.

8.8   Intentionally omitted.

8.9   Independent Contractor. The parties acknowledge that Hyland is an independent contractor and that it will be responsible for its obligations as employer for those individuals providing any services.

8.10   Export. The Software, Third Party Software, Work Products and Documentation are subject to export control laws and regulations of the United States and other jurisdictions. Customer agrees to comply fully with all relevant export control laws and regulations, including the regulations of the U.S. Department of Commerce and all U.S. export control laws, including, but not limited to, the U.S. Department of Commerce Export Administration Regulations (EAR), to assure that the Software, Third Party Software, Work Products or Documentation is not exported in violation of United States of America law or the laws and regulations of other jurisdictions. Customer agrees that it will not export or re-export the Software, Third Party Software, Work Products or Documentation to any organizations or nationals in the United States embargoed territories of Cuba, Iran, North Korea, Sudan, Syria or any other territory or nation with respect to which the U.S. Department of Commerce, the U.S. Department of State or the U.S. Department of Treasury maintains any commercial activities sanctions program. Customer shall not use the Software, Third Party Software, Work Products, or Documentation for any prohibited end uses under applicable laws and regulations of the United States and other jurisdictions, including but not limited to, any application related to, or purposes associated with, nuclear, chemical or biological warfare, missile technology (including unmanned air vehicles), military application or any other use prohibited or restricted under the U.S. Export Administration Regulations (EAR) or any other relevant laws, rules or regulations of the United States of America and other jurisdictions.

8.11   Injunctive Relief. The parties to this Agreement recognize that a remedy at law for a breach of the provisions of this Agreement relating to Confidential Information and intellectual property rights will not be adequate for the aggrieved party's protection and, accordingly, the aggrieved party shall have the right to seek, in addition to any other relief and remedies available to it, specific performance or injunctive relief to enforce the provisions

<div align="center">Page 9 of 32</div>

of this Agreement. Notwithstanding the foregoing, nothing herein contained shall be deemed to constitute a waiver of the sovereign immunity of the State, which immunity is hereby reserved to the State.

8.12 *Intentionally Omitted.*

8.13 <u>Third Parties</u>. Nothing herein expressed or implied is intended or shall be construed to confer upon or give to any person or entity, other than the parties hereto, any rights or remedies by reason of this Agreement; provided, however, that third party suppliers of software products bundled with the Software are third party beneficiaries to this Agreement as it applies to their respective software products.

9. **DEFINED TERMS.**

9.1 General Defined Terms

"Customer" means State of New Hampshire, Department of Labor.

"Delivery" means:

(a)   in the case of Software: (1) for any Software module included in the initial Software referenced in the Initial Purchase Table Schedule, by the electronic downloading of such Software onto Customer's systems, or such Software being made available by Hyland to Customer for electronic download onto Customer's systems from a location identified by Hyland to Customer; or (2) in the case of any later licensed Software module, by the Delivery (in accordance with subparagraph (b) below) by Hyland to Customer of a Production Certificate which includes such Software module; and

(b)   in the case of a Production Certificate, by Hyland either shipping (physically or electronically) the Production Certificate to Customer or making the Production Certificate available for electronic download by Customer from a location identified by Hyland to Customer (including through one of Hyland's authorized solution providers).

"Documentation" means: (a) in the case of the Software: (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; or (b) in the case of any Work Product, the Specifications (if any) for the Work Product.

"Error" means any defect or condition inherent in the Software which is reported by Customer in accordance with this Agreement and which is confirmed by Hyland, that causes the Software to fail to function in any material respect as described in the Documentation.

"Error Correction Services" means Hyland's reasonable efforts to correct an Error, which may be effected by a reasonable workaround.

"Initial Maintenance Period" means the twelve (12) month period of Maintenance and Support that begins on the ninetieth (90th) day after the Effective Date of the Maintenance Schedule.

"Innovations" means all designs, processes, procedures, methods and innovations which are developed, discovered, conceived or introduced by Hyland, working either alone or in conjunction with others, in the performance of this Agreement (including any Services Proposal).

"Maintenance and Support" means for Supported Software, (i) Error Correction Services; (ii) Technical Support Services; and (iii) the availability of Upgrades and Enhancements in accordance with a Maintenance Schedule or Software License and Maintenance Schedule - Subscription.

"Production Certificate" means: license codes, a license certificate, or an IFM file issued by Hyland and necessary for Customer to activate Software for Customer's production use.

"Prohibited Acts" mean any action taken by Customer that is: (i) in violation of Section 1 of a Software License Schedule - Perpetual or Section 1, 2 or 3 of a Software and Maintenance Schedule – Subscription or Section 2 of a SaaS Schedule or (ii) contrary to Section 4 of these General Terms.

"Professional Services" means any professional services provided by Hyland under a Services Proposal, including but not limited to those services listed at https://www.hyland.com/community. Examples of the services include: (a) installation of the Software; (b) consulting, implementation and integration projects related to the Software, including but not limited to the customized configuration of Software integration modules or business process automation modules; (c) project management; (d) development projects in connection with the integration of Software with other applications utilizing any Software application programming interface (API).

"Resolution" means Hyland provides Customer with a reasonable workaround, correction, or modification that solves or mitigates a reported Error.

"Services Proposal" means either: (a) a written proposal, statement of work or services sales order form issued under a Professional Services Schedule, and which sets forth the Professional Services Hyland will provide to Customer and which is signed by Customer and Hyland; or (b) a purchase order submitted by Customer and accepted by Hyland for Professional Services.

"State Fiscal Year" or "SFY" means the New Hampshire State Fiscal Year which runs from July 1 through June 30 of the following calendar year.

Contractor Initials *HBK*
Date *03/17/2020*

"Software" means: (a) Hyland's proprietary software products, listed in the Initial Purchase Table Schedule, and other Hyland proprietary software products for which Customer submits a written purchase order to Hyland (or an authorized solution provider) that Hyland accepts and fulfills, including, in each case, third party software bundled by Hyland together with Hyland's proprietary software products as a unified product; and (b) all Upgrades and Enhancements of the software products described in clause (a) which Customer properly obtains pursuant to Maintenance and Support or received under a SaaS Schedule.

"Specifications" means the definitive, final functional specifications for Work Products, if any, produced by Hyland under a Services Proposal.

"Supported Software; Retired Software". At any particular time during a maintenance period covered by an applicable Maintenance Schedule or Software License and Maintenance Schedule - Subscription: (a) "Supported Software" means the current released version of the Software licensed by Customer from Hyland and any other version of such Software that is not Retired Software; or (b) "Retired Software" means any version of the Software licensed by Customer from Hyland under this Agreement which is identified as being retired on Hyland's applicable secure end user web site. Hyland will specify on its end user web site Software versions which become Retired Software. The effective date of such change will be twelve (12) months from the date Hyland initially posts the status change on its end user web site, and Customer will receive notice as a registered user of Hyland's applicable secure end user web site.

"Technical Support Services" means telephone or online technical support related to problems reported by Customer and associated with the operation of any Supported Software, including assistance and advice related to the operation of the Supported Software. Technical Support Services are not available for Retired Software.

"Upgrades and Enhancements" means any and all new versions, improvements, modifications, upgrades, updates, fixes and additions to Software that Hyland makes available to Customer or to Hyland's end users generally during the term of a Maintenance Schedule or Software License and Maintenance Schedule – Subscription or a SaaS Schedule to correct Errors or deficiencies or enhance the capabilities of the Software, together with updates of the Documentation to reflect such new versions, improvements, modifications, upgrades, fixes or additions; provided, however, that the foregoing shall not include new, separate product offerings, new modules or re-platformed Software.

"Working Hour" means the services of one (1) person for a period of one (1) hour (or any part thereof) during regular business hours, and shall include the travel time during which Hyland's resource(s) is required to travel outside of the metropolitan area in which such Hyland resource(s) regularly works when not at a third party location; provided that time spent commuting from a local place of residence (including a hotel) to a work location in the same metropolitan area will not be included in travel time.

"Work Products" means all items in the nature of computer software, including source code, object code, scripts, and any components or elements of the foregoing, or items created using the configuration tools of the Software, together with any and all design documents associated with items in the nature of computer software, in each case which are created, developed, discovered, conceived or introduced by Hyland, working either alone or in conjunction with others, in the performance of services under this Agreement. If applicable, Work Products shall include any pre-configured templates or VBScripts which have been or may be created or otherwise provided by Hyland to Customer as part of the configuration of the advance capture module of the Software.

9.3   Additional Defined Terms - Hosting Schedule.

"Consumption Fees" means the amounts payable by Customer for storage of data and information in the Hosted Solution in excess of the data storage allocation set forth in the Initial Purchase Table Schedule for the Hosted Solution.

"Customer Data" means any and all electronic data and information of Customer stored within the Hosted Solution.

"Customer Data Incident" means an unauthorized disclosure of Customer Data resulting from Hyland's failure to comply with the Hosted Solution Security Attachment. Without limitation, Customer Data Incident does not include any of the following that results in no unauthorized access to Customer Data or to any Hyland's systems storing Customer Data: (a) pings and other broadcast attacks on firewalls or edge servers; (b) port scans; (c) unsuccessful log-on attempts; (d) denial of service attacks; or (e) packet sniffing (or other unauthorized access to traffic data that does not result in access beyond IP addresses or headers).

"Host Web Site" means the web site hosted by Hyland as part of the Hosted Solution on a web server included in the Network, through which Customer will access the Software and Customer Data stored using the Software.

"Hosted Solution" means a Host Web Site, Network, Software, Third Party Software and Hosting Services provided, collectively, by Hyland under this Agreement.

"Hosted Solution Support" means the services described in Section 2 of the Hosting Schedule.

"Hosting Fees" means the amounts invoiced by Hyland to Customer and payable by Customer to Hyland for Hosting Services included in the Hosted Solution. The initial Hosting Fees are set forth in either the Initial Purchase Table Schedule when Hosting Services are purchased initially, or in an Amendment to this Agreement when Hosting Services are added after the Effective Date.

Contractor Initials _NBK_
Date _8/13/2020_

"Hosting Services" means the Standard Hosting Services and any Optional Hosting Services included in the Hosted Solution.

"Initial Setup Fee" means the one-time fee invoiced by Hyland to Customer and payable by Customer to Hyland for the setup and activation of the Network and the Host Web Site for use applicable to each Software purchase under the Agreement.

"Network" means the computers and peripheral storage devices, switches, firewalls, routers and other network devices provided by Hyland as part of the Hosted Solution.

"Optional Hosting Services" means optional services described in the Process Manual which Hyland offers as Hosting Services, but which are not included in the Standard Hosting Services.

"Process Manual" means the latest version of the manual describing the Hosting Services, the Network and certain other components of the Hosted Solution, including the attestations, certification documents and assistance with compliance and security testing Hyland agrees to provide, based upon the Service Class selected by Customer, as posted by Hyland from time to time on a website designated by Hyland.

"Service Class" means the service level commitment included as part of Standard Hosting Services, as described in the Service Class Manual, and purchased by Customer as part of the Hosted Solution.

"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.

"Standard Hosting Services" means the Hosting Services described in the Process Manual as being standard hosting services.

"Third Party Software" means all third party software products (other than third party software products bundled by Hyland as a part of the Software) licensed by Hyland and sublicensed through this Agreement by Hyland to Customer as part of the Hosted Solution.

"User Testing Environment" means a separate instance of the Software, Third Party Software and Work Products (including Customer Data) hosted by Hyland on the Network for Customer, for use by Customer solely with production data in a non-production environment for the limited purpose of functional and performance testing of the Software and environment, Third Party Software and each Work Product.

"User Testing Lite Environment" means a separate instance of the Software, Third Party Software and Work Products (including Customer Data) hosted by Hyland on the Network for Customer, for use by Customer solely with production data in a non-production environment for the limited purpose of functional testing of the Software and environment, Third Party Software and each Work Product.

Contractor Initials _MBK_

Date _03/13/2020_

EXHIBIT B
SCQPE OF SERVICES

1. Deliverables

This Contract is for Software licensing and Hosting Services as more fully detailed below.

1. Contractor shall provide the State a perpetual, non-exclusive, non-assignable, limited license to the OnBase Enterprise Content Management (ECM) System, an electronic document management system, as specified in Exhibit D, which is incorporated by reference herein.

2. Contractor shall provide hosting services as specified in Exhibit F, which is incorporated by reference herein.

3. Subject to Customer registering for and paying the applicable training fees, Hyland shall make available to the State the OnBase Workflow Administration Certification training and OnBase System Administration Certification Training.

   - The OnBase System Administration Certification Training provides in-depth, hands-on experience that directly maps to the day-to-day activities of an OnBase System Administrator.

   - The OnBase Workflow Administration Certification Training presents a hands-on approach to understanding the Workflow interface, interactions and possibilities

4. Hyland shall provide maintenance services as specified in Exhibit E, which is incorporated by reference herein.

Contractor Initials *NBR*

Date *03/13/2020*

EXHIBIT C
PRICING & PAYMENTS

4. PRICING & PAYMENT SCHEDULE

This is a Not to Exceed Contract. The total Contract value is indicated in Part 1, P-37 General Provisions - Block 1.8: Price Limitation for the period between the Effective Date through date indicated in Part 1, P-37 General Provisions - Block 1.7: Completion Date. The Contractor shall perform its obligations under this Contract at the price as specified below.

The payment by the State of the total contract price shall be the only and the complete reimbursement to the Contractor for all fees and expenses, of whatever nature, incurred by the Contractor in the performance hereof.

Table 4.1

Contractor Initials _7L&L_
Date _03/13/2020_

	ACTIVITY, DELIVERABLE or MILESTONE	PROJECTED DELIVERY DATE	TOTAL AMT	PAYMENT AMOUNT DUE
	SFY20 Hyland Cloud Fees			
1.1	SFY20 Hyland Cloud Annual Hosting Fee	03/01/2020	$109,246.08	$109,246.08
1.2	SFY20 Hyland Cloud Hosting Setup Fee	03/01/2020	$9,103.84	$9,103.84
1.3	SFY20 Hyland Cloud Backfile Conversion Storage Fee	03/01/2020	$6,000.00	$6,000.00
1.4	SFY20 Hyland Cloud Annual Active Directory Federation Services Annual Fee	03/01/2020	$1,632.00	$1,632.00
	SFY20 OnBase Software Acquisition			
2.1	SFY20 Software Procurement (see section 5 OnBase Software Licensing Table Listing)	03/01/2020	$286,497.60	$286,497.60
2.2	SFY20 Software Maintenance Procurement	03/01/2020	$56,810.00	$56,810.00
	Initial Hyland Certification and Online Training			
3.1	OnBase System Administration Certification Training	03/01/2020	$2,570.40	$2,570.40
3.2	OnBase Workflow Administration Certification Training	03/01/2020	$2,570.40	$2,570.40
	SFY20 Contingency Funds			
4.1	SFY20 Funds for purchasing Additional Hosting Storage, Licensing and Training. Additional costs would be in affect if additional storage capacity was in need. Additional costs would be in affect if additional State resources required training. Additional costs would be in affect if additional user licenses were needed.	03/01/2020	$75,000.00	$75,000.00
	SFY21 Annual Sustainability Cost			
5.1	SFY21 Hyland Cloud Annual Hosting Fee	1/1/2021	$109,246.08	$109,246.08
5.2	SFY21 Hyland OnBase Annual Maintenance Fee	1/1/2021	$56,809.92	$56,809.92
5.3	SFY21 Hyland Cloud Annual Active Directory Federation Services Annual Fee	1/1/2021	$1,632.00	$1,632.00
	SFY22 Annual Sustainability Cost			
6.1	SFY22 Hyland Cloud Annual Hosting Fee	1/1/2022	$109,246.08	$109,246.08
6.2	SFY22 Hyland OnBase Annual Maintenance Fee	1/1/2022	$56,809.92	$56,809.92
6.3	SFY22 Hyland Cloud Annual Active Directory Federation Services Annual Fee	1/1/2022	$1,632.00	$1,632.00
	SFY23 Annual Sustainability Cost			
7.1	SFY23 Hyland Cloud Annual Hosting Fee	1/1/2023	$109,246.08	$109,246.08
7.2	SFY23 Hyland OnBase Annual Maintenance Fee	1/1/2023	$56,809.92	$56,809.92
7.3	SFY23 Hyland Cloud Annual Active Directory Federation Services Annual Fee	1/1/2023	$1,632.00	$1,632.00
	SFY24 Annual Sustainability Cost			
8.1	SFY24 Hyland Cloud Annual Hosting Fee	1/1/2024	$109,246.08	$109,246.08
8.2	SFY24 Hyland OnBase Annual Maintenance Fee	1/1/2024	$56,809.92	$56,809.92
8.3	SFY24 Hyland Cloud Annual Active Directory Federation Services Annual Fee	1/1/2024	$1,632.00	$1,632.00

Contractor Initials _7L8L_
Date _03/13/2020_

5. ONBASE SOFTWARE LICENSING TABLE LISTING –

Contractor shall provide the Software at the cost defined below, which such cost reflects initial one-time license fees for perpetual licenses to the Software. Any additional Software licenses require an amendment (if required) to this contract or a separate procurement and will be subject to the current pricing under the procurement vehicle used to purchase such licenses:

#	Software Item	Product	Unit Cost	Units	Cost
	OnBase Software		OMNIA		
1	Multi-User License	OBIPW1	$6,528.00	1	$6,528.00
2	Unity Client Server	UNIPI1	$12,240.00	1	$12,240.00
3	EDM Services	DMIPI1	$4,080.00	1	$4,080.00
4	Document Import Processor (DIP)	DPIPW1	$4,080.00	1	$4,080.00
5	Named Client Software	CTIPN1	$571.20	86	$49,123.20
6	Workflow Named Client SL	WLIPN1	$886.21	86	$76,214.40
7	Production Document Imaging (Kofax or TWAIN) First (1)	DIIPW1	$4,080.00	1	$4,080.00
8	Application Enabler	AEIPI1	$16,320.00	1	$16,320.00
9	Advanced Capture	IAIPW1	$20,400.00	1	$20,400.00
10	Document Retention	DRIPI1	$8,160.00	1	$8,160.00
11	Integration for Microsoft Outlook	OUTIPI1	$8,160.00	1	$8,160.00
12	Full Text Search	FTSIPI1	$16,320.00	1	$16,320.00
13	Mobile Access for iPAD	OMIPW1-IPAD	$4,080.00	1	$4,080.00
14	Mobile Access for iPHONE	OMIPW1-IPHONE	$4,080.00	1	$4,080.00
15	Reporting Dashboards	RHIPI1	$8,160.00	1	$8,160.00
16	Encrypted Disk Groups	EHIPI1	$8,160.00	1	$8,160.00
17	Encrypted Alpha Keywords	AKIPI1	$8,160.00	1	$8,160.00
18	Document Composition	ADIPI1	$16,320.00	1	$16,320.00
19	Single Sign-On for Microsoft Active Directory Federation Services	SNIPI15	$0.00	1	$0.00
20	PDF Framework	PDFIPI1	$2,448.00	1	$2,448.00
22	Archival API	ARIPI1	$4,080.00	1	$4,080.00
23	Virtual Print Driver	PTIPCI	$4,080.00	1	$4,080.00
24	Workview Concurrent Client (1-20)	VLIPCI	$1,224.00	1	$1,224.00

Page 16 of 32

Contractor Initials _NBR_
Date _03/13/2020_

	Total Software Cost:				$286,497.60

6. INVOICING

Contractor shall submit correct invoices to the State for all amounts to be paid by the State. The Contractor shall only submit invoices for Services or Deliverables as permitted by the Contract. Invoices must be in a format as determined by the State and contain detailed information, including without limitation: itemization of each Deliverable and identification of the Deliverable for which payment is sought, and the Acceptance date triggering such payment; date of delivery and/or installation; monthly maintenance charges; any other Project costs or retention amounts if applicable.

Upon Acceptance of a Deliverable, and a properly documented and undisputed invoice, the State will pay the correct and undisputed invoice within thirty (30) days of invoice receipt. Invoices will not be backdated and shall be promptly dispatched.

Invoices shall be emailed to:

NHDOL Business Office: businessoffice@dol.nh.gov
Cc: Joseph.A.Nadeau@DoIT.nh.gov

7. PAYMENT ADDRESS

Payments shall be made via ACH. Use the following link to enroll with the State Treasury for ACH payments:
https://www.nh.gov/treasury/state-vendors/index.htm

8. OVERPAYMENTS TO THE CONTRACTOR

Contractor shall promptly, but no later than fifteen (15) business days, return to the State the full amount of any overpayment or erroneous payment upon discovery or notice from the State.

9. CREDITS

The State may apply credits due to the State arising out of this Contract, against Contractor's invoices with appropriate information attached.

10. TRAVEL EXPENSES

The Contractor must assume all travel and related expenses. All labor rates will be "fully loaded", including, but not limited to: meals, hotel/housing, airfare, car rentals, car mileage, and out of pocket expenses. The State shall not be responsible for any travel or out of pocket expenses incurred in the performance of the Services performed under this Contract.

11. SHIPPING AND DELIVERY FEE EXEMPTION

The State will not pay for any shipping or delivery fees unless specifically itemized in the Contract.

Contractor Initials _TBK_
Date _03/13/2020_

EXHIBIT D

SOFTWARE LICENSE SCHEDULE - PERPETUAL

(Perpetual License for Software)

All capitalized terms not defined in this Schedule shall have the meaning ascribed them in the General Terms.

1.   **SOFTWARE AND WORK PRODUCTS LICENSE.**

1.1   _License Grant._ Subject to Customer's payment in full of the Software license fees and subject further to Customer's compliance with this Agreement, Hyland grants to Customer a perpetual (except as otherwise provided in this Agreement), non-exclusive, non-assignable, limited license to: (a) the Software, in machine-readable object code form only, and the associated Documentation; and (b) Work Products and associated Documentation; in each case solely for use:

        (1)   by Customer internally, and only for storing, processing and accessing Customer's own data; and

        (2)   subject to Section 1.8 below, by a third party contractor retained by Customer as a provider of services to Customer ("Third Party Contractor"), but only by the Third Party Contractor for capturing, storing, processing and accessing Customer's own data in fulfillment of the Third Party Contractor's contractual obligations as a service provider to Customer.

The Software, Work Products and associated Documentation are licensed for use by a single organization and may not be used for processing of third-party data as a service bureau, application service provider or otherwise. Customer shall not make any use of the Software, Work Products or Documentation in any manner not expressly permitted by this Agreement. Software subject to a regulatory control may only be installed in the country identified as the end user location in the purchase order.

1.2   _Modification of Work Products._

1.2.1   _Form of Delivered Work Products._ The form in which Hyland delivers Work Products will be determined by Hyland depending on the purpose and functionality of the Work Product.

1.2.2   _Configuration Work Products._ If Hyland delivers a Work Product: (a) in the form of (1) source code which is compiled by tools in the Software to machine language form; or (2) a script; or (b) created using the configuration tools in the Software (a "Configuration Work Product"), then Hyland grants to Customer the limited right to modify the Configuration Work Product, provided such altered or modified Configuration Work Product is used only in compliance with the terms of the limited license to such Work Product granted under Section 1.1 above.

1.2.3   _Independent Work Products._ If Hyland delivers a Work Product which is not a Configuration Work Product (an "Independent Work Product"), then, except as otherwise provided in the last sentence of this paragraph, Customer may not modify such Independent Work Product. If Hyland delivers an Independent Work Product, and Customer desires to obtain the right to modify the Independent Work Product, then the parties may mutually agree that Hyland shall deliver to Customer a copy of the format of the source Independent Work Product that is necessary to enable the Customer to complete its modifications, subject to and upon the payment by Customer to Hyland of any additional Professional Services fees as Hyland may charge to prepare and deliver such format. In such case, Hyland grants to Customer the right to modify and, if necessary, compile the delivered format of the Independent Work Product, provided the modified Independent Work Product is used only in compliance with the terms of the limited license to such Work Product granted under Section 1.1 above.

1.3   _Use Restriction._ Each module of the Software and each Work Product is licensed for a specific type of use, such as concurrently or on a specified workstation or by a specified individual and the Software may control such use. Software products that are volume-based may: (i) no longer function if applicable volume limits have been exceeded; or (ii) include functionality which monitors or tracks Customer usage and reports that usage. Upon reasonable notice to Customer and to the extent permitted by law, Hyland shall be permitted access to Customer's Software system to measure Customer's volume usage of such Software. Customer acknowledges and agrees that additional fees may apply based on Customer's volume usage. Customer may not circumvent or attempt to circumvent this restriction by any means, including but not limited to changing the computer calendars. Use of software or hardware that reduces the number of users directly accessing or utilizing the Software (sometimes called "multiplexing" or "pooling" software or hardware) does not reduce the number of Software licenses required. The required number of Software licenses would equal the number of distinct inputs to the multiplexing or pooling software or hardware. Customer is prohibited from using any software other than the Software Client modules or a Software application programming interface (API) to access the Software 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 Customer's use of such other software and Customer has paid to Hyland the Software license fees with respect to such access to the Software or data stored in the Software database in accordance with Hyland's licensing policies applicable to the Software modules that provide access to the Software application modules and data stored in the Software database. Customer further agrees that, in connection with any use of the Software and Work Products, the Software and Work Products shall not be copied and installed on additional servers unless Customer has purchased a license therefore, and the number of users of the Software shall not exceed the number of users permitted by the Software Client licenses purchased by Customer.

1.3.1 Any additional fees specified in 1.3 above are subject to prior notice and Customer's prior consent, subject to Provision 4 of the P37, General Provisions, and subject to the amendment process pursuant to Provision 17, of the P37, General Provisions.

Contractor Initials _NBL_
Date _03/13/2020_

1.4   Production and Test Systems. Customer shall be entitled to use one (1) production copy of the Software and each Work Product licensed and one (1) additional copy of the production environment licensed Software and Work Products for customary remote disaster recovery purposes which may not be used as a production system concurrently with the operation of any other copy of the Software and Work Products in a production environment. Subject to the payment of any additional applicable license fees, Customer shall also be entitled to license a reasonable number of additional copies of the production environment licensed Software and Work Products to be used exclusively in a non-production environment on Customer's own computer network and solely for the purposes of experimenting and testing the Software and Work Products, developing integrations between the Software and other applications that integrate to the Software or Work Products solely using integration modules of the Software licensed by Customer under this Agreement, and training Customer's employees on the Software and Work Products ("Test Systems"). Hyland reserves the right to further define the permitted use(s) and/or restrict the use(s) of the Test Systems. Customer's sole recourse in the event of any dissatisfaction with any Software or Work Products in any non-production system is to stop using such Software or Work Products and return it to Hyland, provided that, in the event Customer is currently purchasing Maintenance and Support from Hyland, to the extent that Customer is using the Test System for the purposes of testing an Upgrade or Enhancement of the Software prior to implementing the same in Customer's production environment, then Customer may contact Hyland for the provision of Maintenance and Support as described in Section 1.6 of the Maintenance Schedule. Customer shall not make any copies of the Software or Work Products not specifically authorized by this Section 1.4.

