FRAMEWORK AGREEMENT

THIS FRAMEWORK AGREEMENT (this "Agreement") is made between the **CITY AND COUNTY OF DENVER**, a municipal corporation of the State of Colorado (the "City" or "Customer"), and **NAVIANT, LLC,** a