1.5   Evaluation Software. From time to time Customer may elect to evaluate certain Software modules ("Evaluation Software") for the purpose of determining whether or not to purchase a production license of such Evaluation Software. Evaluation Software is licensed for Customer's use in Customer's Test Systems. Notwithstanding anything to the contrary, as to any Evaluation Software, the Agreement and the limited license granted hereby will terminate on the earliest of: (a) last day of the evaluation period specified in the accepted purchase order delivered for such Evaluation Software; or (b) immediately upon the delivery of written notice to such effect by Hyland to Customer. Upon expiration or other termination of such period, Customer immediately shall either (y) discontinue any and all of use of the Evaluation Software and related Documentation and remove the Evaluation Software; or (z) deliver a purchase order for purchase of such Evaluation Software.

1.6   Third Party Licenses. The Software may be bundled with software owned by third parties, including but not limited to those manufacturers listed in the Help About screen of the Software. Such third party software is licensed solely for use within the Software and is not to be used on a stand-alone basis. Notwithstanding the above, Customer acknowledges that, depending on the modules licensed, the Software may include open source software governed by an open source license, in which case the open source license (a copy of which is either provided in the Software or available upon written request) may grant you additional rights to such open source software. Additionally, in the case of such software to be downloaded and installed on a mobile device, if such software will be downloaded from the application market or store maintained by the manufacturer of the mobile device, then use of such software will be governed by the license terms for the software included at the applicable application store or market or presented to Customer or Customer's user in the software, and this Agreement will not govern such use.

1.7   Integration Code. If applicable, Software also includes all adapters created by Hyland and provided to you by Hyland as part of an integration between the Software and a third party line of business application ("Integration Code"). Such Integration Code may only be used in combination with the Software and in accordance with the terms of this Agreement.

1.8   Contractor Use Agreement. Customer agrees that if it desires to allow a Third Party Contractor to do any of the following:

          (a)   make use of the Software configuration tools, Software administrative tools or any of the Software's application programming interfaces ("APIs");

          (b)   make use of any training materials or attend any training courses, either online or in person, in either case related to the Software; or

          (c)   access any of Hyland's secure websites (including, but not limited to, users.onbase.com, teamonbase.com, training.onbase.com, demo.onbase.com, and Hyland.com/Community), either through Third Party Contractor's use of Customer's own log-in credentials or through credentials received directly or indirectly by Third Party Contractor;

then, Customer must cause such Third Party Contractor to execute a use agreement in a form available for download at Hyland's Community website ("Contractor Use Agreement"). Customer understands and agrees that: (x) Customer may not allow a Third Party Contractor to do any of the foregoing if such Third Party Contractor has not signed a Contractor Use Agreement, and (y) Third Party Contractors may use the Software only in compliance with the terms of this Agreement, and (z) Customer is responsible for such compliance by all Third Party Contractors that do not execute a Contractor Use Agreement.

1.9   No High Risk Use. The Software is not fault-tolerant and is not guaranteed to be error free or to operate uninterrupted. The Software is not designed or intended for use in any situation where failure or fault of any kind of the Software could lead to death or serious bodily injury to any person, or to severe physical or environmental damage ("High Risk Use"). Customer is not licensed to use the Software 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 Software for administrative purposes, 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. Customer agrees not to use, distribute or sublicense the use of the Software in, or in connection with, any High Risk Use.

Page 19 of 32

Contractor Initials _7L61_
Date _03/13/2020_

1.10   Audit Rights. Upon reasonable notice to Customer, Hyland shall be permitted access to audit Customer's use of the Software solely in order to determine Customer's compliance with the licensing and pricing terms this Agreement. Customer shall reasonably cooperate with Hyland with respect to its performance of such audit. Customer acknowledges and agrees that Customer is prohibited from publishing the results of any benchmark test using the Software to any third party without Hyland's prior written approval, and that Customer has not relied on the future availability of any programs or services in entering into this Agreement.

1.11   AnyDoc. The optional AccuZip component of the OCR for AnyDoc and AnyDoc EXCHANGEit Software products contains material obtained under agreement from the United States Postal Service (USPS) and must be kept current via an update plan provided by Hyland to maintain Customer's continued right to use. The USPS has contractually required Hyland to include "technology which automatically disables access to outdated [zip code] products." This technology disables only the AccuZip component and is activated only if AccuZip is not updated on a regular and timely basis. Hyland regularly updates the zip code list as part of Maintenance and Support for the AccuZip module.

2.   U.S. GOVERNMENT END USERS. To the extent applicable, the terms and conditions of this Agreement shall pertain to the U.S. Government's use and/or disclosure of the Software and the Work Products, and shall supersede any conflicting contractual terms or conditions. By accepting the terms of this Agreement and/or the Delivery of the Software, the U.S. Government hereby agrees that the Software qualifies 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 U.S. Federal law, the U.S. Government agrees to return the Software and Work Products to Hyland. In addition to the foregoing, where DFARS is applicable, use, modification, reproduction, release, display, or disclosure of the Software, Work Products or Documentation by the U.S. Government is subject solely to the terms of this Agreement, as stated in DFARS 227.7202, and the terms of this Agreement shall supersede any conflicting contractual term or conditions.

3.   LIMITED WARRANTY FOR SUPPORTED SOFTWARE AND WORK PRODUCTS.

3.1   Supported Software. For a period of sixty (60) days from and including the date a Supported Software module listed in the Initial Purchase Table Schedule has been Delivered to Customer, and for a period of sixty (60) days from and including the date any other Supported Software module has been Delivered to Customer, Hyland warrants to Customer that such Supported Software module, when properly installed and properly used, 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: (a) any Retired Software modules; or (b) any Supported Software module that has been (i) modified by Customer or a third party, (ii) used in combination with equipment or software other than that which is consistent with the Documentation, or (iii) misused or abused.

3.2   Work Products. For a period of sixty (60) days from and including the date that Hyland has delivered a completed Work Product to Customer, Hyland warrants to Customer that such Work Product, when properly installed and properly used, 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, any Work Product that has been (a) modified or added to by Customer or a third party, (b) used in combination with equipment or software other than that which is consistent with the Documentation, or (c) misused or abused.

3.3   Remedy. Hyland's sole obligation, and Customer's sole and exclusive remedy, for any non-conformities to the express limited warranties under Sections 3.1 or 3.2 shall be as follows: provided that, within the applicable 60-day period, Customer notifies Hyland in writing of the non-conformity, Hyland will either (a) repair or replace the non-conforming Supported Software module or Work Product, which may include the delivery of a reasonable workaround for the non-conformity; or (b) if Hyland determines that repair or replacement of the Supported Software module or Work Product is not practicable, then terminate this Agreement with respect to the non-conforming Supported Software module or with respect to the non-conforming Work Product, in which event, upon compliance by Customer with its obligations under Section 6.2 of this Schedule, Hyland will refund any portion of the Software license fees and annual maintenance fees paid prior to the time of such termination with respect to such Supported Software or the services fees paid prior to the time of such termination with respect to the creation and implementation of such Work Product.

3.4   Maintenance. Upon the expiration of the warranty provided in Section 3.1, and solely for the period, if any, that begins with the expiration of the warranty provided in Section 3.1 and ends with the commencement of the Initial Maintenance Period, all Errors will be supported in accordance with the Maintenance Schedule.

4.   SOFTWARE LICENSE FEES.

4.1   Initial Software Licensed. On or after the Effective Date, Hyland shall invoice Customer for the Software license fees specified in the Initial Purchase Table Schedule. Customer shall pay such invoice in full in accordance with the General Terms.

4.2   Follow-on Purchases of Licenses of Software. Software license fees for follow-on purchases of licenses of Software shall be determined at Hyland's retail list prices in effect at the time Customer submits its applicable purchase orders, or at such other prices as the parties may mutually agree upon. Hyland shall invoice Customer for such Software license fees on or after Hyland's acceptance of Customer's applicable purchase orders. Customer shall pay such invoices in full in accordance with the General Terms.

5.   RESERVED.

Contractor Initials _7LBL_

Date _03/13/2020_

6. **TERMINATION.**

6.1   <u>By Customer</u>. Customer or Hyland may terminate this Software License Schedule - Perpetual pursuant to Section 1.2 of the General Terms.

6.2   <u>Effects of Termination</u>. Upon any termination of this Software License Schedule - Perpetual in its entirety, any license to use the Software and Work Products will automatically terminate without other or further action on the part of any party; and Customer shall immediately: (a) discontinue any and all use of the Software, Work Products and Documentation; and (b) either (1) return the Software, Work Products and Documentation to Hyland, or (2) with the prior permission of Hyland, destroy the Software, Work Products and Documentation and certify in writing to Hyland that Customer has completed such destruction.

Contractor Initials _TBR_
Date _03/13/2020_

EXHIBIT E

<u>MAINTENANCE SCHEDULE</u>
(Maintenance and Support for Supported Software; Perpetual)

All capitalized terms not defined in this Schedule shall have the meaning ascribed them in the General Terms.

1. MAINTENANCE AND SUPPORT TERMS.

1.1 <u>Technical Support Services</u>. Hyland will provide telephone or online technical support related to problems reported by Customer and associated with the operation of any Supported Software, including assistance and advice related to the operation of the Supported Software. Technical Support Services are not available for Retired Software.

1.2 <u>Error Correction Services</u>. With respect to any Errors in the Supported Software which are reported by Customer and which are confirmed by Hyland, in the exercise of its reasonable judgment, Hyland will use its reasonable efforts to correct the Error which may be effected by a reasonable workaround. Hyland shall promptly commence to confirm any reported Errors after receipt of a proper report of such suspected Error from Customer. Hyland may elect to correct the Error in the current available or in the next available commercially released version of the Supported Software and the Resolution may require the Customer to implement an Upgrade and Enhancement in order to obtain the correction. Error Correction Services are not available for Retired Software.

1.3 <u>Reporting Policies and Procedures Applicable to Technical Support Services and Error Correction Services</u>. In requesting Maintenance and Support services, Customer will report through Hyland's secure end user website the details of which will be separately provided to Customer through the assigned technical support team. In the case of reporting an Error, Customer will provide Hyland with as much information and access to systems as reasonably possible to enable Hyland to investigate and attempt to identify and verify the Error. Customer will work with Hyland support personnel during the problem isolation process, as reasonably needed. Customer will notify Hyland of any configuration changes, such as network installation/expansion, Software upgrades, relocations, etc.

1.4 <u>Upgrades and Enhancements</u>. Hyland will provide, in accordance with Hyland's then current policies, as set forth from time to time on Hyland's secure end user web site (currently www.hyland.com/community), all Upgrades and Enhancements, if and when released during the term of this Maintenance Schedule. Upgrades and Enhancements are not available for Retired Software.

1.5 <u>On-line Access</u>. Customer acknowledges and agrees that Hyland may require on-line access to the Supported Software installed on Customer's systems in order to provide Maintenance and Support. Accordingly, Customer shall install and maintain means of communication and the appropriate communications software as mutually agreed upon by Hyland and Customer and an adequate connection with Hyland to facilitate Hyland's on-line Maintenance and Support. Such right of access and use shall be provided at no cost or charge to Hyland.

1.6 <u>Test Systems Support</u>. In the event Customer has a license to use a Test System (licensed pursuant to a Software License Schedule - Perpetual, or the applicable provision of a click-through or End User License Agreement) for the purposes of testing an Upgrade or Enhancement of the Software prior to implementing the same in Customer's production environment, then Customer may contact Hyland for the provision of Maintenance and Support as described in this Maintenance Schedule.

2. EXCLUSIONS.

2.1 <u>Generally</u>. Hyland is not responsible for providing, or obligated to provide, Maintenance and Support under this Agreement: (a) in connection with any Errors or problems that result in whole or in part from any alteration, revision, change, enhancement or modification of any nature of the Software, or from any error or defect in any configuration of the Software, which activities in any such case were undertaken by any party other than Hyland; (b) in connection with any Error if Hyland has previously provided corrections for such Error which Customer fails to implement; (c) in connection with any Errors or problems that have been caused by errors, defects, problems, alterations, revisions, changes, enhancements or modifications in the database, operating system, third party software (other than third party software embedded in the Software by Hyland), hardware or any system or networking utilized by Customer; (d) if the Software or related software or systems have been subjected to abuse, misuse, improper handling, accident or neglect; or (e) if any party other than Hyland, or an authorized subcontractor specifically selected by Hyland, has provided any services in the nature of Maintenance and Support to Customer with respect to the Software. Maintenance and Support does not include any services that Hyland may provide in connection with assisting or completing an upgrade of Supported Software with any available Upgrade and Enhancement.

2.2 <u>Work Products</u>. Maintenance and Support is not provided for any Work Products; however, if Customer desires Maintenance and Support regarding the operation or use of Work Products, Customer may request such Maintenance and Support and the parties may agree to enter into a Services Proposal for such Maintenance and Support in accordance with an applicable Professional Services Schedule.

2.3 <u>Excluded Software and Hardware</u>. This Schedule does not govern, and Hyland shall not be responsible for, the maintenance or support of any software other than Supported Software, or for any hardware or equipment of any kind or nature, whether or not obtained by Customer from Hyland.

3. CERTAIN OTHER RESPONSIBILITIES OF CUSTOMER.

Contractor Initials _715L_
Date _03/13/2020_

3.1   Operation of the Software and Related Systems. Customer acknowledges and agrees that it is solely responsible for the operation, supervision, configuration, management and control of the Software and all related hardware and software (including the database software). Customer is solely responsible for obtaining or providing training for its personnel; and for instituting appropriate security procedures and implementing reasonable procedures to examine and verify all output before use.

3.2   Access to Premises and Systems. Customer shall make available reasonable access to and use of Customer's premises, computer hardware, peripherals, Software and other software as Hyland deems necessary to diagnose and correct any Errors or to otherwise provide Maintenance and Support Services. Such right of access and use shall be provided at no cost or charge to Hyland.

4.   MAINTENANCE PERIODS; RENEWAL AND NON-RENEWAL; REINSTATEMENT; FEES.

4.1   Generally. The first period of this Maintenance Schedule shall be the Initial Maintenance Period. This Maintenance Schedule may be renewed for any additional periods only by mutual agreement of the parties on an annual basis. With respect to any renewal maintenance period, mutual agreement may be evidenced by Hyland's invoicing of annual maintenance fees for such renewal maintenance period and Customer's timely payment of such annual maintenance fees. Notwithstanding anything to the contrary, the term of this Maintenance Schedule shall immediately terminate at the time the version of the Supported Software licensed by Customer and in use in its production environment becomes Retired Software.

4.2   Reinstatement. In the event of the termination of Maintenance and Support under this Maintenance Schedule either by Customer's decision not to renew or by the Supported Software becoming Retired Software, Customer may during the term of this Agreement after the effective date of such termination elect to reinstate the term of this Maintenance Schedule in accordance with this paragraph. To obtain reinstatement, Customer shall: (a) deliver written notice to such effect to Hyland; (b) pay to Hyland (1) annual maintenance fees for all maintenance periods which would have elapsed from the effective date of such termination through the effective date of such reinstatement; and (2) an amount equal to one hundred percent (100%) of the annual maintenance fees for the renewal period of such Maintenance Schedule commencing on the effective date of such reinstatement; and (c) if the Supported Software has become Retired Software, upgrade to the latest released version of the Software which is Supported Software. Any reinstatement under this paragraph shall be effective as of the first business day after Hyland has received the notice of reinstatement and all payments required to be made hereunder in connection with such reinstatement. The renewal maintenance period commencing with the effective date of such reinstatement shall be for a period ending on the first annual anniversary of such effective date; and thereafter this Maintenance Schedule shall be renewed for an additional maintenance period as described in paragraph 4.1 above. Any reinstatement specified in this paragraph 4.2 is subject to governmental approval, including but not limited to Governor and Executive Council approval.

4.3   Initial Maintenance Period. On or after the Effective Date, Hyland shall invoice Customer for the annual maintenance fees for the Initial Maintenance Period. Customer shall pay such invoice in full on or before the commencement of the Initial Maintenance Period.

4.4   First Maintenance Period for Add-on Software. The first maintenance period related to Supported Software modules for which Customer purchases licenses under a Software License Schedule after the Effective Date of such Software License Schedule shall begin upon Delivery of such additional Software. Annual maintenance fees for the first maintenance period applicable to such Software shall be determined at Hyland's retail list prices in effect at the time Customer submits its applicable purchase orders, or at such other prices as the parties may mutually agree upon. Hyland shall invoice Customer for the annual maintenance fees for the first maintenance period applicable to such Software promptly upon Hyland's acceptance of Customer's purchase order for the purchase of Maintenance and Support for such Software. Customer shall pay such invoices in full in accordance with the General Terms.

4.5   Subsequent Maintenance Periods. Customer shall pay annual maintenance fees for all renewal maintenance periods after the first maintenance period applicable to a particular Supported Software module. Hyland shall invoice Customer for the annual maintenance fees for each renewal maintenance period at least forty-five (45) days prior to the end of the then-current maintenance period. Customer shall pay each undisputed invoice in full on or prior to the first day of the renewal maintenance period to which such invoice relates.

5.   TERMINATION.

5.1   By Customer. Customer may elect not to renew Maintenance and Support under this Schedule as described in Section 4.1 of this Schedule.

5.2   Termination for Breach. In the event that Customer terminates this Schedule or the entire Agreement under Section 1.2.2 of the General Terms, then Customer shall be entitled to a pro rata refund of annual maintenance fees that Customer has actually paid for the remainder of the maintenance period which terminates as a result of such termination (the "unused portion of annual maintenance fees").

Contractor Initials _7½L_
Date _03/13/2020_

EXHIBIT F

HOSTING SCHEDULE

All capitalized terms not defined in this Schedule shall have the meaning ascribed them in the General Terms.

1. HOSTING SERVICES

1.1   Hosting. Hyland will host the Hosted Solution, including providing to Customer the Standard Hosting Services and any Optional Hosting Services which are part of the Hosted Solution, subject to and in accordance with the terms of the Process Manual and Service Class Manual. The initial Service Class purchased by Customer is set forth in the Initial Purchase Table Schedule. Customer 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 this Hosting Schedule. In the event Customer elects to downgrade such Service Class, such downgrade will not be effective until the beginning of the next renewal of this Hosting Schedule. To modify a Service Class selection, Customer must submit a purchase order indicating the new Service Class.

1.2   Process Manual. Prior to or on the Effective Date, Hyland has delivered a then-current copy of the Process Manual to Customer. After the Effective Date, Hyland will have the right to modify the Process Manual (including the right to issue an entirely restated Process Manual) from time to time. The modifications or the revised Process Manual will be effective thirty (30) days after Hyland provides written notice to Customer informing Customer of Hyland's posting of such modifications or revisions on the website identified in such notice. If the changes to the Process Manual materially adversely affect the services provided to Customer under the Process Manual, Customer may terminate this Agreement by written notice delivered to Hyland within 30 days of Customer's receipt of such notice from Hyland. Such termination shall be effective thirty (30) days after Hyland's receipt of Customer's written notice.

1.3   Service Class Manual. Prior to or on the Effective Date, Hyland has delivered a then-current copy of the Service Class Manual to Customer. After the Effective Date, Hyland will have 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 will be effective thirty (30) days after Hyland provides written notice to Customer informing Customer 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 Customer's then-current Service Class will be effective until the next renewal of this Hosting Schedule.

1.4   Return of Customer Data and Deletion. Upon termination or expiration of this Hosting Schedule for any reason:

    (a)   Upon written request by Customer to Hyland sent to hylandcontracts@hyland.com made within thirty (30) days after the effective date of any such termination or expiration for the return of Customer Data ("Notice of Return of Customer Data"), Hyland will either: (1) return Customer Data to Customer by providing to Customer the 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 Customer the Customer Data for extraction via SFTP. Hyland will work with Customer on determining the extraction method most suitable to meet Customer's requirements. Customer shall be invoiced an amount determined by Hyland based on Hyland's then current list price as consideration for such return of Customer Data, or such other amount as mutually agreed upon by the parties. Customer acknowledges and agrees that thirty (30) days after Hyland has sent or made available to Customer 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 backup copies.

    (b)   Upon written request by Customer to Hyland sent to hylandcontracts@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 backup copies.

    (c)   If Customer 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, Customer acknowledges and agrees that thirty (30) days after any termination or expiration of this 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 backup copies.

1.5   Data Location. Hyland shall initially store Customer Data at the data center location identified in the Initial Purchase Table Schedule. Hyland may, at its expense, change the location of the Customer Data to another data center; provided that Hyland provides at least sixty (60) days prior written notice to Customer, informing Customer of the new location to be used for storing the Customer Data. If Customer objects to the new location proposed by Hyland, Customer may terminate this Hosting Schedule by providing written notice to Hyland within thirty (30) days of the date of Hyland's notice to Customer regarding the change of location. Such termination shall be effective thirty (30) days after such written notice. Notwithstanding anything to the contrary, the Data Location shall be located within the United States of America.

1.6   Customer Relocation of Software. During the term of this Hosting Schedule and upon termination or expiration of this Hosting Schedule, Customer will have the right to relocate the Software to servers owned or used by Customer at a facility operated by Customer.

Contractor Initials _NBL_
Date _03/13/2020_

1.7   Security. During the term of this Hosting Schedule, Hyland shall maintain a security program which shall conform to the Security Attachment, attached hereto as Attachment B. In the event that any terms in the Security Attachment conflict with any terms in the Process Manual, the Security Attachment shall control.

2.   **HOSTED SOLUTION SUPPORT.** In addition to the Maintenance and Support services that Hyland may provide in accordance with the terms of a Maintenance Schedule or Software License and Maintenance Schedule - Subscription, Hyland also agrees to provide maintenance and technical support for the Hosted Solution as described below.

2.1   Technical Support. Hyland will provide telephone or online technical support related to problems reported by Customer and related to the operation of the Network, the Third Party Software or the Host Web Site.

2.2   Network, Third Party Software or Host Site Defects. With respect to any defects (non-conformity to manufacturer's provided user documentation) in the Network, Third Party Software or Host Web Site which are properly reported by Customer and which are confirmed by Hyland or its suppliers, in the exercise of their reasonable judgment, Hyland shall use reasonable efforts to repair the defective component so as to correct the defect, or replace the defective component with a replacement component providing substantially similar functionality. Hyland shall undertake to confirm any reported defects in the Network, Third Party Software or Host Web Site promptly after receipt of proper notice from Customer, in accordance with Hyland's then-current Error reporting procedures.

2.3   Exclusions. Hyland is not responsible for providing, or obligated to provide, Hosted Solution Support under this Agreement:

        (a)   in connection with any Errors, defects or problems that result in whole or in part from any alteration, revision, change, enhancement or modification of any nature of any Third Party Software, any components of the Network or the Host Web Site, or from any error or defect in any configuration of any component of the Hosted Solution, which activities in any such case were undertaken by any party other than Hyland;

        (b)   in connection with any Error in the Software or defect or problem in any other component of the Hosted Solution if Hyland has previously provided corrections for such Error or defect which Customer fails to implement;

        (c)   in connection with any Errors, defects or problems which have been caused by errors, defects, problems, alterations, revisions, changes, enhancements or modifications in any software, hardware or system or networking which is not a part of the Hosted Solution;

        (d)   if the Hosted Solution has been subjected to abuse, misuse, improper handling, accident or neglect; or

        (e)   if any party other than Hyland, or an authorized subcontractor specifically selected by Hyland, has provided any services in the nature of Hosted Solution Support to Customer with respect to the Hosted Solution.

2.4   Update, Upgrade, Change or Replacement of Components of the Hosted Solution. Hyland may update or upgrade the build or version of the Software used in the Hosted Solution from time to time at Hyland's expense. Hyland also may change, replace, update or upgrade the hardware or other software components of the Hosted Solution from time to time. Customer agrees to collaborate with Hyland and assist Hyland in connection with the completion of installation and testing of any update or upgrade of the Software.

3.   **LICENSE OF THIRD PARTY SOFTWARE.**

3.1   Limited License. Hyland grants to Customer a revocable, non-exclusive, non-assignable, limited license to use the Third Party Software, in machine-readable object code form only, for the term of this Hosting Schedule. Customer may use the Third Party Software only as part of the Hosted Solution, solely for use by Customer internally, and only for capturing, storing, processing and accessing Customer's own data. The Third Party Software is licensed for use by a single organization and may not be used for processing of third-party data as a service bureau, application service provider or otherwise. Customer shall not make any use of the Third Party Software in any manner not expressly permitted by this Hosting Schedule.

3.2   Access to Customer Data. Customer acknowledges that the licenses granted herein are limited to the right of concurrent access to the Customer Data via telecommunications equipment by web browser or Software application to the Host Web Site.

3.3   Environments. Customer shall be entitled to use one (1) production copy of the Third Party Software. Further, Customer may purchase limited access to a User Testing Environment or User Testing Lite Environment, or both. HYLAND AND ITS SUPPLIERS MAKE NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE USER TESTING ENVIRONMENT, USER TESTING LITE ENVIRONMENT OR THE SOFTWARE, THIRD PARTY SOFTWARE, OR WORK PRODUCTS PROVIDED THEREIN AND THEY ARE PROVIDED "AS IS." Notwithstanding the foregoing Hyland agrees that the security measures described in the Process Manual section entitled "Security" are also applied to the User Testing Environment and User Testing Lite Environment. Hyland reserves the right to further define the permitted use(s) and/or restrict the use(s) of the User Testing Environment and User Testing Lite Environment. If, at any time, Customer is not satisfied with the User Testing Environment or User Testing Lite Environment, Customer's sole and exclusive remedy shall be to stop using the User Testing Environment or User Testing Lite Environment. Customer shall not make or use any additional copies of the Third Party Software.

4.   **PRICES, INVOICING AND PAYMENT.**

Contractor Initials _NBK_
Date _03/13/2020_

4.1 Initial Setup Fees. Hyland will invoice Customer for Initial Setup Fees in the amount set forth in the Pricing and Payment Schedule as specified in Exhibit C promptly following the Effective Date. Hyland will invoice Customer for Initial Setup Fees upon each additional purchase of Software under the Agreement upon acceptance of Customer's purchase order for such Software. Each such invoice shall be due and payable in accordance with the General Terms.

4.2 Hosting Fees. Customer shall pay Hosting Fees to Hyland for the Hosted Solution licensed hereunder in such amounts as specified in Exhibit C; provided, that during the Initial Term, Customer shall pay Hosting Fees to Hyland for the Hosted Solution as initially composed in accordance with the Initial Purchase Table Schedule. Hyland will invoice Customer on or after the Effective Date for Hosting Fees for the first year of the Initial Term. Such invoice shall be due and payable by Customer to Hyland in accordance with the General Terms. For any subsequent years, Hyland will invoice Customer for Hosting Fees at least sixty (60) days prior to the end of such year, and such invoices shall be due and payable by Customer to Hyland on or before the beginning of the next year. In the event Customer licenses additional Software modules under the applicable Schedule, Hyland will invoice Customer for Hosting Fees for such additional Software modules on a prorated basis, upon Hyland's acceptance of the purchase order for such additional Software modules. Such invoice shall be due and payable by Customer to Hyland in accordance with the General Terms. Thereafter, Hosting Fees relating to such additional Software shall be included in the subsequent invoices issued with respect to the existing licensed Software.

4.3 Consumption Fees. Hyland will invoice Customer for any Consumption Fees, monthly in arrears, promptly upon the end of the month to which such Consumption Fees relate. Consumption Fees will be due for a month if at any time during such month the amount of Customer Data stored in the Hosted Solution exceeds Customer's then-current data storage allocation.

4.4 Other Fees. If Customer procures and Hyland provides any other services or deliverables in connection with the Hosted Solution that are not covered by the fees and charges described in Sections 4.1 through 4.3 above, Hyland will invoice Customer for such other fees or charges based upon the pricing that the parties have mutually agreed upon in connection with such other services or deliverables

5. OWNERSHIP OF HOSTED SOLUTION COMPONENTS. Hyland and its suppliers own the Third Party Software, any and all computer hardware and telecommunications or other equipment and computer software, including the Host Web Site and the Network, and including, without limitation, any and all worldwide copyrights, patents, trade secrets, trademarks and proprietary and confidential information rights in or associated with the components of the Hosted Solution. The Third Party Software and other software components of the Hosted Solution are protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. No ownership rights in the Third Party Software, Host Web Site, Network or other hardware or software components of the Hosted Solution are transferred to Customer. Customer agrees that nothing in this Hosting Schedule or associated documents gives it any right, title or interest in or to any of the foregoing, except for the limited express rights granted in this Hosting Schedule. THIS HOSTING SCHEDULE IS NOT A WORK-FOR-HIRE AGREEMENT. At no time will Customer file or obtain any lien or security interest in or on any components of the Hosted Solution.

6. CERTAIN RESPONSIBILITIES AND OBLIGATIONS OF CUSTOMER.

6.1 Customer Responsibilities. In connection with the relationship established between Customer and Hyland under this Hosting Schedule:

(a) except as otherwise expressly permitted under the terms of this Hosting Schedule, Customer will not permit or authorize any person, legal entity, or other third party to use the Hosted Solution; and

(b) Customer 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 Attachment A.

6.2 Export. Regardless of any disclosure made by Customer to Hyland of an ultimate destination of any components of the Hosted Solution, or related documentation, Customer agrees not to export either directly or indirectly any of the foregoing without first obtaining a license from the United States Government to export or re-export such components or related documentation, as may be required, and to comply with United States Government export regulations, as applicable. Customer agrees that it will not export or re-export any components of the Hosted Solution or related documentation to a country that is subject to a U.S. embargo (such embargoed countries include, but are not limited to, Cuba, Iran, Iraq, North Korea, Burma (Myanmar), Sudan and Syria) under the U.S. Department of Commerce Export Administration Regulations and U.S. Department of State International Traffic in Arms Regulations. Customer will not export or re-export any components of the Hosted Solution (or any related documentation) to any prohibited person or entity in violation of U.S. export laws as described above (for more information visit: http://www.bis.doc.gov/complianceandenforcement/liststocheck.htm). Customer shall not use the Hosted Solution (or any related documentation) for any prohibited end uses under applicable United States laws and regulations, including but not limited to, any application related to, or purposes associated with, nuclear, chemical or biological warfare, missile technology (including unmanned air vehicles), military application or any other use prohibited or restricted under the U.S. Export Administration Regulations (EAR) or any other relevant laws, rules or regulations of the United States of America.

6.3 No High Risk Use. The "No High Risk Use" prohibition provided in the Software License Schedule - Perpetual or Software License and Maintenance Schedule – Subscription shall apply to the Hosted Solution.

6.4 Customer Internet Connection. Customer 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 Customer to properly access and use the Hosted Solution. Hyland shall have no responsibility or liability under this Hosting Schedule for any

Contractor Initials _NBR_
Date _03/13/2020_

unavailability or failure of, or nonconformity or defect in, the Hosted Solution that is caused by or related in any manner to any failure of Customer to obtain and maintain all such software, hardware, equipment and relationships.

7.   CERTAIN EFFECTS OF TERMINATION.

7.1   Termination. If, in the reasonable opinion of Customer or Hyland, the compliance by either party with the terms of this Hosting Schedule will be in violation of any law or regulation implemented or modified after the commencement of Hosting Services provided pursuant to this Hosting Schedule, Customer or Hyland, as the case may be, may terminate this Hosting Schedule upon thirty (30) days written notice to the other party.

7.2   Certain Effects of Termination. Immediately upon any termination or expiration of this Schedule, Customer shall cease any and all uses of the Hosted Solution. Hyland shall refund the unused portion of annual Hosting fees.

8.   COMPLIANCE WITH LAWS AND INDEMNIFICATION.

8.1   Compliance with Laws. Subject to Section 7 above, Hyland agrees to comply in all respects with all applicable laws in performing services under this Agreement.

8.2   Indemnification. This Section 8.2 supersedes any indemnification provision provided in a Software License Schedule or Software License and Maintenance Schedule - Subscription. Hyland agrees to indemnify Customer against all liability and expense, including reasonable attorneys' fees, arising from or in connection with any third party claim, action or proceeding instituted against Customer based upon any infringement or misappropriation by the Hosted Solution, Software and/or Work Products of any patent, registered copyright or registered trademark of a third party, provided that Hyland: (a) is notified promptly after Customer receives notice of such claim; (b) is in charge of the defense of and any settlement negotiations with respect to such claim, provided, that Hyland will not settle any such claim without the prior written consent of Customer if such settlement contains a stipulation to or admission or acknowledgement of any liability or wrongdoing on the part of or otherwise requires payment by Customer; (c) receives Customer's reasonable cooperation in the defense or settlement of such claim; and (d) has the right, upon either the occurrence of or the likelihood of the occurrence of a finding of infringement or misappropriation, either to procure for Customer the right to continue use of the Hosted Solution, Software and/or Work Products, or to replace the relevant portions of the Hosted Solution, Software and/or Work Products with other equivalent, non-infringing portions. If Hyland is unable to accomplish either of the options set forth in the preceding sentence, Hyland shall terminate this Agreement upon thirty (30) days advance written notice to Customer and refund to Customer any Hosting Fees and Subscriptions Fees paid. Notwithstanding anything to the contrary, Hyland shall have no obligation to Customer to defend or satisfy any claims made against Customer to the extent that such claims arise from: (w) any Customer Data; (x) use of the Hosted Solution other than as expressly permitted by this Agreement (except as provided in Exhibit A and paragraph 8.1 of Exhibit F above); (y) the combination of the Hosted Solution or any component thereof with any product not furnished by Hyland or expressly approved by Hyland; or (z) the modification or addition of any component of the Hosted Solution, other than by Hyland or any of its authorized resellers specifically retained by Hyland to provide such modification or addition. THIS SECTION 8.2 STATES HYLAND'S ENTIRE LIABILITY AND THE SOLE AND EXCLUSIVE REMEDY OF CUSTOMER WITH RESPECT TO ANY ALLEGED INFRINGEMENT OR MISAPPROPRIATION OF INTELLECTUAL PROPERTY BY THE HOSTED SOLUTION OR ANY COMPONENT THEREOF.

9.   CUSTOMER LIMITED WARRANTY.

Limited Warranty. Customer represents and warrants to Hyland that: (a) Customer is the legal custodian of the Customer Data and it has the right and authority to use the Hosted Solution in connection with all Customer Data and other materials hereunder; (b) Customer will use reasonable efforts to ensure that any Customer Data submitted to Hyland via electronic media will be free of viruses; and (c) anyone submitting Customer Data to Hyland for use in connection with the Hosted Solution or Professional Services 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. Customer is responsible for all Customer Data that is submitted to Hyland for use in connection with the Hosted Solution or Professional Services.

Contractor Initials _7ll&R_
Date _03/13/2020_

ACCEPTABLE USE POLICY FOR HOSTING

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. ("Hyland") in connection with Hyland's hosting of one or more hosted solutions (collectively referred to herein as "Hosted Solutions"). This AUP is designed to protect the security, integrity, reliability and privacy of Hyland's network and the Hosted Solutions Hyland hosts for its hosting customers.

User's use of the Hosted Solution 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 Hosted Solution. Therefore, User must take all reasonable precautions to protect access and use of any Hosted Solution that it uses.

2.2   Restrictions on Use. User shall not use a Hosted Solution 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 Hosted Solution 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 Hosted Solutions 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.

Contractor Initials _NBR_
Date _03/13/2020_

3.	**ENFORCEMENT.** If a User violates this AUP, Hyland may, depending on the nature and severity of the violation, suspend the hosting of any Hosted Solution 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 Hosted Solutions; 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 hosting of Hosted Solutions 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 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 hosting of Hosted Solutions. 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 related to such Hosted Solutions.

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 Hosted Solution. By using a Hosted Solution, 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 Hosted Solution by User and any liability for any other third party's violation of this AUP or applicable law.

6.	**RESERVED.**

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.

Contractor Initials _____
Date _____

SECURITY ATTACHMENT

Introduction: Hyland's Global Cloud Services division ("GCS") maintains and manages a comprehensive written security program 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. Hyland's security 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 GCS, GCS critical access, and the Hosted Solution environment.
   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. This program will include policies and procedures aligning with industry best practices, including ISO 27001/27002.
   b. Such information security program shall include, as applicable: (i) adequate physical security of all premises in which Customer Data will be processed and/or stored; (ii) reasonable precautions taken with respect to Hyland personnel employment; and (iii) an appropriate network security program.
   c. These policies will be reviewed and updated by Hyland management annually.

III. **Organization of Information Security**
   a. Assigning security responsibilities to appropriate Hyland individuals or groups to facilitate protection of the Hosted Solution environment and associated assets.
   b. Establishing information security goals to be met.

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 Hosted Solutions and/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 is revoked in a timely manner and all 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 is encrypted and stored in a secure location subject to strict physical access controls.
   c. When a 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 hardware 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. Devices used in the administration of the Customer's Hosted Solution that have been decommissioned will be subjected to these or equally effective standards.

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 off-boarding 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 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"

Contractor Initials _LBL_
Date _03/13/2020_

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.

 c. Ensuring strict access controls are in place for Customer Data access by Hyland. Customer administrators control user access, user permissions, and data retention with respect to the Hosted Solution. In the event Customer elects to modify the use of or turn off any encryption functionality, Customer does so at its own risk. [.

VII. System Boundaries

 a. The systems that compose a functioning Hyland cloud platform for the Hosted Solutions are limited to shared components such as network devices, servers, and software that are physically installed and operating within Hyland's Internet-enabled network infrastructure. This system boundary also includes the network connectivity, power, physical security, and environmental services provided by the third-party provider that owns and operates the data centers in which this network infrastructure is collocated.

 b. Hyland is not responsible for any system components that are not within this system boundary, 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.

VIII. Encryption

 a. Customer maintains ownership of all Customer Data uploaded to their Hosted Solution through the full lifecycle period. Customer Data may be uploaded via SFTP, TLS/SSL, or through a Hyland services API over a TLS/SSL connection to the Hyland cloud platform. Hyland will configure TLS and/or SSL certificates.

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

 c. In the event Customer elects to modify the use of or turn off encryption, Customer does so at its own risk.

IX. Physical and Environment Security

 a. The hardware components associated with the Hyland cloud platform used for the Hosted Solution are physically located within data centers that align with TIA-942 Tier 3 or higher. These data centers are owned and operated by 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 services for the Hyland cloud platform used for the Hosted Solution.

 b. An N-tiered architecture is used to support presentation, application, processing, and data services. For enhanced security in the Hyland cloud platform, technologies such as firewalls, intrusion detection and prevention, and vulnerability management are used.

X. Operations Security

 a. Maintaining documented Hyland cloud operating procedures.

 b. Maintaining change management controls to ensure changes to Hosted Solution production systems made by Hyland are properly authorized and reviewed prior to implementation.

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

 d. Utilizing virus protection software programs and definitions, which are configured to meet common industry standards designed to protect the Customer Data and equipment located within the Hyland cloud from virus infections or similar malicious payloads.

 e. Implementing disaster recovery and business continuity procedures. These will include replication of Customer Data to a secondary data center in a geographically disparate location from the primary data center.

 f. Maintaining a system and security logging process to capture critical system logs. 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 servers deployed within the Hyland cloud used for the Hosted Solution.

 h. Ensuring servers, operating systems, and supporting software used in the Hyland cloud for Hosted Solutions 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 Hosted Solution, then Hyland will use reasonable efforts to implement compensating controls until a security patch is available that would not materially adversely affect the Hosted Solution.

 i. Conducting Network vulnerability scans on at least a quarterly basis and remediate all critical and high vulnerabilities identified in accordance with its patch management procedures.

 j. Conducting Network penetration tests at least annually.

XI. Communications Security

 a. Implementing Network security controls to protect information resources within the Hyland cloud. These shall include network based intrusion detection systems, network segregation through use of stateful-inspection firewalls and a semi-trusted zone, and restricting inbound and outbound traffic to only designated and predefined ports.

 b. Upon implementation and once annually thereafter, Customer may request Hyland limit access to Customer's Hosted Solution to a list of pre-defined IP addresses at no additional cost.

XII. Supplier Relationships

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

XIII. Security Incident

Contractor Initials _ABC_

Date _03/13/2020_

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 Hosted Solution 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 the Customer's Hosted Solution has been negatively impacted by a security or availability 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 Platform.

d. 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 in order to prevent further issues. Solution 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 Customers need 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 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.

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. 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. Attestations are completed on an annual schedule and as of the Effective Date of the Agreement utilize the SOC 2 standard. A copy of Hyland's most recent SOC 2 report is available to Customers upon written request.

c. Customer may conduct audits of Hyland's operations that participate in the ongoing delivery and support of the Hosted Solution 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, Hosted Solution configurations, invoices, or application logs, and (b) Customer agrees to Hyland fees (at Hyland's standard rates) for the Professional Services that are required or requested of Hyland in connection with such audit if such audit exceeds 40-hours of Professional Services rendered by Hyland. 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.

d. Customer may conduct penetration testing against the public URL used to access the Hosted Solution on an annual basis; provided Customer provides Hyland with written notice of its desire to conduct such testing and the following criteria are met: (a) Hyland and Customer 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 Customer's cost and expense and Customer 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 Customer to assist with such testing, must be cleared by Hyland and enter into a Non-Disclosure Agreement directly with Hyland. Customer 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 Customer's access to or use of the Hosted Solution. Customer is prohibited from distributing or publishing the results of such penetration testing to any third party without Hyland's prior written approval.

Page 32 of 32

Contractor Initials _MBL_
Date _03/13/2020_

Vendor Instructions
Vendor Response Column: Place a "Yes" if the current release of the software can fully support ALL the functionality described in the row, without special customization. A "Yes" can only be used if the delivery method is Standard (see delivery method instructions below). Otherwise, enter an "No"; A "No" can only be used with delivery method Future, Custom, or Not Available/Not Proposing (see delivery method instructions below).
Criticality Column: (M) Indicates a requirement that is "**Mandatory**". The State considers it to be of such great importance that it must be met in order for the proposal to be accepted. If the proposer believes that there is something about their proposal that either obviates the need for this requirement or makes it of less importance this must be explained within the comments. The State retains the right to accept a proposal if the need of the requirement is reduced or eliminated by another feature of the proposal. (P) Indicates a requirement which is "**Preferred**". This requirement is considered by the State to be of great usefullness but the lack of this feature is not considered serious enough to disqualify the proposal. (O) Indicates a requirement which is "**Optional**". This requirement is considered by the State to be one which usefull or potentially usefull but not a central feature of the Project.

Vendor Instructions
Delivery Method Column:
Complete the delivery method using a Standard, Future, Custom, or Not Available/Not Proposing (as defined below) that indicates how the requirement will be delivered.
Standard - Feature/Function is included in the proposed system and available in the current software release. Future - Feature/Function will be available in a future release. (Provide anticipated delivery date, version, and service release in the comment area.) Custom - Feature/Function can be provided with custom modifications. (Respondent must provide estimated hours and average billing rate or flat cost for the software modification in the comment area. These cost estimates should add up to the total cost for software modifications found in the cost summary table in Section X of the RFP). Not Available/Not Proposing - Feature/Function has not been proposed by the Vendor. (Provide brief description of why this functionality was not proposed.)
Comments Column:
For all Delivery Method responses vendors must provide a brief explanation of how the requirement will be met. Free form text can be entered into this column.

BUSINESS REQUIREMENTS					
State Requirements					**Vendor**
Req #	Requirement Description	Criticality	Vendor Response	Delivery Method	Comments
Protection and Access to Data & Content					
B1.1	Ability to use encryption to protect data and content.	M	Yes	Standard	A number of security modules are available to protect various forms of data at rest, in-use and in transit. Data Protections in OnBase: Data at Rest: The Encrypted Disk Groups module allows for all data stored in the OnBase file system to be encrypted using the AES-256 or AES-128 algorithm when it is not in use. The Encrypted Alphanumeric Keywords module allows for keyword values in the database to be encrypted using the AES-256 or AES-128 algorithm. Data in Transit: OnBase supports the use of Transport Layer Security (TLS) for all communications to the Application Server and/or Web Server. The algorithm used to protect the communication depends on the configuration of TLS. Data in Use: When configurable session timeouts are used, if a user leaves their workstation unattended, any data on the screen will not be able to be modified by an unauthorized party after a certain amount of time has passed without reauthenticating to the OnBase system. Additionally, with the Encrypted Alphanumeric Keywords module, keyword values may be masked. This prevents shoulder-surfing attacks by hiding sensitive data values (such as Social Security numbers) behind asterisks when they are on screen.
B1.2	Ability to manage access and privileges through multiple layers such as users, user groups, active directory, document classifications, document types, etc.	M	Yes	Standard	The security model used in the OnBase system provides for the segregation of data between users, as well as the ability to limit the product functionality available for each user. User Groups and Rights provides for the assignment or restriction of basic and advanced OnBase features. Privileges can be assigned in an extremely granular manner in OnBase. This includes securing applications, document types, folders, and features like the ability to edit. Users can also be given read-only rights to specific keyword types or the keyword values themselves can be hidden. Indexing Limits can also be assigned to a user group, in order to limit a user's ability to index documents with specific keyword values. OnBase also supports single-sign on integration with several leading technologies including Active Directory (AD) and Lightweight Directory Access Protocol (LDAP). Integration with Active Directory Federation Services (ADFS) or SAML is commonly used today.
B1.3	Ability to manage access within Active Workflow folders, Long-Term Storage Documents, Scan Queues, etc.	M	Yes	Standard	All OnBase system and security administration is managed and configured from the point-and-click, menu-driven OnBase Configuration client. This includes workflows, long-term storage, scan queues, etc.
Migration of Legacy Archived Library Documents					
B2.1	Migration of NHDOL's existing legacy electronic document management system's Archived Library documents.	M	Yes	Standard	As part of the proposed solution, ImageSoft will convert existing documents and data from the current system into OnBase. ImageSoft has done many document conversion projects involving a line of business applications, legacy ECM products, and external database solutions. Conversions like this are often done prior to an official system "go live" so that when users are officially "live" with OnBase, all back-file documents are readily available. This approach expedites user adoption of the new system and helps avoid users having to go to two places to find the documents during the early phases of a new implementation. The primary OnBase tool used for migration is the Document Import Processor (DIP). The Processor imports batches of third-party generated documents and indexes into the OnBase system. Support for scheduling and polling allows for hands-off operation. DIP also lends itself to performing large back-file conversions from legacy systems and can be used as a convenient tool used for system/platform conversions. DIP can also create electronic forms with metadata from a delimited file when documents do not already exist.
Migration of Legacy ImportWord Module					
B3.1	Migration of NHDOL's existing legacy ImportWord module.	M	Yes	Standard	The OnBase Document Import Processor tool is the recommend approach to migrate existing data and documents from 3rd party systems, such as the IBM ImportWord module. Please reference additional information in requirement B2.1
Logging					
B4.1	Logging of who and when made changes to a document	M	Yes	Standard	OnBase provides a single document audit log on every document in the system and is important for auditing and compliance initiatives. The log displays the log date, log time, user name, action (a brief description of the action that took place), and a detailed account of the action.

	BUSINESS REQUIEMENTS				
	State Requirements				**Vendor**
Req #	**Requirement Description**	**Criticality**	**Vendor Response**	**Delivery Method**	**Comments**
B4.2	Logging of who and when made changes to an Active Workflow Folder	M	Yes	Standard	The OnBase logs referenced in requirement B4.1 also applies to workflow related documents as well as specific workflow events, such as the entry date and time, the exit date and time and the user information that took action on the document in the workflow.
Scanning Functionality					
B5.1	Are Labor's two Fujitsu fi-5750c scanners compatible with the proposed solution.	P	Yes	Standard	OnBase is hardware independent and supports any TWAIN, ISIS, or Kofax™ compliant scanning device.
B5.2	Are Labor's two Fujitsu fi-6770a scanners compatible with the proposed solution.	P	Yes	Standard	OnBase is hardware independent and supports any TWAIN, ISIS, or Kofax™ compliant scanning device.
B5.3	Are Labor's two Fujitsu fi-5900c scanners compatible with the proposed solution.	P	Yes	Standard	OnBase is hardware independent and supports any TWAIN, ISIS, or Kofax™ compliant scanning device.
B5.4	Is Labor's Fujitsu fi-5950 scanner compatible with the proposed solution.	P	Yes	Standard	OnBase is hardware independent and supports any TWAIN, ISIS, or Kofax™ compliant scanning device.
B5.5	Is Labor's Fujitsu fi-7160 scanner compatible with the proposed solution.	P	Yes	Standard	OnBase is hardware independent and supports any TWAIN, ISIS, or Kofax™ compliant scanning device.
B5.6	Is Labor's ColorTrac SmartLF SC 36 scanner compatible with the proposed solution.	P	Yes	Standard	OnBase is hardware independent and supports any TWAIN, ISIS, or Kofax™ compliant scanning device. Additionally, devices that have the ability to output the scanned image to a network share or email, including Multifunction device, OnBase can monitor and ingests on a regular basis.
B5.7	Ability to scan a batch of 1-sheet single sided forms each creating an individual document targeted for indexing.	M	Yes	Standard	Scan formats can be configured to automatically create a single document for every document scanned into a particular scan queue targeted for indexing. This eliminates the need for a user to prep the batch by inserting a separator sheet in between every page, or electronically separate each page shall all documents be scanned in together for a single batch.
B5.8	Ability to scan a batch of 2-sheet single sided forms each creating an individual document targeted for indexing.	M	Yes	Standard	Scan formats can be configured to automatically create a two-page document scanned into a particular scan queue targeted for indexing This eliminates the need for a user to prep the batch by inserting separator sheets, or electronically separate within the system shall all documents be scanned in together for a single batch. Alternatively, the user does have options during the indexing process to electronically separate, append, merge, etc. shall the need arise.
B5.9	Ability to scan a batch of 1-sheet duplex sided forms each creating an individual document targeted for indexing.	M	Yes	Standard	Scan formats can be configured for simplex or duplex mode, imaging the front and back of document as a single document targeted for indexing.
B5.10	Ability scan a batch of random documents made up of simplex, duplex, single page and multipage sheets prepared for scanning with bar coded folder separators and document separators creating documents grouped together in folders targeted for indexing.	M	Yes	Standard	Scan formats can be configured for multiple mixed batches containing simplex, duplex, single page, or multiple pages with barcodes and separator sheets targeted for indexing.
B5.11	Ability for scanned documents to be tagged with a scanning batch number and document number allowing for tracking back to the hard copy.	M	Yes	Standard	Every batch of documents contains a unique batch number that is automatically generated by the system at the time of scanning. Once indexed, every document will have a unique identifier as well.
B5.12	Ability for scan operator to generate and print a scan batch cover sheet identifying batch number, scan date, batch class, scan station, document count, page count, indexing queue and scan operator for storage with hard copy scanned documents.	M	Yes	Standard	Printing from OnBase is a configurable privilege that can be enabled for Scan Operators to generate a batch coversheet via templates stored accessible within OnBase. The template or Unity Form can be configured to include the examples provided.
B5.13	Ability to automatically apply document names and document numbers to documents when scanning a batch of similar forms, such as a batch of First Reports of Injury.	M	Yes	Standard	Scan queues can automatically set all documents scanned into the queue to a default document type.
B5.14	Ability to automatically apply document names and document numbers based on bar codes or document identifiers located on the form.	P	Yes	Standard	Barcode recognition is native in OnBase at the time of scan that supports a variety of barcode types. The barcode recognition engine will automatically classify and index the values identified in the barcode.
Indexing Functionality					
B6.1	Ability to apply required indexing values per business process to documents prior to entry into the workflow.	M	Yes	Standard	Authorized users, such as an OnBase Systems Administrators, can require certain keyword values for each individual document type are required to be indexed prior to entry into the system and workflow; required keywords are denoted with a red asterisk. If the user tries to upload or submit a document and a required keyword field is not indexed, the user will receive a warning message that certain fields are required to be indexed before uploading.
B6.2	Ability for documents to enter this process from multiple sources, such as the scanning process, ImportWord module, network sweeps and from the workflow when re-indexing is applicable.	M	Yes	Standard	OnBase provides a global configuration option, which is enabled by default, for any document that is re-indexed will automatically be assigned to the respective workflow for processing, regardless of the entry point of the document (e.g. scanning, ImportWord module, network sweeps, ad-hoc upload, etc.)

	BUSINESS REQUIEMENTS				
	State Requirements				**Vendor**
Req #	**Requirement Description**	**Criticality**	**Vendor Response**	**Delivery Method**	**Comments**
86.3	Ability for documents to enter this process with multiple or no indexing values already applied. These values should remain open for the applying of alternative values when applicable.	P	Yes	Standard	OnBase supports the ability for documents to enter the system with multiple or no indexing values applied. It is recommended that if a document enters the system without any keywords, or keywords require subsequent indexing, the document is assigned to a Pending Workflow Queue. This provides the ability for the user to easily locate and identify the documents that require additional indexing
86.4	Ability to designate a business process workflow for the indexed document to be forwarded into:	M	Yes	Standard	Content enters OnBase by being imported via any of the methods supported by OnBase (e.g. scanned, sweep, file import, automated import processors, Outlook integration, etc.), or by being created directly within OnBase. Content imported or created directly within OnBase can be configured to automatically enter OnBase Workflow. In addition, content can be manually pushed into Workflow at any time by users having the appropriate privileges.
86.5	Ability to apply preset document names and their associated document number (code) for consistency in labeling documents.	M	Yes	Standard	The OnBase Configuration Client is entirely point-and-click configurable that allows authorized users to preset document names/types in the system and their associated document number (does) for consistency in labeling documents.
86.6	Ability to extract and apply indexing values from NHDOL's IBM DB2 database. NHDOL's IBM DB2 database stores and maintains most if not all required indexing values. This IBM database is not expected to be replaced by this project. The existing EDMS extracts indexing values from this IBM database through ODBC connections using select statements with where clauses containing key values provided by a user or other means.	M	Yes	Standard	OnBase encourages a single location of master data but also supports the need to index documents based on that data. This is accomplished by making connections to external data sources for indexing. This enables OnBase to make real-time calls to an external software application for indexing information. The duplication of data or manual data entry is not required.
86.7	Ability to classify documents to accommodate functions such as access permissions, document retention, document security classification, etc.	M	Yes	Standard	User groups can be created with access to specific rights and privileges controlled by authorized administrators. The groups accommodate functions, such as access permissions (e.g. read-only, index, modify, print, email), document retention, document security classification, etc. In general, OnBase permissions are applied in a role-based system. Administrators create groups, assign product rights and privileges to those groups, and then place users into those groups
86.8	Ability for side by side viewing of image and data entry of indexing values for user friendly verification of proper indexing.	M	Yes	Standard	OnBase does provide side by side viewing of images and data entry of indexing values in a user-friendly view with verification of proper indexing.
Active Workflow Folder Functionality					
87.1	Ability to associate documents based on one or more identical key indexing data values such as Case number or Elevator number. This association of documents should simulate the hard copy manila folder containing all documents associated for a given case file.	M	Yes	Standard	OnBase File Cabinets and Folders provide a familiar interface for grouping documents without changing their physical storage in the database or association with a document type. A folder can contain more than one document type, and documents can be accessed either from the folder or through other types of document retrieval. As documents enter the system through various entry points (e.g. scanning, ad-hoc uploads, migration, automated import processors, emails, etc.) identical keyword indexing values, such as a Case or Elevator Number, will automatically group documents associated with the common value for a given case file, simulating the same look and feel of a traditional hard-copy manila folder.
87.2	Ability for each workflow process to have a unique set of one or more key indexing data attributes for associating documents. Some examples being in the Worker Comp Coverage process the key indexing data attributes is the FEIN of the employer, in the Workers Comp Hearing process the key indexing data attribute is the case number and in the Elevator Inspection process the key indexing data attribute is the Elevator number.	M	Yes	Standard	OnBase point-and-click configuration allows system administrators to establish keywords and data sets that define valid values for index fields on documents. Every document in the system can contain their own set of keywords or share common keywords across multiple document types. For example Document Type 1: Workers Comp Coverages Keywords: FEIN of the Employer, Company Name, Employee Name, Date of Injury Document Type 2: Workers Comp Hearing Keywords: Case Number, Employee Name, Date of Injury - FEIN can also be assigned to the Workers Comp Hearing if desired Document Type 3: Elevator Inspections Keywords: Elevator Number, Inspected By, Inspected Date, Type of Inspection, Inspection Status (e.g. pending, pass, or

BUSINESS REQUIREMENTS					
State Requirements				Vendor	
Req #	Requirement Description	Criticality	Vendor Response	Delivery Method	Comments
87.3	Ability to differentiate between documents associated in an active Workflow Folder and historical documents having identical key indexing data values. An example is in the Elevator Inspection workflow process where the elevator number is a key indexing value. Elevators are inspected once a year and an active workflow folder is generated containing only the current year documents such as the inspection report, invoice, payment, certificate, etc. Documents from previous years' inspections should not be included in the current year workflow folder.	M	Yes	Standard	OnBase does provide the ability to configure the workflow process to only show inspections and related document types for the current year. Previous years inspections and related documentation are easily accessible in the repository, folders, etc. to reference if needed, however, previous years will not be assigned to active workflow folders.
87.4	Ability for active workflow folders to be forwarded to a queue designated for a particular action. An example being within the Elevator Inspection process after issuing a certificate invoice the workflow folder is forwarded to a queue pending receipt of payment.	M	Yes	Standard	OnBase Workflow enables users to route documents for task assignment, updates, decisions, or other functions from one queue to another. The OnBase Workflow module uses rules, tasks, and actions for the logic of routing each document through the business process.
87.5	Ability for new documents entering the system to automatically be associated with an active workflow folder containing identical key indexing data values. An example being when a payment is received within the Elevator Inspection process the payment image/document should become part of the current year active workflow folder of the elevator.	M	Yes	Standard	Documents imported or created directly within OnBase can be configured to automatically enter OnBase Workflow and assign to the desired queue or step in the process. The concept of a related document work folder is used in Workflow to display documents identified as related to the primary document. The related document window is easily viewed by the user within the Workflow Life Cycle and allows the user to identify the presence or absence of related documents.
87.6	Ability for actions to be triggered when a new document becomes associated with an active Workflow Folder. An example being when a payment is received within the Elevator Inspection process and the new payment image/document based on its indexing data values gets associated with the active workflow folder of the elevator. This new association triggers the active workflow folder to be automatically	M	Yes	Standard	OnBase Workflow provides for advanced logic within work processes, where the Workflow engine will interrogate the document, its values, or information stored in some other system and automatically route the document to the appropriate work queue.
87.7	Ability for automatic forwarding of workflow folders in special time pending queues to be triggered when the designated period has expired. An example being when no payment or other document is received within the Elevator Inspection process for an Elevator workflow folder sitting in a queue waiting for a certificate payment. The time period expiration triggers the active workflow folder to be automatically forwarded to the next step in the workflow.	M	Yes	Standard	Holding a document in a pending queue until additional supporting documentation is standard functionality of OnBase Workflow. Once the outstanding supporting documents are placed into OnBase, or when the designed period has expired, Workflow evaluates their criteria, and if the criteria equal the missing supporting documentation criteria then Workflow will automatically trigger an action to send the document to the next step in the process (queue).
87.8	Ability for a user to bypass the normal workflow process and forward a folder to any step within the process.	M	Yes	Standard	OnBase Workflow accommodates exceptions to the configured model by assigning specific users with rights to add or reroute stages of a process on an ad-hoc basis.
87.9	Ability to set validation rules within the workflow to assure procedures or policies is followed. An example being in the Elevator Inspection process a rule may be inserted to assure the certificate payment has been received prior to allowing the workflow folder to move into the Issue Certificate step.	M	Yes	Standard	OnBase Workflow uses rules, based on a documents' metadata (keyword values), together with user decisions (actions), or system logic (actions) to route work items between various sub-processes that comprise a complete business process. Rules and logic configured by an OnBase Administrator ensure that documents are routed in a standard, controlled and prompt manner.
87.10	Ability to manage access to process workflows through permissions. An example being a Coverage Unit resource might only have access into the Coverage workflows.	M	Yes	Standard	OnBase Workflow can assign work to the job position, employee group, or a specific role. If a user is not a member of a group that has permissions to a particular queue, such as a Coverage, the user will not be able to see or access the queue.
87.11	Ability for a local administrator to modify permissions that manage access to process workflows.	M	Yes	Standard	Authorized users can easily modify permissions that manage access to process workflows directly within the OnBase Configuration and/or Studio client. OnBase also integrates with Active Directory so user group administration can be managed directly within AD.
87.12	Ability to manage access to steps within a process workflow through permissions. An example being a Workflow Folder residing I the "Supervisor Review" step should only be accessible by a supervisor	M	Yes	Standard	OnBase Workflow can assign work to the job position, employee group, or a specific role. If a user is not a member of a group that has permissions to a particular queue, such as a Supervisor Review, the user will not be able to see or access the queue.
87.13	Ability for a local administrator to modify permissions that manage access to steps within a process workflow.	M	Yes	Standard	Authorized users can easily modify permissions that manage access to process workflows directly within the OnBase Configuration and/or Studio client. OnBase also integrates with Active Directory so user group administration can be managed directly within AD.

BUSINESS REQUIEMENTS

	State Requirements				Vendor	
Req #	Requirement Description	Criticality	Vendor Response	Delivery Method	Comments	

Req #	Requirement Description	Criticality	Vendor Response	Delivery Method	Comments
87.14	Ability to manage access at the document level within a workflow folder. An example being in a Workers Comp Hearing case when the hearing officer is not allowed to view specific documents within the case folder. Access or viewing of these documents by the hearing officer needs to be prevented.	M	Yes	Standard	OnBase Workflow respects the permissions and security settings at the user group level. If a user is a member of a group that has permissions to the Workers Comp Hearing queue but does not have access to view specific documents within the case folder, access or viewing of these documents will not be available to the hearing officer.
87.15	Ability for a local user to set access or viewing permissions on workflow folder documents. As an example support staff responsible for reviewing a case file prior to it going into a hearing might reclassify a document (or another technique) to prevent access by the hearing officer.	P	Yes	Standard	Users with reindex permissions have the ability to reclassify a document that is assigned to a workflow queue or related folder. Once reclassified and indexed the document will be removed from the current workflow and reassigned to a new workflow process if the new classified document is designed for a workflow process. If the new classified document is not designed for a workflow process, the document will remain in the OnBase repository for access and long-term storage.
87.16	Ability within random Workflow Folders for the user to be able to set the order of how the documents appear in the folder. As an example in the Wage & Hour Inspection process today they can manually set the sequence order of each document unrelated to any indexing data attribute.	P	Yes	Standard	Work items assigned to a workflow queue for review and processing have the ability to set configurable columns to sort by default ascending or descending order, set flags and priorities, use typeahead and grouping by column to further filter the results.
87.17	Ability for a single user to have access to multiple or more than one workflow process. As an example a manager may have access into the Workers Comp Claims process, plus the Workers Comp Coverage process and also the Workers Comp Hearing process.	M	Yes	Standard	OnBase Workflow can assign work to the job position, employee group, or a specific role. An employee's assignment to specific work can be based on their assignment to a specific user group, which in turn can be used to control access to specific Workflow work queues for the purpose of performing specific tasks. If a user is a member of multiple job positions, employee group, or multiple roles, the user can be granted appropriate access to multiple workflow processes.

Active Workflow Folder Notes

Req #	Requirement Description	Criticality	Vendor Response	Delivery Method	Comments
88.1	Ability to simulate the chronological notes currently being documented as Folder Notes in the current NHDOL EDMS system. In the current NHDOL EDMS system folder notes do not always exist but when present they are automatically displayed upon opening the Workflow Folder. These notes document the pertinent chronological events such as phone conversations or key instructions. These notes document the date, the DOL staff member, any external party and pertinent comments or instructions. Actual folder notes: • Originated from Youth Cert • 6/18/18 Prepared CP Ltr and Inv for signature. cag • 6/25/18-ER (Chris) called to schedule an Informal Conference for Thursday August 23rd @ 10:00 AM. ER was told to bring proof of compliance and photo ID.	M	Yes	Standard	A note is a visual reminder that can be attached to a document. The note can be "text-based," displaying user-generated text comments, or can be a graphic image or highlight with the comments, referred to as an "annotation." Other note formats include the document "staple," which indicates the presence of a reference list of documents, and the "redaction," which allows for a specific portion of the image to be visibly blocked from the display. The appearance and functionality of any of these note types can be configured with a variety of characteristics (e.g., color, icon, etc.) depending on the type. Notes can also be modified at any time.
88.2	Ability for when a Workflow Folder is opened it should be explicit whether Folder Notes exist.	P	Yes	Standard	Notes can be configured to display open by default so the text can be read when viewing the document or folder. Notes also appear as an icon that best illustrates the type of note, for instance, a telephone icon would indicate conversations by phone, a calendar would represent a scheduled appointment, etc.
88.3	Ability for Folder Notes to be retained as a document with appropriate indexing values in long term storage when Workflow Folder is closed and no longer active.	M	Yes	Standard	Notes are electronic sticky notes are virtually connected to the document or folder and can be retained as a permanent association to support long term storage. When a document or folder is closed, following the legal retention period, the content, including the note, will no longer be active.

Active Workflow Folder Search

Req #	Requirement Description	Criticality	Vendor Response	Delivery Method	Comments
89.1	Ability for users to have their own predefined Active Workflow Folder searches.	P	Yes	Standard	OnBase Custom Queries (i.e. saved searches) allow users to quickly access predefined and most frequently retrieved documents, including active workflow folders and work items.
89.2	Ability for users to perform ad hoc Active Workflow Folder searches.	M	Yes	Standard	Many OnBase items and layouts can be added ad-hoc by the user to their Personal Page as tiles. Tiles serve as easy access points to the files, items, and interfaces for the users choice. The Personal Page can be opened by clicking the Personal Page ribbon button from the OnBase Unity Client
89.3	Ability for searches to differentiate between Active Workflow Folders and documents in long term storage.	M	Yes	Standard	OnBase provides the ability for users to differentiate searches between work items that are active in a workflow process or non-active that reside in the OnBase repository for access and long-term storage. For example, a user can search for active cases within a predefined workflow process or closed cases.
89.4	Ability for editing of Active Workflow Folders and their associated documents from an Active Workflow Folder search.	P	Yes	Standard	Authorized users with permission to modify, edit, re-index, etc. have the ability to perform the appropriate task for work items that are active in the workflow as well as their associated documents related to the primary work item from an active workflow folder search.

BUSINESS REQUIREMENTS					
	State Requirements				Vendor
Req #	Requirement Description	Criticality	Vendor Response	Delivery Method	Comments
Document Search Functionality					
B10.1	Ability for users to have their own predefined document searches.	P	Yes	Standard	OnBase Custom Queries (i.e. saved searches) allow users to quickly access predefined and most frequently retrieved documents.
B10.2	Ability for users to perform ad hoc document searches.	M	Yes	Standard	Many OnBase items and layouts can be added ad-hoc by the user to their Personal Page as tiles. Tiles serve as easy access points to the files, items, and interfaces for the users choice. The Personal Page can be opened by clicking the Personal Page ribbon button from the OnBase Unity Client.
B10.3	Ability for editing of documents from a document search.	M	Yes	Standard	Authorized users with permission to modify, edit, re-index, etc. and can perform the appropriate task from a document search result list.
Network Folder Sweeping					
B11.1	Ability to scan specific NHDOL network folders with automated importation of documents found into designated long-term storage, workflows or indexing queues.	M	Yes	Standard	The OnBase Document Imaging module provides the ability to schedule a sweep of documents in a network directory as a batch, which is assigned to an indexing scan queue for further processing. Each Scan Queue will have a dedicated default import path to the network share. Sweeps can occur from any process that can output to a network share, such a fax server, Multi-Function Device (MFD) etc. Once the documents are classified and indexed the documents that belong to a workflow process will automatically transition accordingly, otherwise, the document will remain in the OnBase repository for long-term storage.
B11.2	Ability for NHDOL local admin to set up new and maintain existing Network Folder Sweeps.	P	Yes	Standard	Authorized users can set up a new scan queue designed to sweep a network directory as well as maintain existing network folder sweeps. The scan queue and the network sweep directories are easily configurable with point-and-click configuration options in the OnBase Configuration Client with over 200 options to choose from.
Document Editing Lock-Down					
B12.1	Ability to Lock-Down a document from further editing or modifications. For example when a civil penalty letter gets approval from management and is issued to the recipient any further modifications need to be prevented. The current NHDOL EDMS system accomplishes this by converting the MS Word document to tiff format which is triggered by either the DOL staff member manually clicking a TIF button or an indicator being programmatically set in the ImportWord module.	M	Yes	Standard	OnBase provides the ability for documents to be locked for editing or modifications once a predefined disposition is complete. A common method that many customers leverage this type of functionality is by revisions and versions, utilizing the OnBase Electronic Document Management Services (EDM Services) module. With EDM Services, users with the correct privileges can create and manage document revisions/versions. Whenever a document's content changes, the modified document can be saved as a revision. Previous revisions are retained, allowing users to view content in prior revisions and track document history. Versions comprise a series of revisions made to one document. To create a new version of a document, users with the correct permissions can stamp a document as a version. This marks that document complete (up to that point in time). Versioning a document can also provide a way of limiting which revisions of a document certain users can see; certain user groups may be configured to only see stamped versions of documents, ensuring that they see the correct content.
Document Access Controls					
B13.1	Ability to set permissions on who can export a document to email	M	Yes	Standard	Emailing a document outside of OnBase is a privilege that is applied to a user group. If a user is a member of a user group that has "external email" privilege enabled, the user will be able to email a document directly from OnBase by selecting the email icon from the client's ribbon bar, or right click on the document and select "send to external email." If a user is not a member of a user group that has external email" privilege enabled, the user will not have the option to email a document from OnBase.
B13.2	Ability to set read and/or write access privileges on documents. An example being when a hearing case goes into a hearing the hearing officer may be restricted from viewing some documents within the folder.	P	Yes	Standard	Read and/or write is a privilege that is applied to a user group. If a user is a member of a user group that has "Retrieve/View" privilege enabled, the user will only be able to retrieve and view documents that the user has access to. If a user doesn't have access to a document type, they will not be able to access, search by, or view the respective document type. Conversely, if a user is a member of a user group that has "Retrieve/View" and "Create" privileges enabled, the user will be able to retrieve, view, and save/create only the document types they have access to.

	BUSINESS REQUIEMENTS				
	State Requirements				**Vendor**
Req #	Requirement Description	Criticality	Vendor Response	Delivery Method	Comments
813.3	Ability to set read/write permissions on documents per staff providing just needed privileges.	P	Yes	Standard	OnBase can be configured to create a robust security model that allows access to data and functionality in OnBase at the granular user-account level. Users are also assigned to User Groups, which allows for the assignment or restriction of OnBase rights, privileges, and features at the group level, even as it maintains the accountability of distinct user accounts. OnBase is designed to allow an administrator to rapidly implement a custom security profile for each user and User Group in the enterprise to help implement the concept of least privilege. User accounts can be added, deleted, and modified with an intuitive point-and-click interface in the OnBase Configuration module. The product rights and privileges defined for each User Group are similarly managed in the OnBase Configuration module.
ImportWord Module Integration					
814.1	Ability to modify NHDOL's existing vb.net ImportWord module to allow for integration with the new solution.	P			ImageSoft resources are experienced in VB.net. The appropriate resource will need to examine the module to determine what changes, if any, are required to allow the integration with OnBase. Typically, customers with third-party applications that require integrations between two systems (i.e. VB.Net ImportWord and OnBase) work collectively to establish necessary integration protocols. If the NH DOL IT does not have a dedicated technical resource to support the VB.Net ImportWord module, ImageSoft will require further discussions to understand required scope of services.
Outlook Integration.					
815.1	Ability to integrate with Microsoft Outlook 2010 and Microsoft Outlook 2016. An example being to import an incoming email or an outgoing email with or without attachments into an active Workflow Folder or long term storage with indexing values. Another example being to export one or more documents from an active Workflow Folder or long term storage as an attachment to an email.	M	Yes	Standard	The OnBase Integration for Microsoft Outlook enables users to store email messages and attachments in the OnBase system through the familiar Outlook interface. Users also have access to retrieve documents directly from the OnBase repository, as well as attach documents from OnBase when composing an email. OnBase v18, which is the current version, supports Microsoft Outlook 2010 and 2016.
815.2	Ability to control who and what is exported into an email attachment.	M	Yes	Standard	The OnBase Outlook integration module provides user options during the installation process allow certain functions of the integration to be available or not appear by enabling or disabling the appropriate option. For example, the ability to allow a user to upload a document received from email to OnBase, and search documents from OnBase within the Outlook Integration can be enabled, whereas, the ability to attach a document from OnBase to email can be disabled.
Document Retention Functionality					
816.1	Ability to configure for automatic removal of documents based on document retention policies. For example a Boiler Inspector's license invoice may only need to be maintained in the system for 3 years. After three years these document should begin the process of being removed.	P	Yes	Standard	The OnBase Document Retention module allows for the automatic destruction and removal of qualified documents that have exceeded their retention period and have not been marked for exclusion. This process varies, depending on whether a static or dynamic retention plan is set for that document type. Static retention plans will automatically purge documents when the user-specified time interval has elapsed. The retention period can begin based on either the creation date of a document (date stored), the document date, or a date keyword that has been configured for the document type. To remove documents associated with a static retention type, system administrators must configure a single, purging Document Retention Processay. This may be the most effective
816.2	Ability for a NHDOL local admin to set up new and maintain existing Document Retention configurations.	P	Yes	Standard	Users with the correct privileges may modify retention plans at any time to reflect different processing options and evaluation criteria. When modifying the length of time for a retention plan, the new length of time is immediately applied to every record in the system. If a document has already been marked for purging, and an updated retention plan would extend the expiration date, that document can be reactivated and/or excluded from a purge process provided the retention period has not already passed.
Checklist Validation					
817.1	Ability to validate required documents present in a Workflow Folder prior to allowing the folder to progress further in the workflow. An example being within the Elevator Inspection process a Workflow Folder should not be allowed to progress to the "Issue Certificate" step until the Payment for the certificate is present in the folder.	P	Yes	Standard	OnBase Workflow provides for advanced logic within work processes, where the Workflow engine will interrogate the document, its values, or information stored in some other system and automatically route the document to the appropriate work queue. If information is missing as required by a defined business process, such as payment for the certificate, OnBase will prevent the ability for a user or an automated system task to progress an Elevator Inspection to the Issue Certificate step in the workflow process. Rules and actions can be configured to prompt the user that payment for the certificate is missing and is required before continuing to issue a certificate.

BUSINESS REQUIEMENTS					
State Requirements					Vendor
Req #	Requirement Description	Criticality	Vendor Response	Delivery Method	Comments
Mobile Device Remote Access					
B18.1	Ability to access and manipulate documents remotely via a secure internet connection the same as when onsite and on the Granite domain. An example being an Elevator Inspector being able to use their Apple iPad to access the previous year's inspection report while inspecting the elevator at an off-site location.	P	Yes	Standard	There are multiple options in which OnBase can provide access to external users. One of the main things to keep in mind when deciding which option would be the most appropriate in a given situation would be to consider the specific needs of the external users in question as well as how NH DOL envision these users interacting with content in OnBase. In regards to external access with mobile devices, OnBase provides interfaces for iPad, iPhone, Android, and Windows tablet devices. These interfaces are developed on the native OS for each device. This allows OnBase to take advantage of the device's native user experience and allows users to work with their device in a familiar way.
Redaction Capabilities					
B19.1	Ability for view redacted information based on permissions of the user.	P	Yes	Standard	Documents that are redacted can be saved as a revision or as a different document type so that they can be secured and accessed independently (i.e. internal copy vs public copy).
B19.2	Ability on an ad hoc basis to redact data elements on a form prior to transferring then to a third party or exporting them to an email attachment.	P	Yes	Standard	Ad-hoc redaction is available in OnBase to remove sensitive information from being viewable prior to making that document available to the third party or exporting to an email attachment. The end user would first select the redaction icon from the OnBase viewer toolbar. Next, the user would select an area on the document with their mouse pointer and highlight the area of the document to be redacted. As the redaction is created, an entirely new image document is produced in which the annotations or bitmap images are permanently affixed to the document. Redactions can be performed in black or white to the redacted area of the document. The original version of the document, without redactions, can be saved and security can be applied to limit access based on user rights. The redacted copy can be exported and sent to a third-party, granted the user has the ability to export or email a document from OnBase.
B19.3	Ability to automatically set fields for redaction when certain actions take place, such as exporting to an email attachment.	P	Yes	Standard	Automated Redaction uses optical character recognition (OCR) technology to automatically identify and redact private or sensitive information from documents. Automated Redaction has the ability to identify three separate types of data values for redaction: • OnBase Keywords: Keyword values associated with the specified Keyword Types are redacted. • Regular Expressions. Text matching the pattern specified by the regular expression is redacted. • Text Strings. Static text can be specified and redacted. Certain Document Types (i.e. documents that require automated redactions) could have system tasks associated with them. When a document belongs to a Document Type that is configured to use system tasks, system task, such as "Send to Automated Redaction" can be initiated on the document.
B19.4	Ability to undo or reverse a redaction. Is considered conditionally mandatory only if Redaction Capabilities are installed.	M	Yes	Standard	Users with appropriate permissions have the ability to view the original content of a redacted image. If a redaction is burned into the image with redaction and bitmaps, with EDM Services, users with the correct privileges can create and manage document revisions/versions. Whenever a document's content changes, the modified document can be saved as a revision. Previous revisions are retained, allowing users with appropriate permissions to view content in prior revisions and track document history.
Reporting					

BUSINESS REQUIEMENTS

	State Requirements			Vendor
Req #	Requirement Description	Criticality	Vendor Response	Delivery Method	Comments
820.1	NHDOL is seeking analytical reports for managers and department leaders.	P	Yes	Standard	OnBase provides a variety of analytical reports for managers and department leaders. Reporting options include standard options for advanced reporting solutions. Standard report options include configuration, exception, transaction and verification reports. OnBase also offers a Report Services module which gives organizations the ability to gain valuable information about system and business health. Report Services is an easily deployed application that includes over 140 pre-configured reports for evaluating a complete picture of OnBase and the repositories and processes it manages. ImageSoft or organizations can also create their own custom reports to meet their specific business reporting needs from standard reporting tools, such as Microsoft SQL Server Report Services (SSRS) or Crystal Reports. Newer features like the Reporting Dashboards module, allow users to create graphical views based on relevant information. Dashboards present data in a variety of graphical formats including charts, graphs, scorecards, maps and more. Interactive features then allow users to easily monitor performance and analyze trends in real-time.
820.2	Ability for managers and department heads to generate their own reports or manipulate existing ones.	P	Yes	Standard	Manager and department heads have the ability to generate their own reports by exporting to .csv file from document search results list, workflow inventory, etc. This reporting feature is out of the box and a great tool to create ad-hoc reports on their own. Additionally, Report Services and Reporting Dashboards provides managers and department heads the ability to generate their own reports or manipulate existing reports using a point-and-click designer, highlighting business data

Signatures

	State Requirements			Vendor
821.1	Ability to apply an electronic signature to a document.	P	Yes	Standard	ImageSoft's trademarked TrueSign™ (Integrated Electronic Signature) provides a tool for signing documents electronically that produces an image with an actual "wet looking" signature. TrueSign includes markup capabilities, allows users to apply anchors for easy one-click signing, and allows signing by proxy. TrueSign also supports electronic seals and stamps and the use of signature pad devices.
821.2	Ability to apply electronic signatures to a batch of documents based on the authenticated user. An example being NHDOL's Commissioner wishes to be able to review all items in his queue, reject those not meeting his approval and then apply in batch mode his signature to those remaining.	P	Yes	Standard.	TrueSign supports the ability to electronically apply a signature to all documents in a batch based on the authenticated user.

Document Text String Search

	State Requirements			Vendor
822.1	Ability for text string searches on documents within an Active Workflow Folder. An example being during a hearing when one of the parties references an item in a 250 page medical report and the hearing officer wishes to find and read the page referencing the item.	P	Yes	Standard	The OnBase client offers External Text Searching to search across multiple documents and identify the instances of a specific string of text in one or multiple documents. The search is done where the data is stored so that OnBase does not have to send all the raw data to the workstation to complete the search, saving time and limiting network traffic. Combining keyword and text searching narrows the results even further. Those "hits" can then become the basis of a cross-reference to another document or another text search. Additionally, the Full-Text Search module provides a simple, unified interface for retrieving textual information stored in OnBase documents. This module extends native OnBase search capabilities to both structured and unstructured data. Advanced searches can be performed based on keywords and phrases that exist within OnBase documents to quickly and easily locate relevant content. The advanced search functions include stem, exact (""), fuzzy, thesaurus, near, Soundex, wildcard (*, ?) and Boolean (and, not, or) operators to quickly and accurately locate specific documents.

Optical Character Recognition

	State Requirements			Vendor
823.1	Ability for automated indexing of documents imported from Network Folder Sweeps through optical character recognition (OCR).	P	Yes	Standard	Advanced Capture brings template-based document classification and OCR data extraction technology into OnBase. Predefined template forms and rules, combined with an accurate and reliable OCR engine, provide the means to automatically classify and index image documents from any source, which includes, but not limited to scanned paper, imported from network folder sweeps, email, fax, etc.
823.2	Ability for NHDOL local admin to toggle automated indexing using OCR on and off under Network Folder Sweeps.	P	Yes	Standard	Advance Capture and OCR recognition can be toggled on or off by authorized users, such as the NH DOL local administrators.

BUSINESS REQUIEMENTS					
	State Requirements			Vendor	
Req #	Requirement Description	Criticality	Vendor Response	Delivery Method	Comments
B23.3	Ability to OCR specified areas of an incoming document for key values.	P	Yes	Standard	Advance Capture is a template based OCR capture engine that automatically extracts keyword information from specific areas of a document. Automating document indexing can eliminate the bottleneck associated with manually indexing high volumes of structured business documents.
B23.4	Ability to formulate a confidence level on an OCR read and determine next workflow navigation path on it.	P	Yes	Standard	The OnBase Advance Capture module supports confidence level, also referred to as the "suspect level." By default, the Suspect Level threshold is set to 75 and the average score given to a processed field is 70. It is considered a best practice to set the Suspect Level to the default threshold of 75 to ensure that forms are correctly and consistently being matched to documents. After a zone is processed, the OCR engine gives the resulting value a score between 1 and 99, depending on how confident it is in the result that was returned. A score returned by the OCR engine higher than the Suspect Level threshold causes the value captured from that zone to be marked as suspect, requiring further action. All scores lower than the Suspect Level threshold indicate that the captured value is considered by the OCR engine to be acceptable.
B23.5	Ability to use key values obtained from OCR to execute SQL select statements in obtaining further indexing data from OOBC connections on NHDOL's IBM.	P	Yes	Standard	Advance Capture provides the ability to use the keyword values obtained from the OCR engine to execute a SQL select statement to obtain further indexing data from OOBC connections to the NH DOL IBM system. This functionality is referred to in OnBase as an External Autofill Keyword Set. The value can be applied by a user that then executes the SQL statement to the IBM system or applied automatically by the Advance Capture OCR engine.
Evoking EDMS from IBM Green Screen					
B24.1	Ability to evoke an Active Workflow Folder on a green screen from an application on the NHDOL IBM.	P	Yes	Standard	OnBase Application Enabler allows integrations between third-party business applications and content or processes in OnBase without any coding. Application Enabler works in the background, allowing users to access related content on demand without leaving the screen of their business applications. Application Enabler can integrate with virtually any line-of-business system, including Windows, text-based (e.g. IBM Green Screen), Java, WPF, Silverlight, HTML, and more. The Application Enabler's four-step configuration wizard is all that is needed to build integrations that retrieve the document, index documents, launch workflow, create electronic forms and much more. No custom coding or API integrations are required.
Fax Integration					
B25.1	Ability to accept incoming faxes into the solution.	P	Yes	Standard	OnBase has the ability to store faxes electronically. Faxes can be swept into OnBase from any network directory or can be imported automatically via Hyland Software's fax integrations. Once archived, faxes can be indexed, assigned to a document type, sent to a Workflow life cycle for continued routing, or sent to a scan queue for further processing, including OCR or document separation. OnBase also provides direct integrations for importing faxes directly from the fax server, which includes the integration for Open Text Fax Server RightFax Edition, Biscom FASCOM and Esker Fax. This integration provides automatic archiving of faxes into OnBase, rules-based configuration to assign document types and route faxes, and metadata mapping, which allows properties assigned to a fax document by the fax server to be used as keywords in OnBase.
B25.2	Ability split an incoming 5-page fax of 1-page injury reports into five separate documents.	P	Yes	Standard	Business process owners will find that faxed documents are archived into OnBase are immediately available, not only for access but for automating business processes through tools such as Workflow. Fax metadata, including the sending and received fax numbers can be used to automatically route the documents to specific business users or queues to split and/or verify the faxed documents for completeness before processing continues.
B25.3	Ability to fax out a document from the solution.	P	Yes	Standard	To fax out of OnBase, a separate fax server application, such RightFax Edition, is required. OnBase can be configured to launch the standard Windows print dialogue, where print-to-fax implementations allow for outbound faxing from any application. No fax integration is needed to provide this functionality.
Document Versioning Tracking					

		BUSINESS REQUIEMENTS			
	State Requirements				Vendor
Req #	Requirement Description	Criticality	Vendor Response	Delivery Method	Comments
B26.1	Ability to store and manage versions of documents as they are revised.	P	Yes	Standard	OnBase Electronic Document Management (EDM) Services controls and tracks the modification of documents stored in OnBase through revisions and versions. This ensures the integrity of the document, protecting it against the risk of overlapping changes from multiple editors. Revisions are copies of an original document where the content has been modified, but the same file format is maintained. With EDM Services, users can create and manage revisions. When a document's content changes, the modified document can be saved as a revision. Previous revisions are retained, allowing users to view prior revisions and track document history. OnBase also keeps checking on documents being used, to prevent more than one user from changing a document at the same time. Revisions of Word documents can be 'compared' so that users know exactly what has changed between copies.
B26.2	Ability to toggle versioning off and on.	P	Yes	Standard	Versioning is applied at the individual document type within the OnBase Configuration client and can be enabled or disabled as desired by authorized users.
B26.3	Ability to remove old versions based on conditions or steps in the workflow.	P	Yes	Standard	Old versions that are no longer needed can be removed during defined conditions or steps in a workflow process.

APPLICATION REQUIREMENTS				
State Requirements				**Vendor**
Req ID	Requirement Description	Criticality	Vendor Response	Delivery Method	Comments
GENERAL SPECIFICATIONS					
A1.1	Ability to access data using open standards access protocol (please specify supported versions in the comments field).	M	Yes	Standard	To ensure compatibility with current and future hardware and software standards, the OnBase solution has always embraced open standards and does not use an proprietary formatting or compression. OnBase is built on the Microsoft Platform leveraging industry standard languages and protocols like .NET, ODBC, SQL, XML, TCP/IP, and HTTPS.
A1.2	Data is available in commonly used format over which no entity has exclusive control, with the exception of National or International standards. Data is not subject to any copyright, patent, trademark or other trade secret regulation.	M	Yes	Standard	Data in OnBase is available in commonly used formats and does not utilize any proprietary data format that is subject to any copyright, patent, trademark or other trade secret regulation.
A1.3	Web-based compatible and in conformance with the following W3C standards: HTML5, CSS 2.1, XML 1.1	M	Yes	Standard	The OnBase Web Server is compatible and in conformance with the W3C standards, which includes HTML 5 specifications and components to provide rich functionality and a performance user interface in today's modern browsers, CSS and XML standards.
APPLICATION SECURITY					
A2.1	Verify the identity or authenticate all of the system client applications before allowing use of the system to prevent access to inappropriate or confidential data or services.	M	Yes	Standard	A standard OnBase installation provides support for the standard OnBase username and password authentication, NT/Active Directory authentication, and LDAP authentication. For solutions hosted in the Hyland Cloud, standard Active Directory is not supported. Active Directory Federated Services (ADFS) or SAML is required, which is more secure and is commonly used today. NT Authentication/Active Directory allows users to be logged into OnBase automatically, based upon the user's NT/Active Directory domain login. This is an effective method for controlling single authentication over a LAN. This capability is completely out-of-the-box functionality and requires no customization. Authorization determines what permissions and privileges an authenticated user has within the application or system. In OnBase, permissions and privileges allow the authenticated user to access different areas and functionality in the application, such as document retrieval, Workflow administration, and the ability to view and edit Keywords.
A2.2	Verify the identity and authenticate all of the system's human users before allowing them to use its capabilities to prevent access to inappropriate or confidential data or services.	M	Yes	Standard	Please see the response to requirement A2.1
A2.3	Enforce unique user names.	M	Yes	Standard	OnBase security does require unique user names. Additionally, OnBase integrates with Active Directory for on-premise solutions as well as ADFS and SAML for solutions hosted in the Hyland Cloud.
A2.4	Enforce complex passwords for Administrator Accounts in accordance with DoIT's statewide User Account and Password Policy	M	Yes	Standard	Offers two options (high and medium) for password strength developed by Hyland security experts, which alleviates the need for creating a complex policy from a non-security-trained administrator and provides solid security out-of-the-box. Administrators also have the ability to create their own custom password policies with controls for complexity, content quotas, rotation, change frequency and account lockout.
A2.5	Enforce the use of complex passwords for general users using capital letters, numbers and special characters in accordance with DoIT's statewide User Account and Password Policy.	M	Yes	Standard	Offers two options (high and medium) for password strength developed by Hyland security experts, which alleviates the need for creating a complex policy from a non-security-trained administrator and provides solid security out-of-the-box. Administrators also have the ability to create their own custom password policies with controls for complexity, content quotas, rotation, change frequency and account lockout.
A2.6	Encrypt passwords in transmission and at rest within the database.	M	Yes	Standard	Passwords in OnBase combined with a value unique for each user (a process known as "salting") and then hashed in the database using 30,000 iterations of the PBKDF2 cryptographic hash algorithm.

APPLICATION REQUIREMENTS				
State Requirements				**Vendor**
Req #	Requirement Description	Criticality	Vendor Response	Delivery Method	Vendor Comments
A2.7	Establish ability to expire passwords after a definite period of time in accordance with DoIT's statewide User Account and Password Policy	M	Yes	Standard	In order to ensure that users are rotating passwords in a secure manner, administrators can: • Require that a designated amount of hours pass between password changes • Designate the number of days before a password expires and will need to be changed • Require that a password expires on first use and must be changed
A2.8	Provide the ability to limit the number of people that can grant or change authorizations	M	Yes	Standard	OnBase Administration provides the ability to limit the number of people that can grant or change authorizations. The configuration of OnBase is accessible within the OnBase Configuration Client, only to authorized users that has the client installed. In addition, Granular Rights Management allows administrators to control access to every part of their environment down to an extremely granular level, preventing users, including administrators, from having more access than they should.
A2.9	Establish ability to enforce session timeouts during periods of inactivity.	M	Yes	Standard	Session timeouts can be configured at the user group level. Depending on the client used, the client will either simply end its HTTP session with the server after the allotted time has passed or will close the client entirely. With both methods, the license is released on timeout, and the user will have to re-authenticate and consume an available license to resume working within the system.
A2.10	The application shall not store authentication credentials or sensitive data in its code.	M	Yes	Standard	Passwords for authentication or sensitive data is never stored is stored in code.
A2.11	Log all attempted accesses that fail identification, authentication and authorization requirements.	M	Yes	Standard	Attempted access that fails identification is logged in the OnBase transaction log reports and is restricted to authorized users only. Error messages that disclose the reason for a login failure (i.e. the username is incorrect, the account is locked, the password is incorrect, etc.) make it easier for attackers to successfully login using stolen credentials. For this reason, the only error message that is displayed to a user following a failed login is "Login failed. Either the credentials were incorrect or the account is locked."
A2.12	The application shall log all activities to a central server to prevent parties to application transactions from denying that they have taken place.	M	Yes	Standard	OnBase audits all use of the system as well as any user access modification. The log reports are available in the OnBase system that is protected and available to only authorized users by allowing users with the appropriate rights to view transaction log reports. The list of items tracked is immense, but includes all access to the system by logging on or off, failed login attempts, opening documents, changing documents, changing any user account information, and more.
A2.13	All logs must be kept for one year.	M	Yes	Standard	Logs in OnBase are kept for the desired length of time and is only accessible for deletion by authorized users, such as a Systems Administrator.
A2.14	The application must allow a human user to explicitly terminate a session. No remnants of the prior session should then remain.	M	Yes	Standard	Administrators have the ability to manually lock accounts, which will prevent login. Accounts manually locked by an administrator must also be manually unlocked by an administrator. Additionally, administrators may simply delete accounts that are no longer needed.
A2.15	Do not use Software and System Services for anything other than they are designed for.	M	Yes	Standard	ImageSoft will comply
A2.16	The application Data shall be protected from unauthorized use when at rest	M	Yes	Standard	The Encrypted Disk Groups module allows for all data stored in the OnBase file system to be encrypted using the AES-256 or AES-128 algorithm when it is not in use. The Encrypted Alphanumeric Keywords module allows for keyword values in the database to be encrypted using the AES-256 or AES-128 algorithm.
A2.17	The application shall keep any sensitive Data or communications private from unauthorized individuals and programs.	M	Yes	Standard	The assignment of user rights, privileges, and User Group membership in OnBase should follow the principle of least privilege. Least privilege means that users have no more permissions, rights, or privileges than they require to complete their tasks in the system. For example, users who only use OnBase to retrieve and index documents should not be assigned any user administration privileges, just as users who are not authorized to view sensitive documents should not be given access to those documents.
A2.18	Subsequent application enhancements or upgrades shall not remove or degrade security requirements	M	Yes	Standard	Application enhancements and upgrades do not remove or degrade security requirements.

	APPLICATION REQUIREMENTS				
	State Requirements				Vendor
Req #	Requirement Description	Criticality	Vendor Response	Delivery Method	Comments
A2.19	Utilize change management documentation and procedures	M	Yes	Standard	ImageSoft follows change management documentation and procedures. Additionally, for OnBase solutions in the Hyland Cloud, Hyland follows internal change management procedures when changes are initiated by Hyland, or when a customer requests to make a change on their behalf to existing systems, or when new systems are deployed to the Hyland Cloud.
A2.20	Web Services : The service provider shall use Web services exclusively to interface with the State's data in near real time when possible.	M	Yes	Standard	The Unity API is an object-oriented programming model that communicates via a .NET Web Service that can be used to integrate with applications across the internet. Web Services is the preferred integration method to interface with the NH DOL state's data, and in most instances, can integrate in real-time.

					TESTING	
		State Requirements				**Vendor**
Req #		**Requirement Description**	**Criticality**	**Vendor Response**	**Delivery Method**	**Comments**
APPLICATION SECURITY TESTING						
T1.1		All components of the Software shall be reviewed and tested to ensure they protect the State's web site and its related Data assets.	M	Yes	Standard	As part of the implementation, ImageSoft will review and test the solution to ensure the NH DOL data is protected. Also, please reference the response to requirement H3.1 for further details on how data is protected in the Hyland Cloud.
T1.2		The Vendor shall be responsible for providing documentation of security testing, as appropriate. Tests shall focus on the technical, administrative and physical security controls that have been designed into the System architecture in order to provide the necessary confidentiality, integrity and availability.	M	Yes	Standard	The Hyland Cloud Services SOC 3 report is available without an NDA and is available upon request. The report is relevant to Security, Availability and Confidentiality. In addition, Hyland GCS completes network vulnerability scans on a weekly basis. A third party completes an annual penetration test against OnBase to assess security. A report is provided on their findings, and Hyland provides a documented response to the OnBase penetration test that details the resolution for each finding.
T1.3		Provide evidence that supports the fact that Identification and Authentication testing has been recently accomplished; supports obtaining information about those parties attempting to log onto a system or application for security purposes and the validation of users	M	Yes	Standard	As part of the SOC 3 Report conducted by a third-party security reviews, the results conclude that "We have examined management's assertion that Hyland's Software, Inc. maintained effective controls to provide reasonable assurance that: "the Hyland Cloud Platform was protected against unauthorized access, use, or modification to achieve Hyland's Software, Inc.'s commitments and system requirements."
T1.4		Test for Access Control; supports the management of permissions for logging onto a computer or network	M	Yes	Standard	As part of the implementation services, ImageSoft will review and test for access control, in combination with the NH DOL resources during the Users Acceptance Testing (UAT) process, to support that the appropriate access controls are in place.
T1.5		Test for encryption; supports the encoding of data for security purposes, and for the ability to access the data in a decrypted format from required tools.	M	Yes	Standard	As part of the implementation services, ImageSoft will review and test for encryption, in combination with the NH DOL resources during the Users Acceptance Testing (UAT) process, to support the encoding of data for security purposes, and for the ability to access the data in a decrypted format from the required tools.
T1.6		Test the Intrusion Detection; supports the detection of illegal entrance into a computer system	M	Yes	Standard	Because the Hyland Cloud provides network access, security, and monitoring services to its customers, each service is monitored and tested to assure performance and recoverability that does include Network Security Services (e.g., firewalls, data encryption, intrusion detection, anti-virus/anti-malware).
T1.7		Test the Verification feature; supports the confirmation of authority to enter a computer system, application or network	M	Yes	Standard	As part of the implementation services, ImageSoft will review and test the verification feature, in combination with the NH DOL resources during the Users Acceptance Testing (UAT) process, to support the confirmation of authority to enter a computer system, application, or network.
T1.8		Test the User Management feature; supports the administration of computer, application and network accounts within an organization.	M	Yes	Standard	As part of the implementation services, ImageSoft will review and test the user management feature, in combination with the NH DOL resources during the Users Acceptance Testing (UAT) process, to support the administration of computer, application and network accounts within the organization.

	TESTING				
	State Requirements				**Vendor**
Req #	**Requirement Description**	**Criticality**	**Vendor Response**	**Delivery Method**	**Comment**
T1.9	Test Role/Privilege Management; supports the granting of abilities to users or groups of users of a computer, application or network	M	Yes	Standard	As part of the implementation services, ImageSoft will review and test the test role and privilege management, in combination with the NH DOL resources during the Users Acceptance Testing (UAT) process, to support the granting of abilities to user or groups of users of a computer, application or network.
T1.10	Test Audit Trail Capture and Analysis; supports the identification and monitoring of activities within an application or system	M	Yes	Standard	As part of the implementation services, ImageSoft will review and test the audit trail capture and analysis, in combination with the NH DOL resources during the Users Acceptance Testing (UAT) process, to support the identification and monitoring of activates within the OnBase application or system.
T1.11	Test Input Validation; ensures the application is protected from buffer overflow, cross-site scripting, SQL injection, and unauthorized access of files and/or directories on the server.	M	Yes	Standard	Hyland Global Cloud Services monitors for and protects against common web application security vulnerabilities (e.g. SQL injection, XSS, XSRF, etc.), by utilizing many security controls, such as firewalls, IDS, and vulnerability management to ensure that customer data is secure. Additionally, Cloud Services uses a combination of enterprise and custom tools to monitor the Hyland Cloud platform. In addition to this, we contract with Accuvant Labs, Inc. to perform third-party penetration testing against the software as part of the finalization process for release.
T.1.12	For web applications, ensure the application has been tested and hardened to prevent critical application security flaws. (At a minimum, the application shall be tested against all flaws outlined in the Open Web Application Security Project (OWASP) Top Ten (http://www.owasp.org/index.php/OWASP_Top_Ten_Project))	M			The Hyland Internal R&D and Hyland Global Cloud Services (GCS) teams are well-versed in common vulnerabilities and exploits including those outlined in the OWASP Top 10. Utilizing secure development practices, automated security scanning, and manual penetration testing (internal and external), OnBase is continually tested against a wide range of attack vectors and hardened against them.
T1.13	Provide the State with validation of 3rd party security reviews performed on the application and system environment. The review may include a combination of vulnerability scanning, penetration testing, static analysis of the source code, and expert code review (please specify proposed methodology in the comments field).	M			The Hyland Cloud Services SOC 3 report is available without an NDA and is available upon request. The report is relevant to Security, Availability and Confidentiality. As part of the SOC 3 Report conducted by a third-party security reviews, the results conclude that "We have examined management's assertion that Hyland's Software, Inc. maintained effective controls to provide reasonable assurance that: • "the Hyland Cloud Platform was protected against unauthorized access, use, or modification to achieve Hyland's Software, Inc.'s commitments and system requirements." • "the Hyland Cloud Platform was available for operation and use to achieve Hyland's Software, Inc.'s commitments and system requirements." • "the Hyland Cloud Platform information is collected, used, disclosed and retained to achieve Hyland's Software, Inc.'s commitments and system requirements."
T1.14	Prior to the System being moved into production, the Vendor shall provide results of all security testing to the Department of Information Technology for review and acceptance.	M	Yes	Standard	As part of the implementation services, ImageSoft will provide the results of all security testing to the dedicated NH DOL project resource so that the information, in combination with the Users Acceptance Testing (UAT) results, to support that the NH DOL Department of Information Technology for review and acceptance.

				TESTING	
	State Requirements				**Vendor**
Req #	**Requirement Description**	**Criticality**	**Vendor Response**	**Delivery Method**	**Comments**
T1.15	Vendor shall provide documented procedure for migrating application modifications from the User Acceptance Test Environment to the Production Environment.	M	Yes	Standard	As part of the implementation services, ImageSoft will provided documented procedures for migrating application modifications from the User Acceptance Test Environment (UAT) to the Production Environment.
STANDARD TESTING					
T2.1	The Vendor must test the software and the system using an industry standard and State approved testing methodology as more fully described in Appendix G-2.	M	Yes	Standard	ImageSoft will comply
T2.2	The Vendor must perform application stress testing and tuning as more fully described in Appendix G-2.	M	Yes	Standard	ImageSoft will comply
T2.3	The Vendor must provide documented procedure for how to sync Production with a specific testing environment.	M	Yes	Standard	OnBase provides a tool to help with OnBase configuration change management – Test System Creation. This allows administrators to easily create copies of OnBase environments that are suitable for test and development purposes. A technical documented procedure is available in the Systems Administration Module Reference Guide (MRG) under the Change Management section. In addition, documented procedures are available on how to sync production with a test environment utilizing the Change Management import/export utility as well as traditional methods that include database backup and restore. For solutions hosted in the Hyland Cloud, test systems are available, however, the environment and synchronization is conducted by the Hyland Global Cloud Services team.
T2.4	The vendor must define and test disaster recovery procedures.	M	Yes	Standard	Hyland Global Cloud Services does have a defined DR plan and regularly tests its ability to recover the Hyland Cloud services. Customers who select the Hyland Cloud Platinum or Double Platinum class of service have the ability to request joint data center failover testing on an annual schedule. Additional information regarding the Hyland Cloud Disaster Recovery plan may be provided

Req. ID	State Requirements – Requirement Description	Criticality	Vendor Database Response	Delivery Method	Vendor – Comments
OPERATIONS:					
M1.1	Vendor shall provide an ANSI/TIA-942 Tier 3 Data Center or equivalent. A tier 3 data center requires 1) Multiple independent distribution paths serving the IT equipment, 2) All IT equipment must be dual-powered and fully compatible with the topology of a site's architecture and 3)Concurrently maintainable site infrastructure with expected availability of 99.982%	M	Yes	Standard	The data centers currently in use for the Hyland Cloud are TIA Tier 3 or 4 facilities. Hyland's hosting facilities are co-located data centers, with the data center providing all of the environmental safeguards such as air cooling, fire suppression, and power redundancy. However, Hyland owns and maintains all of the equipment supporting the hosted application of OnBase. Hyland Software offers multiple service classes for the Hyland Cloud that commit to uptime ranging from 99% to 99.9% uptime.
M1.2	Vendor shall maintain a secure hosting environment providing all necessary hardware, software, and Internet bandwidth to manage the application and support users with permission based logins.	M	Yes	Standard	Hyland Software owns and operates all of the equipment comprising the Hyland Cloud platform, and the Hyland Cloud architecture is both specialized and optimized for hosted Hyland products. Hyland determines the best configuration, and Hyland engineers manage the environment transparently to the Hyland Cloud customer. Specific hardware information is maintained as proprietary to Hyland. Hyland Global Cloud Services uses redundant, overlapping bandwidth monitoring applications to ensure accurate usage and quality measurements. Bandwidth is also provisioned on burstable connections to ensure temporary spikes in activity do not result in a degradation of service.
M1.3	The Data Center must be physically secured – restricted access to the site to personnel with controls such as biometric, badge, and others security solutions. Policies for granting access must be in place and followed. Access shall only be granted to those with a need to perform tasks in the Data Center.	M	Yes	Standard	The physical security measures at the data center are consistent with those of a TIA Tier 3 or 4, ISO 27001-certified data center. All Hyland Cloud data centers are staffed by security personnel and covered by surveillance cameras. Hyland limits physical access to pre-authorized staff and visitors, who are provided with access via multi-factor authentication that limits them to authorized areas only. • Hardware is physically separated from any other hosting provided in the data center. • Hardware is physically secured using separate cages and locking cabinets. • Man traps, air locks, multiple access doors and other security measures prevent unauthorized access. • Biometric controls and other cutting-edge technologies are utilized. • Access to hardware is via multi-factor authentication. • Network infrastructure components and services such as routing, switching and bandwidth are monitored 24/7. • Certified engineers are available to resolve any issues as per the customer's chosen service class. • Automated network intrusion monitoring procedures operate 24/7.
M1.4	Vendor shall install and update all server patches, updates, and other utilities within 60 days of release from the manufacturer.	M	No	Not Available/Not Proposing	Patches are applied within 90 days of release, but only after they have been tested in a non-production environment. Hyland Software evaluates each patch released for the Microsoft Windows operating system in order to ensure compatibility. Our partnership with Microsoft enhances Hyland's ability to identify and resolve compatibility issues more effectively. Hyland GCS makes every effort to have patches applied within 30 days following release.
M1.5	Vendor shall monitor System, security, and application logs.	M	Yes	Standard	The Hyland Cloud has numerous security controls and monitoring mechanisms in place, which includes firewalls at the Web and App server level, IDS, and vulnerability management. Logs are captured from these and other critical servers and network hosts and maintained in a centralized log repository. These logs are kept in non-repudiation format and kept for one year. Access to the central log repository is limited to a small team based on job role. Monitoring of these systems is active and alerts are configured to notify appropriate personnel within the department of potential security or availability incidents. Staff is available/on call 24/7 to respond to alerts
M1.6	Vendor shall manage the sharing of data resources.	M	Yes	Standard	The Hyland Cloud is a private, managed, multi-instance cloud. Each Hyland Cloud customer is provided its own instance of OnBase so each customer has its own database and disk groups. However, the hardware and some servers are shared for the individual Hyland Cloud customers. As a result, there is no co-mingling of data in the cloud. Customers are assigned a unique encryption key that effectively renders the documents unreadable outside of the customer's dedicated instance of OnBase.
M1.7	Vendor shall manage daily backups, off-site data storage, and restore operations.	M	Yes	Standard	The Hyland Cloud is N+1 redundant. End users are provided three copies of data. Two are stored in the primary data center on separate hardware, and a third copy is located in a different data center in a different geographic location. These copies are stored to online storage so there is no offline storage to be destroyed. Hard copy documents are not created. Data sanitization techniques are used to overwrite data on the servers in use for the Hyland Cloud

	State Requirements				Vendor		
Req #	Requirement Description	Criticality	Vendor Response	Proposed Method		Comments	
H1.8	The Vendor shall monitor physical hardware.	M	Yes	Standard	Because the Hyland Cloud provides network access, security, and monitoring services to its customers, each service, including hardware, is monitored and tested to assure performance and recoverability. This includes: • Data center availability and environment services (e.g., power, cooling, fire detection/suppression) • Network connectivity and support services (e.g., HTTPS, DNS, SFTP) • Network security services (e.g., firewalls, data encryption, intrusion detection, anti-virus/anti-malware) • OnBase processing services (e.g., document retrieval and business process workflow)		
H1.9	Remote access shall be customized to the State's business application. In instances where the State requires access to the application or server resources not in the DMZ, the Vendor shall provide remote desktop connection to the server through secure protocols such as a Virtual Private Network (VPN).	M	Yes	Standard	Customers who host their OnBase solution within the Hyland Cloud are not permitted to examine shared systems or connect directly to application servers over a VPN network. However, Hyland Cloud Services offers a Cloud Portal with access for the management of some of the components of the Hyland Cloud solution. Hyland Cloud customers are empowered to manage their solution as they see fit. As such, system administrators have access to their solutions via the Internet. As the Hyland Cloud is a hosted offering, the expectation is that end-user access is over 443. A VPN is a non-standard component with a Hyland Cloud offering. If there is a technical requirement for a VPN, it can be provisioned as a fee-based		
H1.10	The Vendor shall report any breach in security in conformance with State of NH RSA 359-C:20. Any person engaged in trade or commerce that is subject to RSA 358-A:3, I shall also notify the regulator which has primary regulatory authority over such trade or commerce. All other persons shall notify the New Hampshire attorney general's office.	M	Yes	Standard	The Hyland GCS Incident Response Plan is documented as a part of the GCS IS Policy Suite. Procedures are in place for the escalation and notification in the event of a qualified security incident. This information is documented in the Hyland Global Cloud Services Security Incident Management Policy. The Incident Response Plan mandates that all Security Incidents are to be investigated promptly and thoroughly by qualified team members. Every Security Incident is treated as a Security Breach until determined otherwise. Availability and privacy incidents follow a general incident response. Global Cloud Services will provide a Root Cause Analysis (RCA) report to customers impacted by a qualified Information Security Incident (i.e. Security, Availability, etc.). The RCA includes the duration of the event, business impact, resolution, technical summary*, outstanding issues, and any follow-up that may include steps customers' need to take in order to prevent further issues. This report sent to customers generally has enough details for customers to in turn communicate issues to their end users. *Note that solution information including sensitive data elements which require additional confidentiality and security measures (including that of other customers impacted in the event) will not be publicly disclosed. If Hyland Cloud customers need additional details of an incident, a request to the GCS Support team must be submitted and handled on a case by case basis. This Release of Information process may require an on-site review to protect the confidentiality and security of the requested information. Hyland will not unreasonably delay this notice, but it will only occur after initial corrective actions have been taken to contain the security threat or stabilize the Hyland Cloud platform.		
DISASTER RECOVERY							
H2.1	Vendor shall have documented disaster recovery plans that address the recovery of lost State data as well as their own. Systems shall be architected to meet the defined recovery needs.	M	Yes	Standard	The Hyland Cloud DR Plan establishes procedures to provide disaster recovery for all customers following a disruption of service. This plan focuses on disaster recovery for customer data and solutions housed in Hyland Cloud data centers. Services are grouped according to the service class levels described in the Service Class Manual. Those classifications are Silver, Gold, Platinum, and Double Platinum. The following objectives are contained within this plan: • Accounting of services and data sources • Prioritize services and data sources based on their relative business value • Prevent service disruptions from occurring • Avoid the loss of data through backup routines • Identify service disruptions when they occur • Recover disrupted services and data in a prioritized fashion • Resume normal service operations • Identify recovery limitations • Validate ongoing accuracy and operability of the Hyland Cloud Disaster Recovery Plan		

State Requirements					Vendor
Req #:	Requirement Description	Criticality	Vendor Response	Delivery Method	Comments
H2.2	The disaster recovery plan shall identify appropriate methods for procuring additional hardware in the event of a component failure. In most instances, systems shall offer a level of redundancy so the loss of a drive or power supply will not be sufficient to terminate services however, these failed components will have to be replaced.	M	Yes	Standard	The Hyland Cloud is N+1 redundant and every Hyland Cloud solution is replicated to a secondary data center. All data files are replicated, and the database is log shipped to this secondary location where the logs are also applied. The Hyland Cloud DR plan does identify appropriate methods for procuring additional hardware in the event of a component failure.
H2.3	Vendor shall adhere to a defined and documented back-up schedule and procedure.	M	Yes	Standard	The Hyland Cloud Disaster Recovery (DR) Plan was developed to assist the Hyland Global Cloud Services department to minimize disruptions and meet customer expected service levels in the event of a disaster at one of the Hyland Cloud data centers. This plan helps advance that directive by identifying services and data sources that the Hyland Cloud customers use and prioritizing those according to business need. These classifications are then incorporated into the procedure for recovering disrupted services, with higher priority services being restored first. The Hyland Cloud DR Plan also outlines methods used to mitigate potential disaster situations, including disaster prevention, avoidance of data loss, and continual monitoring of system components
H2.4	Back-up copies of data are made for the purpose of facilitating a restore of the data in the event of data loss or System failure.	M	Yes	Standard	Hyland Cloud customers are provided three copies of the data, two within the primary data center and one in a second data center in a different geographic location. These copies are stored to online storage so there is no offline storage to be destroyed. Hard copy documents are not created. Data sanitization techniques are used to overwrite data on the servers in use for the Hyland Cloud
H2.5	Scheduled backups of all servers must be completed regularly. The minimum acceptable frequency is differential backup daily, and complete backup weekly.	M	Yes	Standard	Redundant storage facilities, data backup, and replication are monitored daily and tested quarterly.
H2.6	Tapes or other back-up media tapes must be securely transferred from the site to another secure location to avoid complete data loss with the loss of a facility.	M	NA	NA	Customer data (database and images) in the Hyland Cloud is replicated within the primary hosting facility (Two are stored in the primary data center on separate hardware) and to a secondary data center in a different geographical location. Hyland does not use offline media for the replication of customer data within the Hyland Cloud. All copies remain on online media, and Hyland Cloud customers are empowered to manage the retention schedules of the content
H2.7	Data recovery – In the event that recovery back to the last backup is not sufficient to recover State Data, the Vendor shall employ the use of database logs in addition to backup media in the restoration of the database(s) to afford a much closer to real-time recovery. To do this, logs must be moved off the volume containing the database with a frequency to match the business needs.	M	Yes	Standard	The Hyland Cloud is N+1 redundant and every Hyland Cloud solution is replicated to a secondary data center. All data files are replicated, and the database is log shipped to this secondary location where the logs are also applied.

HOSTING SECURITY

Req #	Requirement Description	Criticality	Vendor Response	Delivery Method	Comments
	State Requirements				**Vendor**
H3.1	The Vendor shall employ security measures ensure that the State's application and data is protected.	M	Yes	Standard	The following outlines the efforts Hyland takes to secure the Hyland Cloud platform and our customers' hosted data: • The Hyland Cloud has numerous security controls and monitoring mechanisms in place, which includes firewalls at the Web and App server level, IDS, and vulnerability management. Logs are captured from these and other critical servers and network hosts and maintained in a centralized log repository. These logs are kept in non-repudiation format and kept for one year. Access to the central log repository is limited to a small team based on job role. Monitoring of these systems is active and alerts are configured to notify appropriate personnel within the department of potential security or availability incidents. Staff is available/on call 24/7 to respond to alerts from these systems. • Hyland uses commercially available safeguards to protect the Hyland Cloud platform and hosted data from intrusion, attack, or virus infection. The hosts on the Hyland Cloud platform employ anti-virus software, and the anti-virus signatures are updated daily by an automated signature repository. Anti-malware is installed and updated regularly within the Hyland Cloud platform. Software vendor information is not shared externally for security considerations. • In the Hyland Cloud, all data transfer is encrypted. By default, the Hyland Cloud uses AES - 256 bit TLS 1.2 and SSH2 transport encryption. When using 256 bit SSL, data is encrypted both from the workstation to the OnBase infrastructure and vice versa. Data transfers that utilize SFTP (SSH2 protocol) also encrypt traffic in both directions. • The OnBase modules Encrypted Alpha Keywords and Encrypted Disk Groups are included in standard Hyland Cloud solutions. These modules provide an additional layer of security for content stored in OnBase using AES – 256 encryption. Sensitive alphanumeric keywords are stored in the database in an encrypted format, with access to view full or partial values granted to authorized users. Documents are automatically encrypted as they are imported into OnBase, becoming indecipherable when retrieved outside of the system. Even within OnBase, these files are accessible only to permissioned users, further decreasing risk of exposure. • When customer data is replicated from the primary data center to the secondary data center, it remains
H3.2	If State data is hosted on multiple servers, data exchanges between and among servers must be encrypted.	M	Yes	Standard	In the Hyland Cloud, all data transfer is encrypted. By default, the Hyland Cloud uses AES - 256 bit TLS 1.2 and SSH2 transport encryption. When using 256 bit SSL, data is encrypted both from the workstation to the OnBase infrastructure and vice versa. Data transfers that utilize SFTP (SSH2 protocol) also encrypt traffic in both directions.
H3.3	All servers and devices must have currently-supported and hardened operating systems, the latest anti-viral, anti-hacker, anti-spam, anti-spyware, and anti-malware utilities. The environment, as a whole, shall have aggressive intrusion-detection and firewall protection.	M	Yes	Standard	Hyland uses commercially available safeguards to protect the Hyland Cloud platform and hosted data from intrusion, attack, or virus infection. The hosts on the Hyland Cloud platform employ anti-virus software, and the anti-virus signatures are updated daily by an automated signature repository. Anti-malware is installed and updated regularly within the Hyland Cloud platform.
H3.4	All components of the infrastructure shall be reviewed and tested to ensure they protect the State's hardware, software, and its related data assets. Tests shall focus on the technical, administrative and physical security controls that have been designed into the System architecture in order to provide confidentiality, integrity and availability.	M	Yes	Standard	Hyland Global Cloud Services utilizes many security controls, such as firewalls, IDS, and vulnerability management to ensure that customer data is secure. Additionally, Cloud Services uses a combination of enterprise and custom tools to monitor the Hyland Cloud platform. In addition to this, we contract with Accuvant Labs, Inc. to perform third-party penetration testing against the software as part of the finalization process for release. Because the Hyland Cloud provides network access, security, and monitoring services to its customers, each service is monitored and tested to assure performance and recoverability. This includes: Data center availability and environment services (e.g., power, cooling, fire detection/suppression) Network connectivity and support services (e.g., HTTPS, DNS, SFTP) Network security services (e.g., firewalls, data encryption, intrusion detection, anti-virus/anti-malware) OnBase processing services (e.g., document retrieval and business process workflow)

	State Requirements				Vendor
Req #	Requirement Description	Criticality	Vendor / Provides Response	Delivery Method	Comments
X3.5	The Vendor shall ensure its complete cooperation with the State's Chief Information Officer in the detection of any security vulnerability of the hosting infrastructure.	M	Yes	Standard	The Hyland Cloud has numerous security controls and monitoring mechanisms in place, which includes firewalls at the Web and App server level, IDS, and vulnerability management. Hyland Global Cloud Services will comply with and cooperate to the best of their ability in the detection of any security vulnerability of the hosting infrastructure within reason.
X3.6	The Vendor shall authorize the State to perform scheduled and random security audits, including vulnerability assessments, of the Vendor' hosting infrastructure and/or the application upon request.	M	Yes	Standard	Hyland GCS policies and procedures align with ISO 27001 controls. Hyland GCS is SOC 2 audited on an annual basis to ensure adherence to the documented policies and procedures. Customers who host their OnBase solution within the Hyland Cloud are not permitted to examine shared systems. Customers who select the Gold, Platinum, or Double Platinum classes of service are provided operational/risk audit rights. However, the scope of those audits is restricted to the customer's own data and configurations. Upon request, employees of Hyland Global Cloud Services will facilitate customer audits by collecting this type of evidence in a manner that has been deemed acceptable by the customer on a billable basis. OnBase functionalities are subjected to a penetration test or a vulnerability assessment by a third party. This is done in addition to the continuous penetration testing done by internal security testers. The results of the third-party tests are reviewed by the security team and prioritized for remediation. A summary report can be provided under an NDA. An independent third party conducts penetration testing on the Hyland Cloud network infrastructure within each of the Hyland Cloud datacenters at least once a year, and after any significant infrastructure or application upgrade or modification. Any vulnerability that has a risk of 'Critical' or 'High' (or equivalent based on the classifications of the vendors in use by GCS) will be remediated or mitigated. Documentation will be provided under an NDA. A Hyland Cloud customer may conduct an annual penetration test against the public URL used to access the hosted OnBase solution. This is contingent upon at least ninety (90) days' prior written notice and the mutual agreement on the timing, scope and criteria of the testing. This testing is offered at the customer's cost and expense to Hyland for the Professional Services required for the penetration test. An NDA will be required to
X3.7	All servers and devices must have event logging enabled. Logs must be protected with access limited to only authorized administrators. Logs shall include System, Application, Web and Database logs.	M	Yes	Standard	The Hyland Cloud has numerous security controls and monitoring mechanisms in place, which includes firewalls at the Web and App server level, IDS, and vulnerability management. Logs are captured from these and other critical servers and network hosts and maintained in a centralized log repository. These logs are kept in non-repudiation format and kept for one year. Access to the central log repository is limited to a small team based on job role. Monitoring of these systems is active and alerts are configured to notify appropriate personnel within the department of potential security or availability incidents. Staff is available/on call 24/7 to respond to alerts
X3.8	Operating Systems (OS) and Databases (DB) shall be built and hardened in accordance with guidelines set forth by CIS, NIST or NSA	M	Yes	Standard	Audit program and testing plans are developed based on industry best practices and standards, including ISO 27001, AICPA Trust Services Criteria, NIST, FFIEC. Auditing plans are established annually and approved by the Associate Vice President of Global Cloud Services. Auditing plans including selected controls, testing frequency, and scope. Additional standards are also followed for various functions as well. For instance, data destruction: Hyland Global Cloud Services uses techniques recommended by the National Institute for Standards and Technology (NIST) to destroy data as part of the decommissioning process. If a hardware device is unable to be decommissioned using these procedures, the device will be virtually shredded or physically destroyed in accordance with industry-standard practices. Devices used in the administration of the customer's hosted solution that have been decommissioned will be subjected to these or equally effective standards. Policies and Procedures: Global Cloud Services utilizes a variety of industry frameworks as the basis for our policies, procedures, and standards including NIST SP 800-53, ISO 27001 (data centers), and SOC2.
X3.9	The Vendor shall notify the State's Project Manager of any security breaches within two (2) hours of the time that the Vendor learns of their occurrence.	M	No	Not Available/Not Proposing	If Hyland has determined the customer's Hosted Solution has been negatively impacted by a security or availability incident, Hyland will deliver a root cause analysis summary. Although the notice will not be unreasonably delayed, it will only occur after initial corrective actions have been taken to contain the security threat or stabilize the Hyland Cloud platform.

	State Requirements				Vendor
Req #	Requirement Description	Criticality	Vendor Response	Delivery Method	Comments
H3.19	The Vendor shall be solely liable for costs associated with any breach of State data housed at their location(s) including but not limited to notification and any damages assessed by the courts.	M	Yes	Standard	Hyland carries security and privacy liability insurance, which contemplates coverage in the event of a covered security failure or privacy event. This is a third party coverage (meaning it is coverage in the event a covered security failure or privacy event causes damage to a customer or other 3rd party); however, it does not provide coverage to a customer directly or otherwise. Individual limits of liability are documented in the agreements from Hyland Software.
SERVICE LEVEL AGREEMENT					
H4.1	The Vendor's System support and maintenance shall commence upon the Effective Date and extend through the end of the Contract term, and any extensions thereof.	M	Yes	Standard	ImageSoft complies with this requirement.
H4.2	The vendor shall maintain the hardware and Software in accordance with the specifications, terms, and requirements of the Contract, including providing upgrades and fixes as required.	M	Yes	Standard	Software Support: The solution includes ImageSoft Standard and Customer Care Support. With Standard Support, ImageSoft will provide support for bug fixes and errors in the provided software. ImageSoft will liaise with Hyland Software support personnel to coordinate the resolution of the bug or software product error. With Customer Care Support, ImageSoft will assist NHDOL with upgrades to the solution, which includes Customer System Review, Establishing Upgrade Vision/Specification, Upgrade Planning and Upgrade Execution Assistance for both the server and client software, and remote technical services. NHDOL is responsible for testing and backup prior to an upgrade. With ImageSoft Customer Care support, we will work hand-in-hand with your Systems Administrators. Hardware Support: ImageSoft provides hardware maintenance support for equipment (e.g., scanners) purchased through ImageSoft. For the on-premise deployment option, NHDOL is responsible for hardware and hardware maintenance through their hardware vendor agreements. For a Hyland Cloud deployment option, Hyland is responsible for the hosting hardware and hardware maintenance, and ImageSoft Customer Care engages Hyland as necessary.
H4.3	The vendor shall repair or replace the hardware or software, or any portion thereof, so that the System operates in accordance with the Specifications, terms, and requirements of the Contract.	M	Yes	Standard	ImageSoft complies with this requirement.
H4.4	All hardware and software components of the Vendor hosting infrastructure shall be fully supported by their respective manufacturers at all times. All critical patches for operating systems, databases, web services, etc., shall be applied within sixty (60) days of release by their respective manufacturers.	M	No	Not Available/Not Proposing	Patches are applied within 90 days of release, but only after they have been tested in a non-production environment. Hyland Software evaluates each patch released for the Microsoft Windows operating system in order to ensure compatibility. Our partnership with Microsoft enhances Hyland's ability to identify and resolve compatibility issues more effectively.
H4.5	The State shall have unlimited access, via phone or Email, to the Vendor technical support staff between the hours of 8:30am to 5:00pm- Monday through Friday EST.	M			Included in ImageSoft Customer Care Support. See response to TOPIC 47 - SUPPORT AND MAINTENANCE.

	State Requirements				Vendor
Req #	Requirement Description	Criticality	Vendor Response	Delivery Method	Comment
H4.6	The Vendor shall conform to the specific deficiency class as described: o Class A Deficiency - Software - Critical, does not allow System to operate, no work around, demands immediate action; Written Documentation - missing significant portions of information or unintelligible to State; Non Software - Services were inadequate and require re-performance of the Service. o Class B Deficiency - Software - important, does not stop operation and/or there is a work around and user can perform tasks; Written Documentation - portions of information are missing but not enough to make the document unintelligible; Non Software - Services were deficient, require reworking, but do not require re-performance of the Service. o Class C Deficiency - Software - minimal, cosmetic in nature, minimal effect on System, low priority and/or user can use System; Written Documentation - minimal changes required and of minor editing nature; Non Software - Services require only minor reworking and do not require re-performance of the Service.	M	Yes	Standard	Services/Implementation: From a Services/Implementation perspective, project implementation challenges/deficiencies arise from many factors, some of which can be controlled, and some of which are more difficult to control. In general, issues should be resolved at the lowest level possible without escalation. When an individual recognizes an issue, they should first and foremost try to resolve the issue with informal conversation within the team. Those issues that cannot be resolved by the originator within the team should be raised to the project manager. The project manager will log the issue into the issue log along with the following information: Issue Number (sequentially assigned) Who raised the issue (originator) Date Raised Priority from High, Medium and Low (set by originator or project manager) Owner (assigned by project manager, if possible) The Hyland team reviews all issues during the internal status meeting. If possible, the issue will be assigned to a member of the team for resolution. In the event that Hyland and client project managers cannot resolve the issue, the issue will be escalated to the executive sponsors. Additionally, during the discovery phase, Hyland will document the requirements based off meetings with the customer. It is expected that the customer will base their use cases for testing off of this document and the business process that the solution supports. The Solution Requirements Document will be signed by the customer prior to implementation, and Hyland will configure the solution according to these specifications. Initial testing by Hyland will ensure that all requirements have been met, and the customer is also responsible for verifying this during their test process. Software Development: From a software development perspective, any software related deficiencies that are uncovered which are deemed to be caused by possible issues encountered within the software itself are handled via our internal Software Change Request (SCR) process. This process incorporates both software issues as well as software enhancements that are recorded within the SCR system. There is ongoing maintenance work within R&D when a defect is identified in a production release of the software. Hyland prides itself on being highly responsive to
H4.7	As part of the maintenance agreement, ongoing support issues shall be responded to according to the following: a. Class A Deficiencies - The Vendor shall have available to the State on-call telephone assistance, with issue tracking available to the State, eight (8) hours per day and five (5) days a week with an email / telephone response within two (2) hours of request; or the Vendor shall provide support on-site or with remote diagnostic Services, within four (4) business hours of a request; b. Class B & C Deficiencies - The State shall notify the Vendor of such Deficiencies during regular business hours and the Vendor shall respond back within four (4) hours of notification of planned corrective action; The Vendor shall repair or replace Software, and provide maintenance of the Software in accordance with the Specifications, Terms and Requirements of the Contract;	M			Support Issue Prioritization and Escalation Support issues that materially impact production use of the system are addressed immediately. Hyland will attempt to identify a workaround whenever a permanent solution to a software error cannot be provided within a reasonable timeframe. The Technical Support analyst assigned to a support issue is empowered to determine its impact on an end-customer's solution per the Severity Levels defined below, and to obtain immediate attention to the issue as required. Hyland partners who believe that the resolution process is not proceeding in a satisfactory manner are encouraged to contact Technical Support management. Support issue severity level and terminology is located in the Hyland Partner Technical Support Handbook.
H4.8	The hosting server for the State shall be available twenty-four (24) hours a day, 7 days a week except for during scheduled maintenance.	M	Yes	Standard	Hyland commits to system availability ranging from 99% to 99.9% uptime, depending on the Service Class selected by the customer.

	State Requirements			Vendor	
Req #	Requirement Description	Criticality	Vendor's Narrative Response	Delivery Method	Comments
M4.9	A regularly scheduled maintenance window shall be identified (such as weekly, monthly, or quarterly) at which time all relevant server patches and application upgrades shall be applied.	M	Yes	Standard	Hyland has no regularly scheduled downtime. When patching is required, Hyland provides two types of maintenance windows: scheduled maintenance and unscheduled maintenance. Hyland will notify customers of scheduled maintenance that is expected to impact or potentially impact system availability or functionality. The notification will typically be sent at least one week in advance, but not less than 24 hours prior to the specified start time. Hyland will notify customers of unscheduled maintenance that is expected to impact or potentially impact system availability or functionality. The notification will typically be sent at least 24 hours in advance, but not less than 2 hours prior to the specified start time. Both scheduled and unscheduled maintenance will be restricted to the hours of 10:00 p.m. to 8:00 a.m., based on the time zone of the impacted data center. Limitations on the aggregate number of hours of maintenance are determined based on the customer's selected
M4.10	If The Vendor is unable to meet the uptime requirement, The Vendor shall credit State's account in an amount based upon the following formula: (Total Contract Item Price/365) x Number of Days Contract Item Not Provided. The State must request this credit in writing.	M				Financial remedies are in place and are based on the customer's chosen service class level.
M4.11	The Vendor shall use a change management policy for notification and tracking of change requests as well as critical outages.	M	Yes	Standard	Hyland follows internal change management procedures when changes are initiated by Hyland, or when a customer requests to make a change on their behalf to existing systems, or when new systems are deployed to the Hyland Cloud. Generally speaking, change requests are submitted via a change management system and are then evaluated by subject matter experts. Upon approval by such subject matter experts changes are implemented, documented, and tested. In the event an issue occurs with the approved change, rollback procedures, documented as part of the change request, are performed in order to return the system to its original state.
M4.12	A critical outage will be designated when a business function cannot be met by a nonperforming application and there is no work around to the problem.	M	Yes	Standard	Hyland Cloud Services Definition of system availability: Hyland commits to system availability ranging from 99% to 99.9% uptime, depending on the Service Class selected by the customer. "Downtime" means the aggregate time (in minutes) each calendar month, as confirmed by Hyland following written notice from the customer, that the customer has experienced Network Unavailability, no documents stored in the Software can be retrieved from the Hosted Solution, or no documents can be input into the Software. The length of downtime is measured from the time the customer first reports the covered failure condition(s) to Hyland in writing until the time when Hyland's testing confirms that the failure condition(s) reported are no longer present.
M4.13	The Vendor shall maintain a record of the activities related to repair or maintenance activities performed for the State and shall report quarterly on the following: Server up-time; All change requests implemented, including operating system patches; All critical outages reported including actual issue and resolution; Number of deficiencies reported by class with initial response time as well as time to close.	M	Yes	Standard	For Hyland Cloud customers, Hyland Global Cloud Services (GCS) maintains documented incident reporting procedures. Incident reports are recorded and tracked to completion within Hyland's document management system. Customer notification is provided when applicable. GCS maintains a Customer Process Manual which describes the Hyland Cloud platform, its boundaries, the obligations/commitments of each party as it concerns security and availability, customer notification of related incidents, and also the procedure for customers to report security and/or availability issues. The Customer Process Manual is updated and released annually by GCS directly to registered customers through email. GCS maintains an internal audit program that focuses on developing, implementing, maintaining, and reassessing security controls to support risk mitigation strategies. The areas of focus include, but are not limited to, policy and procedure, logical and physical access, and business continuity. Quarterly internal audit results are compiled by the Governance, Risk and Compliance team and sent to the Vice President of GCS.

	State Requirements				Vendor	
Req #	Requirement Description	Criticality	Vendor Yes/No Response	Delivery Method	Bid	Comment
H4.14	The Vendor will give two-business days prior notification to the State Project Manager of all changes/updates and provide the State with training due to the upgrades and changes.	M	Yes	Standard	Upgrades are performed as they are available and typically upon request. They are scheduled with each Hyland Cloud customer. All configuration and software release changes made by Cloud Services on the customer's behalf will be implemented in a non-production environment before they are implemented on a production system. This non-production environment is designed to closely match the production hosting network configuration, including firewall policies. The customer must test the changes in this environment and provide a form of written acknowledgement before they can be applied to systems within our production hosting facility (e.g., an email stating that the changes are functioning as they are intended to).	

	SUPPORT & MAINTENANCE REQUIREMENTS				
	State Requirements				Vendor
Req #	Requirement Description	Criticality	Vendor Response	Delivery Method	Comments
SUPPORT & MAINTENANCE REQUIREMENTS					
S1.1	The Vendor's System support and maintenance shall commence upon the Effective Date and extend through the end of the Contract term, and any extensions thereof.	M	Yes	Standard	ImageSoft complies with this requirement.
S1.2	Maintain the hardware and Software in accordance with the Specifications, terms, and requirements of the Contract, including providing upgrades and fixes as required.	M	Yes	Standard	Software Support: The solution includes ImageSoft Standard and Customer Care Support. With Standard Support, ImageSoft will provide support for bug fixes and errors in the provided software. ImageSoft will liaise with Hyland Software support personnel to coordinate the resolution of the bug or software product error. With Customer Care Support, ImageSoft will assist NHDOL with upgrades to the solution, which includes Customer System Review, Establishing Upgrade Vision/Specification, Upgrade Planning and Upgrade Execution Assistance for both the server and client software, and remote technical services. NHDOL is responsible for testing and backup prior to an upgrade. With ImageSoft Customer Care support, we will work hand-in-hand with your Systems Administrators. Hardware Support: ImageSoft provides hardware maintenance support for equipment (e.g., scanners) purchased through ImageSoft. For the on-premise deployment option, NHDOL is responsible for hardware and hardware maintenance through their hardware vendor agreements. For a Hyland Cloud deployment option, Hyland is responsible for the hosting hardware and hardware maintenance, and ImageSoft Customer Care engages Hyland as necessary.
S1.3	Repair Software, or any portion thereof, so that the System operates in accordance with the Specifications, terms, and requirements of the Contract.	M	Yes	Standard	Included in Standard Support. See response to TOPIC 47 - SUPPORT AND MAINTENANCE.
S1.4	The State shall have unlimited access, via phone or Email, to the Vendor technical support staff between the hours of 8:30am to 5:00pm Monday through Friday EST.	M	Yes	Standard	Included in Standard Support. See response to TOPIC 47 - SUPPORT AND MAINTENANCE.

| SUPPORT & MAINTENANCE REQUIREMENTS | | | | | |
| State Requirements | | | | Vendor | |
Req #	Requirement Description	Criticality	Vendor Response	Delivery Method	Comments
S1.5	The Vendor response time for support shall conform to the specific deficiency class as described below or as agreed to by the parties: o Class A Deficiency - Software - Critical, does not allow System to operate, no work around, demands immediate action; Written Documentation - missing significant portions of information or unintelligible to State; Non Software - Services were inadequate and require re-performance of the Service. o Class B Deficiency - Software - Important, does not stop operation and/or there is a work around and user can perform tasks; Written Documentation - portions of information are missing but not enough to make the document unintelligible; Non Software - Services were deficient, require reworking, but do not require re-performance of the Service. o Class C Deficiency - Software - minimal, cosmetic in nature, minimal effect on System, low priority and/or user can use System; Written Documentation - minimal changes required and of minor editing nature; Non Software - Services require only minor reworking and do not require re-performance of the Service.	M	Yes	Standard	The deficiency classes align well to ImageSoft's Issue priority levels. See the Issue Resolution section in the response to TOPIC 47 - SUPPORT AND MAINTENANCE.
S1.6	The Vendor shall make available to the State the latest program updates, general maintenance releases, selected functionality releases, patches, and Documentation that are generally offered to its customers, at no additional cost.	M	Yes	Standard	OnBase provides one main software release annually, typically between July and August. Subsequent build versions or service packs are released at various times throughout the year. Customers automatically receive access to new version upgrades when they are available. However, no upgrade is performed without customer knowledge nor are upgrades forced. End users elect when they prefer to upgrade to a more recent version.
S1.7	For all maintenance Services calls, The Vendor shall ensure the following information will be collected and maintained: 1) nature of the Deficiency; 2) current status of the Deficiency; 3) action plans, dates, and times; 4) expected and actual completion time; 5) Deficiency resolution information, 6) Resolved by; 7) Identifying number i.e. work order number, 8) Issue identified by;	P	Yes	Standard	Customer Care Support calls collect and store the following information in our Case Management System: 1) nature of the Deficiency stored as Case Subject and Notes; 2) current status of the Deficiency stored as Status; 3) action plans, dates, and times stored as Tasks in the case. Each Task has an end time, duration, summary and notes; 4) expected and actual completion time stored as Resolution Date; 5) Deficiency resolution information stored as Resolution and Resolution Notes, 6) Resolved by stored as Case Owner, 7) Identifying number i.e. work order number stored as Case number, 8) Issue identified by stored as Contact;
S1.8	The Vendor must work with the State to identify and troubleshoot potentially large-scale System failures or Deficiencies by collecting the following information: 1) mean time between reported Deficiencies with the Software; 2) diagnosis of the root cause of the problem; and 3) Identification of repeat calls or repeat Software problems.	P	Yes	Standard	A large-scale System failure or Deficiency would be defined as a Critical Error. See the Issue Resolution section in the response to TOPIC 47 - SUPPORT AND MAINTENANCE

		SUPPORT & MAINTENANCE REQUIREMENTS				
	State Requirements				Vendor	
Req #		Requirement Description	Criticality	Vendor Response	Delivery Method	Comments
S1.9		As part of the Software maintenance agreement, ongoing software maintenance and support issues, shall be responded to according to the following or as agreed to by the parties: a. Class A Deficiencies - The Vendor shall have available to the State on-call telephone assistance, with issue tracking available to the State, eight (8) hours per day and five (5) days a week with an email / telephone response within two (2) hours of request; or the Vendor shall provide support on-site or with remote diagnostic Services, within four (4) business hours of a request; b. Class B & C Deficiencies – The State shall notify the Vendor of such Deficiencies during regular business hours and the Vendor shall respond back within four (4) hours of notification of planned corrective action; The Vendor shall repair or replace Software, and provide maintenance of the Software in accordance with the Specifications, Terms and Requirements of the Contract; or as agreed between the parties	M			The deficiency classes align well to ImageSoft's issue priority levels. See the Issue Resolution section in the response to TOPIC 47 - SUPPORT AND MAINTENANCE.
S1.10		The Vendor shall use a change management policy for notification and tracking of change requests as well as critical outages.	M	Yes	Standard	ImageSoft complies with this requirement. Internal change management procedures are followed when changes are initiated by ImageSoft or Customer requests to make a change.
S1.11		A critical outage will be designated when a business function cannot be met by a nonperforming application and there is no work around to the problem.	M	Yes	Standard	ImageSoft complies with this requirement. A Critical Outage is designated when the Error has been confirmed and Error Tracking Number has been assigned. The Error is either causing a significant portion of the system to be unusable, or is significantly affecting Customer productivity.
S1.12		The Vendor shall maintain a record of the activities related to repair or maintenance activities performed for the State and shall report quarterly on the following: All change requests implemented; All critical outages reported including actual issue and resolution; Number of deficiencies reported by class with initial response time as well as time to close.	M	Yes	Standard	ImageSoft is able to comply with this requirement. The following reports may be requested. 1) Service Availability, 2) Technical Support Activity, 3) Service Configuration, 4) Service Consumption, and 5) Datacenter Audit.
S1.13		The hosting server for the State shall be available twenty-four (24) hours a day, 7 days a week except for during scheduled maintenance.	M	Yes	Standard	ImageSoft complies with this requirement.
S1.14		The Vendor will guide the State with possible solutions to resolve issues to maintain a fully functioning, hosted System.	M	Yes	Standard	Included in ImageSoft Customer Care Support. See response to TOPIC 47 - SUPPORT AND MAINTENANCE.
S1.15		A regularly scheduled maintenance window shall be identified (such as weekly, monthly, or quarterly) at which time all relevant server patches and application upgrades shall be applied.	M	Yes	Standard	Customer will be notified of scheduled maintenance at least one week in advance, but in no event will such notice be sent less than 24 hours prior to the specific start time. In the event of a need for unscheduled maintenance, notification will be sent at 24 hours in advance, but in no event will such notice be less than 2 hours prior. Both scheduled and unscheduled maintenance will be restricted to the hours of 10 PM to 8 AM, based on the time zone of the impacted datacenter, unless other arrangements are mutually agreed to.
S1.16		The Vendor will give two-business days prior notification to the State Project Manager of all changes/updates and provide the State with training due to the upgrades and changes.	M	Yes	Standard	Changes, updates and upgrades to the solution are at the request of and coordinated with the Customer. The Customer may ImageSoft Professional Services can be engaged to develop specific training for their solution.

SUPPORT & MAINTENANCE REQUIREMENTS

		State Requirements				Vendor	
Req #		Requirement Description	Criticality	Vendor Response	Delivery Method		Comments
S1.17		All hardware and software components of the Vendor hosting infrastructure shall be fully supported by their respective manufacturers at all times. All critical patches for operating systems, databases, web services, etc, shall be applied within sixty (60) days of release by their respective manufacturers.	M	Yes	Standard		Vendors hosted infrastructure is in compliance with one or more of the following standards: International Organization for Standardization (ISO) 27001, Service Organization Controls (SOC), and/or SysTrust.
S1.18		The Vendor shall provide the State with a personal secure FTP site to be used by the State for uploading and downloading files if applicable.	M	Yes	Standard		ImageSoft complies with this requirement

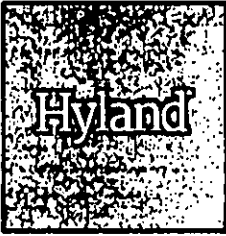| PROJECT MANAGEMENT					
State Requirements				**Vendor**	
Req #	Requirement Description	Criticality	Vendor's Response	Delivery Method	Comments
PROJECT MANAGEMENT					
P1.1	Vendor shall participate in an initial kick-off meeting to initiate the Project.	M	Yes	Standard	Conducting a kick-off meeting is a standard part of the Plan and Define phase of the project. See ImageSoft's response to TOPIC 39 – STATUS MEETINGS AND REPORTS for a description of ImageSoft's approach to conducting a project kick-off meeting.
P1.2	Vendor shall provide Project Staff as specified in the RFP.	M	Yes	Standard	The ImageSoft project team consists of highly trained specialists to support all phases of solution development. Each member plays a pivotal role in the success of a project. See ImageSoft's response to Section VI: Qualifications of Key Vendor Staff in the RFP response document.
P1.3	Vendor shall submit a finalized Work Plan within ten (10) days after Contract award and approval by Governor and Council. The Work Plan shall include, without limitation, a detailed description of the Schedule, tasks, Deliverables, critical events, task dependencies, and payment Schedule. The plan shall be updated no less than every two weeks.	M	Yes	Standard	See ImageSoft's response to TOPIC 43 - WORK PLAN.
P1.4	Vendor shall provide detailed bi-weekly status reports on the progress of the Project, which will include expenses incurred year to date.	M	Yes	Standard	Bi-weekly status meetings are recommended and allow both the ImageSoft and NHDOL project teams to work cooperatively on project planning, resource planning, communications and contractual activity. ImageSoft will prepare and distribute meeting minutes to all NHDOL Project Team members to ensure that both teams are aligned and informed on the current project status. See ImageSoft's response to TOPIC 39 – STATUS MEETINGS AND REPORTS. For fixed priced projects, ImageSoft does not typically include expenses incurred year to date in the bi-weekly status report.
P1.5	All user, technical, and System Documentation as well as Project Schedules, plans, status reports, and correspondence must be maintained as project documentation. (Define how- WORD format- on-Line; in a common library or on paper)	M	Yes	Standard	ImageSoft creates all project document deliverables in the Microsoft Office suite of tools and stores them on our BaseCamp project management collaboration tool website. Issues, risks, and decisions are maintained in the JIRA online repository. JIRA, by Atlassian, is ImageSoft's issue and project tracking software, which is used by our agile software development and implementation teams. See ImageSoft's response to TOPIC 43 - WORK PLAN.
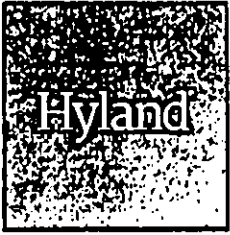
HYLAND CLOUD
CUSTOMER PROCESS MANUAL
VERSION 2019.1

Table of Contents

Introduction

The Hyland Cloud Customer Process Manual ("Process Manual") provides Customers a description of the services provided within the Hyland Cloud Platform ("Platform") by Hyland Software, Inc. ("Hyland"). Capitalized terms not defined in this Process Manual have the meanings as set forth in Hyland's Master Agreement, Terms of Use, Hosting Schedule, SaaS Schedule or other contractual agreement between Hyland and the Customer which incorporates the Process Manual by specifically referencing the Process Manual in such underlying agreement.

An electronic copy of the latest Process Manual is available to customers through the Hyland Community site in the Secure Downloads area at: https://www.hyland.com/community and through the Cloud Portal at https:// https://mycloud.onbaseonline.com/. The Process Manual is reviewed by Hyland, periodically, and modifications or the revised Process Manual is posted on the listed web locations. Authorized Customer Representatives will receive notice when modification to the Process Manual are released.

System Description

This system description delineates the boundaries of the various components of a functioning Platform, including: the products and services provided by Hyland and its vendors; the products and services provided by Hyland's authorized solution providers; and the services and obligations fulfilled by the Customer and its partners or vendors.

Background

The Platform is a multi-instance hosting platform for Hyland's cloud-based products and services. Customers utilize these products and services to fulfil their unique business needs. The Global Cloud Services ("GCS") department within Hyland is responsible for the administration of the Platform.

Infrastructure

The Platform offers hosting services for products and services developed and owned by Hyland. Hyland may from time to time choose additional products or services to have a hosting option. Hyland provides hosting services through co-location, internet-enabled network infrastructure that is owned and operated by Hyland and ISP providers ("Co-location Services"), or through deployment with a third-party cloud provider for solutions in the Platform. However, deployment options are product dependent. ·

When applicable, Hyland deploys servers within each data center on an as-needed basis which may include, but is not limited to, web, application, file and database servers. A variety of peripheral devices are also used. This

may include, but is not limited to, network appliances, disk drives, and keyboard video monitor switches. This includes industry-leading technology designed to provide a load balanced, redundant, and highly available Hosted Solution. An N-tiered architecture is used to support presentation, application, processing, and data services. For enhanced security in the Platform, technologies such as, but not limited to, firewalls, intrusion detection and prevention, and vulnerability management are used.

Co-location Services

The hardware components associated with the Platform's Co-location Services are physically located within data centers that provide the availability and resiliency necessary to operate the Platform. These data centers are owned and operated by Internet Service Providers (ISPs) 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 ISPs provide Internet connectivity, physical security, power, and environmental systems and services for the Hyland Cloud Platform.

Third-Party Cloud Provider

Hosting services may be provided to customers through an internet-enabled network and infrastructure that is owned by a third-party cloud provider. Hyland deploys and manages the servers, OS services, storage, and network access and is ultimately responsible for the architecture and deployment of the cloud environment used to deploy the Platform. Solutions can be deployed in domestic and international regions within the third-party cloud environment. Hyland has no direct access to the physical infrastructure of the third-party cloud provider and enforces these requirements via contractual agreements with the third-party.

Data

Customer maintains ownership of all Customer Data uploaded to their Hosted Solution through the full lifecycle period. Customer Data is uploaded via TLS/SSL or through a services API over a TLS/SSL connection to the Platform. Customer Data that resides in the Platform is encrypted at rest. Strict access control is in place for Customer Data within the Platform. Customer administrators control user access, user permissions, and data retention with respect to the Hosted Solution. Hyland treats Customer Data with the most restrictive data classification and applies technical controls as described in this Process Manual to comply with all applicable privacy and confidentiality laws, rules, and regulations (e.g. data encryption at rest and in transit, strict access controls). The Customer is responsible for ensuring that the Hosted Solution meets the Customer's legal and/or compliance obligations.
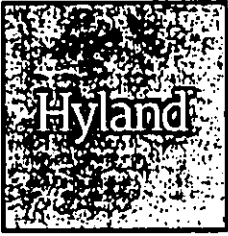
Data Access Controls in the Hyland Cloud Platform

As a multi-instance hosting platform, the Platform provides logically separated storage for each customer, which prevents the documents and metadata belonging to multiple tenants from being comingled. Access to documents, meta-data, output command, configuration commands, and processing commands may be controlled via permissions. Customers manage the user group membership and authentication records for their users. Multi-factor authentication is required before any Hyland employee is permitted administrative access to the Platform. Hyland employee access is provisioned using the least-privilege methodology.

Device Decommissioning

Hyland procedures include a decommissioning process that is designed to prevent Customer Data from being exposed to unauthorized individuals. Hyland uses the techniques recommended by NIST to destroy data as part of the decommissioning process. If a hardware 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.

People

Hyland employees must undergo comprehensive screening during the hiring process. Background checks and reference validation are performed to determine whether candidate qualifications are appropriate for the proposed position. Subject to any restrictions imposed by applicable law, these background checks include federal, state, and county criminal background checks, employment validation, and education verification.

Candidates for employment within GCS, including internal transfers, must be approved by the Vice President of Global Cloud Services and Hyland Human Resources before the employment positions are offered. This approval may be contingent upon the successful completion of additional security screening and training.

Hyland personnel are granted only the specific privileges required for them to carry out their normal duties in supporting the Platform. Hyland uses a variety of preventive, detective, and reactive controls. These include strict data access controls for Customer Data and confidential information, multiple levels of monitoring, logging, reporting, and combinations of controls that provide for the independent detection of unauthorized activity or access to customer solutions and data.

System Boundaries

The systems that compose a functioning Platform are limited to shared components such as network devices, servers, and software that are deployed and operating within the Platform. This system boundary also includes the

network connectivity, power, physical security, and environmental services provided by the third-party ISP that owns and operates the data centers in which this network infrastructure is collocated (when applicable).

Hyland is not responsible for any system components that are not within this system boundary, 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.
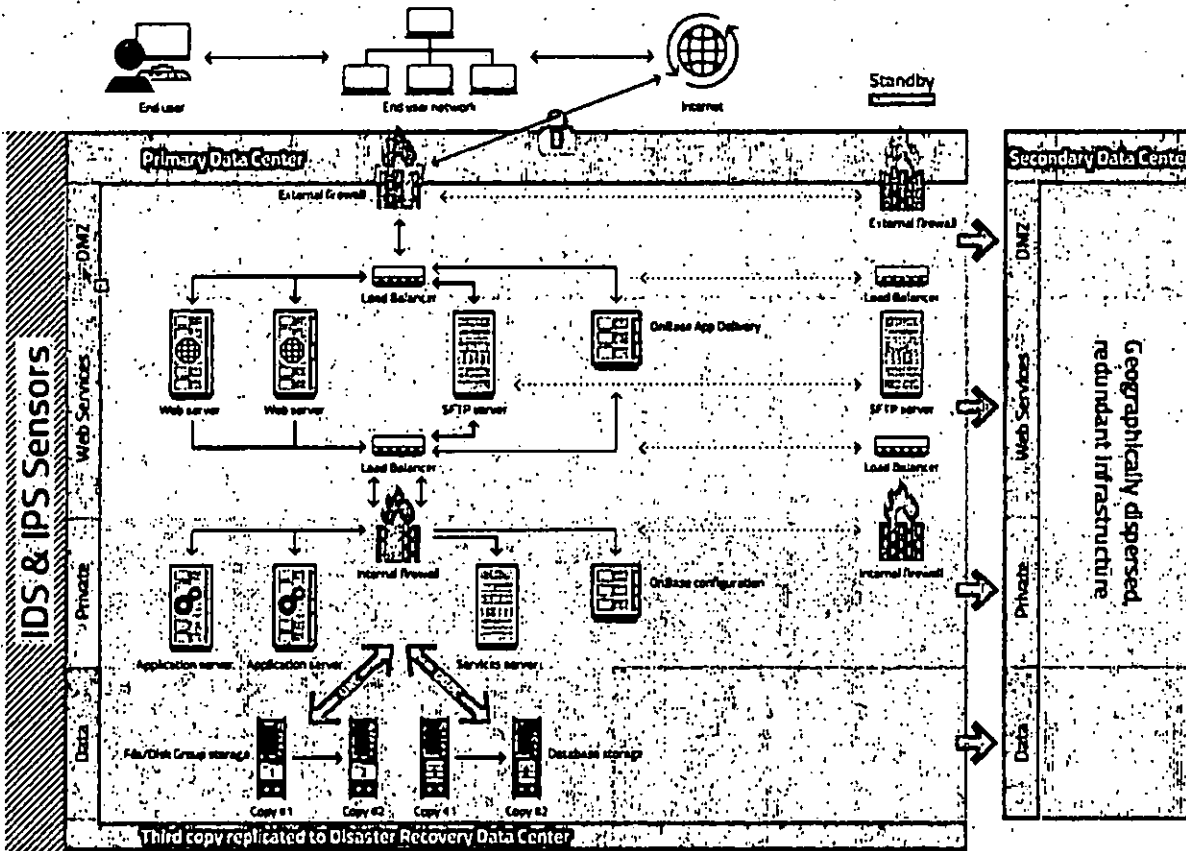
FIGURE 1 – GENERAL DIAGRAM OF HYLAND CLOUD PLATFORM ARCHITECTURE. ARCHITECTURE MAY VARY BASED ON PRODUCT SELECTED.

Process Boundaries

The processes executed within the Platform are limited to those that are executed by a Hyland employee (or authorized third party) or processes that are executed within our established system boundaries, in whole. This includes, but is not limited to, hardware installation, software installation, data replication, data security, and authentication processes.

Certain business processes may cross these boundaries, meaning one or more tasks are executed outside of the system boundaries that have been established for the Platform, one or more tasks are executed by individuals who are not Hyland employees (or authorized third-parties), or one or more tasks are executed based on written requests placed by a 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. Examples of business processes that cross these boundaries include, but are not limited to, Hosted Solution configuration changes, processing that occurs within the Hosted Solution, user authorization, and file transfers.

Special Considerations

This section applies to Hosted Healthcare customers who are receiving designated administration services from the Hyland Hosted Healthcare Services Team.

If the Hosted Solution includes hardware and/or software interfaces to be used for data integration and those resources will be remotely managed and supported by Hyland, Customer must provide access and administrative permissions to hardware and software interfaces located on the Customer's network to the appropriate Hyland personnel. Local technical and systems support for these data communication interfaces and systems at the Customer's location may also be required.

The Customer is responsible for maintaining all clinical and diagnostic activity, and for implementation and operation of all accounting, management and reporting systems, and audit functions.
If the Hosted Solution includes Master Patient Index feeds (MPI), Customer must provide such data and the related specifications in a timely manner.

Responsibilities

Responsibilities are applicable to all Hyland Cloud products unless otherwise noted.

Hyland Responsibilities

Hyland will:

1. Provide access to the Hosted Solution for use by the Customer by deploying and managing system components within the Platform system boundaries, as defined within this document. This hosting service will be delivered in a manner that is consistent with the underlying agreement.
2. Upon request and the payment of applicable fees by Customer, deploy the Hosted Solution for use by Customer.
3. Manage Hosted Solution configuration changes performed on behalf of Customer based on written requests from authorized Customer employees or authorized third parties, when applicable.
4. Report and respond to qualified security incidents. If Hyland has determined the Customer's Hosted Solution has been negatively impacted by a security incident, Hyland will deliver a root-cause analysis summary to the Authorized Customer Representative. Such notice will not be unreasonably delayed, but will only occur after initial corrective actions have been taken to contain the threat and stabilization of the Platform has been completed. Assistance from the Customer may be required.
5. Respond to reported availability incidents. This may include, but is not limited to, activities required to restore access to the Customer's Hosted Solution. If Customer has reported an availability incident to Hyland Technical Support, Hyland will deliver a root-cause analysis summary to the Authorized Customer Representative. Such notice will not be unreasonably delayed, but will only occur after initial corrective actions have been taken to contain the threat and stabilization of the Platform has been completed. Assistance from Customer may be required.
6. Maintain disaster recovery preparations, including data replication and periodic reviews.
7. Use reasonable efforts to test work performed by Hyland employees and Hyland vendors.
8. Use reasonable efforts to monitor the overall security and availability of the Platform.
9. Upon request of Customer, provide information on available features and functionality of Customer's Hosted Solution that could assist Customer in storing confidential or personal identifying information.

Customer Responsibilities

Customer will:

1. Designate to Hyland Authorized Customer Representatives, such as:
   a. Customer Security Administrator ("CSA") personnel who are authorized to communicate Customer's policies, submit Hosted Solution configuration requests to Hyland, or speak authoritatively on behalf of Customer and shall receive and provide, as applicable, all notifications related to maintenance, security, service failures and the like.
   b. Failure Notification Contact ("FNC") personnel who are to be notified of circumstances affecting access to the Hosted Solution, such notifications related to maintenance, security, service failures and the like.

c. Or other personnel as required by Hyland during the deployment of the Hosted Solution and associated products.

2. Be responsible for revocation of access to the environment immediately for unauthorized users and reporting changes to the Authorized Customer Representative as soon as possible to prevent inappropriate access and privileges.

3. Access the Hosted Solution remotely.

4. Provide web browser software, other compatible client software, and necessary communications equipment to access the Hosted Solution.

5. Install and manage system components outside of the Platform system boundaries, as described in this document.

6. Provide workstations that meet or exceed Hyland's minimum requirements for each software module installed.

7. Execute processes that are outside of the process boundaries as described in this document.

8. Identify and make use of Hosted Solution features to properly store confidential information and personal identifying information.

9. Be responsible for ensuring the Hosted Solution meets Customer's legal and/or compliance obligations.

10. Be responsible for all testing of the Hosted Solution upon installation prior to any production use, except as otherwise set forth in a Hyland Services Proposal, when applicable.

11. Be responsible for all testing of any configuration changes to the Hosted Solution software, except as otherwise set forth in a Hyland Services Proposal.

12. Perform Hosted Solution user authorization.

13. Control user group membership and the related permissions within the Hosted Solution.

14. Transfer files to the Platform using supported protocols and standards, when applicable.

15. Use reasonable efforts to monitor business processes and quality controls that are unique to the Customer's Hosted Solution. This includes batch processing of documents uploaded to the Platform.

16. Report and respond to security and availability incidents of which Customer becomes aware. Customer should report all such incidents to Hyland's Technical Support Department. The Hyland Technical Support representative will serve as the primary point of contact for the duration of the support issue unless Customer is advised differently by Hyland.

17. Work collaboratively with Hyland to respond to incidents, including security and availability incidents.

Standards and Procedures

Security

1. If Customer administrators believe they have experienced a security incident, they should contact their appropriate Technical Support contact as soon as possible after discovering the incident. The Hyland

Technical Support representative will serve as the primary point of contact for the duration of the support issue unless Customer is otherwise advised by Hyland.

2. Employees of Customer are not permitted to share their Hosted Solution login credentials (e.g. passwords, tokens, personal certificates, etc.) with other users.

3. Customer, must remove all inactive Hosted Solution accounts in a timely manner (e.g. when an employee is terminated).

4. Customer is responsible for all distribution of output under their control within the Hosted Solution.

5. Hyland utilizes virus protection software programs and definitions, which are configured to meet common industry standards in an attempt to protect the data and equipment located within the Hyland Cloud Platform from virus infections or similar malicious payloads.

6. If technically feasible, Customer may conduct penetration testing against the public URL used to access the Hosted solution on an annual basis; provided, that, (a) Customer provides Hyland with at least ninety (90) days' prior written notice of its desire to conduct such testing, (b) Hyland and Customer 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 (c) such testing is at Customer's cost and expense and Customer 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 Customer to assist with such testing, must enter into a Non-Disclosure Agreement directly with Hyland. Customer 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 Customer's access to or use of the Hosted Solution. Customer is prohibited from distributing or publishing the results of such penetration testing to any third party without Hyland's prior written approval.

Incident Response

Hyland employs incident response standards that are based upon applicable ISO/IEC 27001:2013 and National Institute for Standards and Technology ("NIST") standards to maintain the information security components of the environment by protecting and preserving the security, availability, confidentiality, and integrity of information.

Main categories of incidents that are considered in the Platform include:

- **Availability** – These are issues, related to the ability to access any component of the solution and/or environment. Availability issues can be a result of a security incident and/or include sub types such as data loss or integrity.
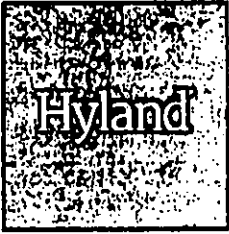
- **Security** – Any action or event that may have resulted in one or more individuals obtaining access to additional resources beyond those allocated or circumvention of information security measures will be treated as a Security Incident. Security incident may also be qualified as Confidential or Privacy to identify incidents related to unauthorized access, disclosure, and/or the usage confidential, protected, or personal information.

Responses to these incidents follow the Hyland documented incident response sequence. This sequence includes the following phases:

- **Preparation Phase** – All work done to prevent incidents and prepare team in the event of an incident.
- **Detection & Analysis Phase** – Initial report and review of the potential issue to determine if issue is qualified as an incident.
- **Containment, Eradication & Recovery Phase** – Activities involved in responding to the incident including stabilizing impact environment components to normal operations.
- **Post-Incident Activity Phase** – Activities involved in the closure of the incident, including final housekeeping with the customers and any follow-up.
- Any other activities involved in the incident documentation, continuous analysis of risk and impact, and communication to involved parties and stakeholders.

If Hyland has determined the Customer's Hosted Solution has been negatively Impacted by a security or availability incident, Hyland will deliver a root cause analysis summary. Such notice will not be unreasonably delayed, but will only occur after initial corrective actions have been taken to contain the security threat or stabilize the Platform

Change Management

Customer is responsible for testing all configuration changes, authentication changes, and upgrades to their Hosted Solution. In cases where the Customer relies upon Hyland to implement changes on its behalf, a written request describing the change must be submitted to technical support by an Authorized Customer Representative. Hyland will make scheduled configuration changes that are expected to impact Customer access to their Hosted Solution during a planned maintenance window. Hyland may make configuration changes that are not expected to impact Customer during normal business hours.

Hyland follows internal change management procedures. Generally, change requests are submitted via a change management system and are then evaluated by subject matter experts. Upon approval by such subject matter experts, changes are implemented, documented, and tested. In the event an issue occurs with the approved change, rollback procedures, documented as part of the change request, are performed in order to return the system to its original state.

Implementation Acknowledgement

When the Customer's Hosted Solution is first deployed on the Platform, or an existing Hosted Solution is upgraded to a newer release of the software, Hyland may ask the Customer to submit written acknowledgement affirming that the Hosted Solution has been successfully tested to the Customer's satisfaction. Hyland may delay the implementation of certain data protection or support services until Customer has submitted this written acknowledgement. This acknowledgement does not prevent Customer from making independent changes to the Hosted Solution. Rather, the intent is to facilitate effective change management by helping to ensure all parties work from a common point that is known to be fully functional and confirming that no loss of functionality has occurred as a result of hosting the solution on the Platform.

## Maintenance Communications and Restrictions

Hyland will notify Customer of scheduled maintenance that is expected to impact or potentially impact system availability or functionality. Hyland will use reasonable efforts to notify Customer of unscheduled maintenance that is expected to impact or potentially impact system availability or functionality. Notification will typically be sent at least one week in advance, but in no event will such notice be sent less than 24 hours prior to the specified start time. These notifications will be delivered electronically via e-mail or website notification to the Customer's Authorized Customer Representative.

Both scheduled and unscheduled maintenance will be restricted to within the hours of 10 PM to 8 AM, based on the time zone of the impacted data center, unless other arrangements have been mutually agreed to by Customer and Hyland. Scheduled hours for maintenance may be decreased by Hyland at Hyland's discretion, based on Customer's selected class of service. The scheduled hours of maintenance will be communicated to each Customer via e-mail in accordance with above notice provisions. For Customers that have purchased a Service Class, limitations on the aggregate number of hours of maintenance are set forth in the Service Class Manual, based on the Customer's selected class of service.

Audits

Hyland Cloud Data Centers

All third-party Internet Service and Cloud Providers used by Hyland have demonstrated compliance with the AICPA Service Organization Controls ("SOC") Reports for Service Organizations and/or ISO 27001 attestation standards (or a reasonable equivalent). Hyland validates the audit status of each third-party Internet Service
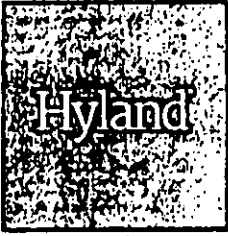
Provider on an annual basis. A copy of the most recent audit report is available to Customers in accordance with the third-party's audit report distribution policies.

Hyland Cloud Solutions

Hyland maintains a periodic external audit program for the Platinum and Double Platinum Service Class Customers as identified in their underlying agreement and for the OnBase Accelerated Financial Reporting Management (AFRM), ShareBase, and Perceptive hosted products. Attestations are typically completed on an annual schedule and currently utilize the SOC 2 standard. Platinum and Double Platinum Customer Hosted Solutions are expressly included in the SOC 2 sample size for testing. A copy of Hyland's most recent SOC 2 report is available to all customers upon written request. Hyland's SOC 3 report is available at Hyland.com.

Vulnerability assessments

Upon written request and no more than once per year, Hyland will perform a vulnerability assessment of the public URL used to access the Hosted Solution, for the purpose of identifying potential security weaknesses which may include (but is not limited to) inadequate input validation, sensitive data exposure, privilege escalation, cross site scripting, and broken session management. Hyland will create a report listing the number and severity of any weaknesses identified. Hyland will also provide a copy of such report to Customer. If the report contains vulnerabilities with a severity rating of "High" or "Critical", Hyland will coordinate with the Customer to perform additional analysis and/or document a remediation plan intended to reduce the associated risks. Customer is prohibited from distributing or publishing the results of such report to any third party without Hyland's prior written approval.

Customer Audits

Customer may conduct audits of Hyland's operations that participate in the ongoing delivery and support of the hosting services purchased by Customer on an annual basis; provided all the following criteria are met, (a) Customer provides Hyland with at least ninety (90) days prior written notice of its desire to conduct such audit, (b) 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, Hosted Solution configurations, invoices, or application logs, and (c) such audit is at Customer's cost and expense and Customer pays to 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 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.

Business Continuity

The GCS Business Continuity Management program establishes the standards and procedures that support the availability and resiliency of the Platform. GCS Business Continuity plans are reviewed annually with representatives in all applicable Hyland business and functional areas to ensure appropriate coverage and consideration of business objectives.

When technically feasible, Customers who purchase the Platinum or the Double Platinum Service Class, as described in the Service Class Manual, may participate in a data center failover test of Customer's Hosted Solution in order to determine each party's preparedness for a disaster or service failure; provided, that, (a) Customer provides Hyland with at least ninety (90) days' prior written notice of its desire to conduct failover testing, and (b) Hyland and Customer mutually agree upon the timing, scope, and criteria of such test, which may include document retrieval, document processing, and name resolution capabilities and (c) such failover testing is at Customer's cost and expense and Customer 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. Customer is prohibited from distributing or publishing the results of such testing to any third party without Hyland's prior written approval.

Reporting

Customer may request the following reports for all of their Hosted Solutions in the Hyland Cloud Platform

1. Service availability report containing a list of service level availability ("SLA") incidents that have been reported by Customer. The report will reflect each incident's confirmation or rejection by Hyland.
2. Technical Support Activity report containing a list of issues that have been reported by Customer. The listing of each issue will reflect the current status (Open, Closed, etc.).
3. Data center audit report containing the most recent attestation demonstrating that the third party data center provider used by Hyland in support of the Customer's Hosted Solution is compliant with the AICPA SOC Reports for Service Organizations, and/or ISO 27001 audit standards (or a reasonable equivalent).

The following reports are available to Customers that purchase the OnBase product option in the Hyland Cloud Platform:

1. Service Configuration report for the Customer's Hosted Solution. These reports will contain an accounting of the services that are currently configured in support of the Customer's Hosted Solution. For each service, the report will indicate the version of the OnBase software used, the number of servers on which it is hosted, and the version of the operating system in use on these servers.
2. Service Consumption Report containing a detailed accounting of the measurements used to generate the most recent invoice for the Customer's Hosted Solution. Totals are generated in multiple categories including disk group storage, database storage, and SFTP Archive storage.

SERVICE CLASS MANUAL

A Hyland Cloud Document

Version 2017.2
December 1, 2017
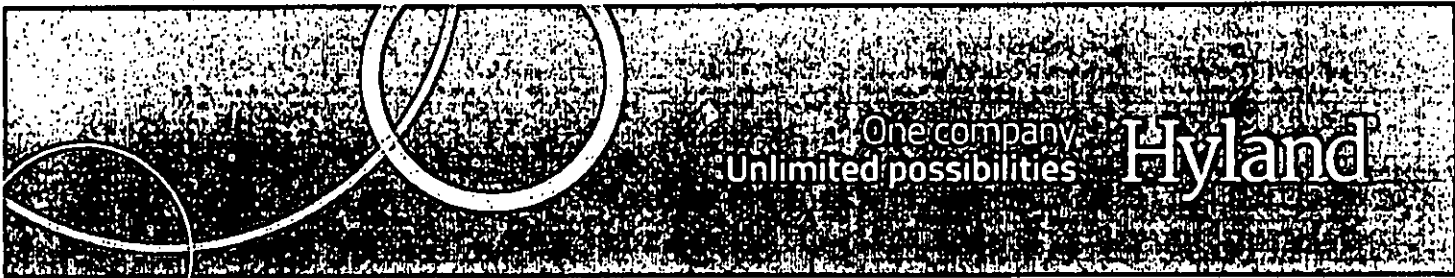
Table of Contents

Introduction

This Service Class Manual provides Customers a detailed description of the Service Level Commitments available for purchase by Customer as part of Standard Hosting Services. Capitalized terms not defined in this Service Class Manual have the meanings set forth in the Hosting Agreement.

Definitions

"Monthly Hosting Fee" means the Hosting Fees allocable to the month in which the applicable service failure occurred.

"Downtime" means the aggregate time (in minutes) each calendar month, as confirmed by Hyland following written notice from Customer, that: (1) Customer has experienced Network Unavailability; (2) no documents stored in the Software can be retrieved from the Hosted Solution; or (3) no documents can be input into the Software. The length of Downtime will be measured from the time Customer first reports the covered failure condition(s) to Hyland in writing until the time when Hyland's testing confirms that the failure condition(s) reported are no longer present. Downtime does not include any failure condition(s) described above which occur due to an Exclusion Event. Hyland agrees that following the occurrence of a Downtime event, Hyland shall provide to Customer a report which will include, as applicable, a detailed description of the incident, start and end times of the incident, duration of the incident, business/functional impact of the incident, description of remediation efforts taken, and a description of outstanding issues or tasks relating to the incident.

"Eligible Customer Data" means all Customer Data that Hyland confirms has been stored within the Software included in the Hosted Solution for a number of hours (prior to the time Hyland provides a Failover Notice) that exceeds the applicable recovery point objective set forth in table 2 under "Service Level Commitments" below.

"Exclusion Event" means any of the following occurrences:

(1) System Maintenance that is within the System Maintenance hours limit of the applicable Service Class (see "System Maintenance" below);

(2) failure of Customer's equipment or facilities;

(3) acts or omissions of Customer, including but not limited to (a) performance or non-performance of any services by a third party (other than Hyland) contracted by Customer to provide services to Customer related to the Hosted Solution, (b) any failure that Customer mutually agrees is not due to fault of Hyland or Hyland's contracted third party hosting company, (c) changes in Customer's business requirements that are not reported in advance to Hyland and addressed by
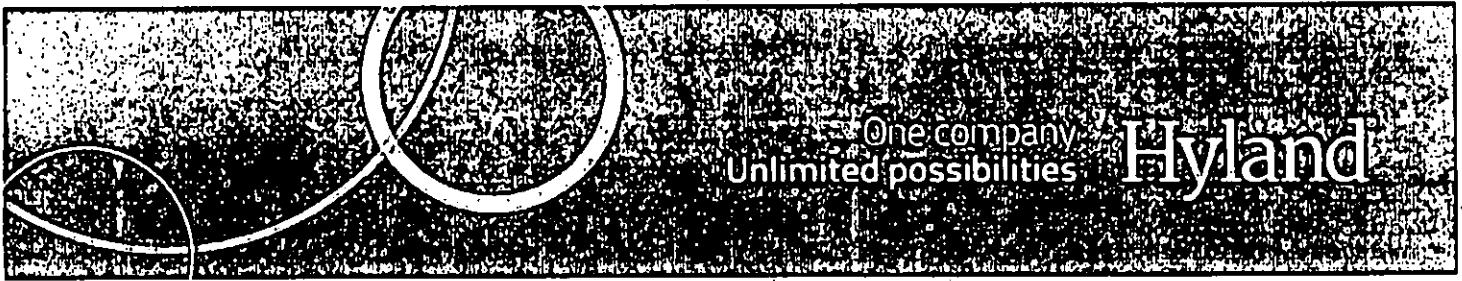
the parties through a change order (as described in the Hosting Agreement), or (d) failure of any code or configurations managed or written by Customer or any third party vendor to Customer;

(4) the occurrence of a force majeure event (as described in the Hosting Agreement)

(5) Internet failure or congestion;

(6) any defect or failure of any Third Party Software or hardware that is part of the Hosted Solution, where the manufacturer has discontinued maintenance and support of such Third Party Software or hardware, Hyland has notified Customer of such discontinuance and the need to upgrade, and Customer has not notified Hyland (within thirty (30) days after receipt of Hyland's notice) that Customer agrees to permit Hyland to upgrade such Third Party Software or hardware to a supported version; or

(7) provided that Hyland has fulfilled its obligations under the Process Manual with respect to virus protection, Hosted Solution failures or other failures caused directly or indirectly by known or unknown computer viruses, worms or other malicious programs.

"Failover Notice" means a written notice provided by Hyland to Customer (which notification may be made by electronic communication, including e-mail) indicating that Hyland is initiating a data center failover for the Hosted Solution.

"Monthly Uptime Percentage" means the total number of minutes in a calendar month, minus the number of minutes of Downtime in such month, divided by the total number of minutes in such month.

"Network Unavailability" means: (a) a loss of more than 1% of network traffic between the Network and data center provider's Internet backbone network; or (b) a latency of more than 100 milliseconds between the Network and the data center provider's Internet backbone network, in each case which is confirmed by Hyland over a period of at least five (5) minutes. The length of the Network Unavailability will be measured from the time Customer first notifies Hyland in writing of the failure condition(s) to the time when Hyland's measurements indicate that the failure condition(s) described are no longer present.

"System Maintenance" means the maintenance of the Hosted Solution, whether such maintenance is scheduled (e.g., for upgrading of the Software or any other Hosted Solution components or for any other scheduled purpose) or unscheduled (due to emergency), and which results in the Hosted Solution being unavailable or inaccessible to Customer.

"Recovery Point" means the minimum number of hours (prior to the time Hyland provides a Failover Notice) that Customer Data shall be stored within the Software included in the Hosted Solution to qualify as Eligible Customer Data.

"Recovery Time" means the number of hours from the time a Failover Notice is delivered to the time the Hosted Solution has been Restored, excluding all time during that period when an Exclusion Event affects both the current primary and secondary data centers.

"Restore" or "Restored" means that, except to the extent prevented by an Exclusion Event: (1) Eligible Customer Data can be stored in the Software and retrieved from the Hosted Solution; and (2) new Customer Data can be input into the Software.

Service Level Commitments

Table 1: Monthly Uptime Percentage

Service Classes	Silver	Gold	Platinum	Double Platinum
Monthly Uptime Percentage				
Monthly Uptime Percentage	99%	99.50%	99.80%	99.90%
Monthly Uptime Percentage Service Level Credits				
Monthly Uptime Percentage Service Credit Ranges and Applicable Credit Determinations	Less than 99% 25% of the Monthly Hosting Fee	99.49-99% 25% of the Monthly Hosting Fee	99.79-99% 25% of the Monthly Hosting Fee	99.89-99% 25% of the Monthly Hosting Fee
		Less than 99% 50% of the Monthly Hosting Fee	Less than 99% 50% of the Monthly Hosting Fee	Less than 99% 50% of the Monthly Hosting Fee

Table 2: Business Continuity

Service Classes	Silver	Gold	Platinum	Double Platinum
Business Continuity				
Recovery Point Objective	8 hours	4 hours	2 hours	1 hour
Recovery Time Objective	168 consecutive hours	48 consecutive hours	24 consecutive hours	4 consecutive hours
Business Continuity Service Level Credits				
Business Continuity Service Level Credit	50% of the Monthly Hosting Fee	50% of the Monthly Hosting Fee	50% of the Monthly Hosting Fee	50% of the Monthly Hosting Fee

Service Level Commitment Terms

Monthly Uptime Percentage. Hyland will meet the Monthly Uptime Percentage corresponding to the applicable Service Class purchased by Customer, as identified in table 1 above, during each calendar month.

Business Continuity. Hyland shall provide a Failover Notice prior to commencing a failover of the Hosted Solution from the current production data center to any backup data center. In the event Hyland delivers a Failover Notice to Customer, Hyland shall restore the Hosted Solution within the applicable Recovery Time objective set forth in the table 2 above.

Exclusive Remedies Terms

Monthly Uptime Percentage. In the event the Monthly Uptime Percentage during any calendar month is less than the applicable Monthly Uptime Percentage set forth in the Table 1, Hyland shall provide to Customer the applicable credit against Hosting Fees specified in Table 1 above.

For example, purposes only, assume Customer purchased the gold Service Class. In such event:

(i)   if Monthly Uptime Percentage is equal to or greater than 99%, but less than 99.5%, Customer shall receive a one-time credit against Hosting Fees in an amount equal to twenty-five percent (25%) of the Monthly Hosting Fee; or

(ii) If the Monthly Uptime Percentage is less than 99%, Customer shall receive a one-time credit against Hosting Fees in an amount equal to fifty percent (50%) of the Monthly Hosting Fee.

Business Continuity. If, following delivery of a Failover Notice, the Hosted Solution is not restored within the applicable Recovery Time objective set forth in Table 2, Hyland shall provide to Customer the applicable credit against Hosting Fees specified in Table 2 above.

Maximum Service Level Credit. Notwithstanding anything to the contrary herein, Customer acknowledges and agrees that Customer is only entitled to a maximum of one (1) service level credit for all events occurring in a particular calendar month. Customer shall be entitled to only the largest service level credit which may be payable for one or more of the service level failures occurring in such calendar month.

Application of Service Level Credits. Service level credits will be applied first to any outstanding amounts which are due and owing from Customer, and then to future Hosting Fees.

Termination Remedy. If Customer earns a service level credit either: (i) in two (2) consecutive calendar months, or (ii) in three (3) calendar months during any six (6) consecutive month period; then Customer may, by written notice to Hyland delivered within thirty (30) days after the last credit described in either clause or (i) or (ii) above is earned, terminate the Hosting Agreement.

Exclusivity. The remedies set forth above constitute the sole and exclusive remedies available to Customer for any failure to meet the service level commitments set forth in this Service Class Manual.

System Maintenance

Table 3: System Maintenance

Service Classes	Silver	Gold	Platinum	Double Platinum
System Maintenance				
Monthly System Maintenance Hours Limit	16 hours	16 hours	6 hours	6 hours

Except as otherwise agreed by Customer and Hyland, for the purposes of an Exclusion Event, System Maintenance shall not exceed the number of hours specified in the table above in any calendar month.

State of New Hampshire

Department of State

CERTIFICATE

I, William M. Gardner, Secretary of State of the State of New Hampshire, do hereby certify that HYLAND SOFTWARE, INC. is a Ohio Profit Corporation registered to transact business in New Hampshire on June 26, 2009. I further certify that all fees and documents required by the Secretary of State's office have been received and is in good standing as far as this office is concerned.

Business ID: 615852

Certificate Number: 0004896021

IN TESTIMONY WHEREOF,
I hereto set my hand and cause to be affixed
the Seal of the State of New Hampshire,
this 18th day of April A.D. 2020.

William M. Gardner
Secretary of State

Hyland

HYLAND SOFTWARE, INC.

SECRETARY'S CERTIFICATE

I, the undersigned, the duly elected and acting Secretary of Hyland Software, Inc. a corporation organized and existing under the laws of the State of Ohio (the "Corporation"), do hereby certify that Noreen Kilbane, Executive Vice President & Chief Administrative Officer, is a duly elected Officer of the Corporation and is authorized to enter into, execute, acknowledge and attest to any agreements, instruments or documents on behalf of the Corporation.

IN WITNESS. WHEREOF, I have hereunto set my hand on behalf of the Corporation as of the date first written above.

HYLAND SOFTWARE, INC.

By: _Abby Moskovitz_

Date: April 17, 2020

Name: Abby Moskovitz

Title: Corporate Secretary

ACORD® CERTIFICATE OF LIABILITY INSURANCE

DATE (MM/DD/YYYY) 03/15/2020

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

IMPORTANT: If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must have ADDITIONAL INSURED provisions or be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

PRODUCER		CONTACT NAME: Karen Ormiston	
The James B. Oswald Company		PHONE (A/C, No, Ext): (216) 367-8787	FAX (A/C, No): (216) 241-4520
1100 Superior Avenue East		E-MAIL ADDRESS: KOrmiston@oswaldcompanies.com	
Suite 1500			

		INSURER(S) AFFORDING COVERAGE	NAIC #
Cleveland	OH 44114	INSURER A : Federal Insurance Company	20281
INSURED		INSURER B : Great Northern Insurance Co.	20303
HSI Holdings I, Inc.		INSURER C : Pacific Indemnity Company	20346
Hyland Software, Inc		INSURER D : Nat'l Union Fire Ins Co of Pittsburgh PA	19445
28500 Clemens Road		INSURER E :	
Westlake	OH 44145	INSURER F :	

COVERAGES CERTIFICATE NUMBER: 19/20 GL/AUTO/WORK/ REVISION NUMBER:

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

INSR LTR	TYPE OF INSURANCE	ADDL INSD	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS	
A	☒ COMMERCIAL GENERAL LIABILITY ☐ CLAIMS-MADE ☒ OCCUR			35783325	12/31/2019	12/31/2020	EACH OCCURRENCE	$ 1,000,000
							DAMAGE TO RENTED PREMISES (Ea occurrence)	$ 1,000,000
							MED EXP (Any one person)	$ 10,000
							PERSONAL & ADV INJURY	$ 1,000,000
	GEN'L AGGREGATE LIMIT APPLIES PER: ☐ POLICY ☐ PROJECT ☐ LOC OTHER:						GENERAL AGGREGATE	$ 2,000,000
							PRODUCTS - COMP/OP AGG	$ 2,000,000
							Employee Benefit Liab	$ 1,000,000
B	AUTOMOBILE LIABILITY ☒ ANY AUTO ☐ OWNED AUTOS ONLY ☐ SCHEDULED AUTOS ☐ HIRED AUTOS ONLY ☐ NON-OWNED AUTOS ONLY			7352-28-83	12/31/2019	12/31/2020	COMBINED SINGLE LIMIT (Ea accident)	$ 1,000,000
							BODILY INJURY (Per person)	$
							BODILY INJURY (Per accident)	$
							PROPERTY DAMAGE (Per accident)	$
								$
A	☒ UMBRELLA LIAB ☒ OCCUR ☐ EXCESS LIAB ☐ CLAIMS-MADE			7988-20-68	12/31/2019	12/31/2020	EACH OCCURRENCE	$ 25,000,000
							AGGREGATE	$ 25,000,000
	☐ DED ☐ RETENTION $							$
C	WORKERS COMPENSATION AND EMPLOYERS' LIABILITY Y/N ANY PROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? (Mandatory in NH) If yes, describe under DESCRIPTION OF OPERATIONS below	N/A		(20) 7171-39-93	12/31/2019	12/31/2020	☒ PER STATUTE ☐ OTHER	
							E.L. EACH ACCIDENT	$ 1,000,000
							E.L. DISEASE - EA EMPLOYEE	$ 1,000,000
							E.L. DISEASE - POLICY LIMIT	$ 1,000,000
D	Errors & Omissions Liability			03-981-67-58	12/31/2019	12/31/2020	Retention:$500,000	Limit: $10M

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)

CERTIFICATE HOLDER	CANCELLATION
State of NH, Department of Information Technology ATTN:Chief Information Officer 27 Hazen Drive Concord NH 03301	SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS. AUTHORIZED REPRESENTATIVE Sara Miller

ACORD 25 (2016/03)   The ACORD name and logo are registered marks of ACORD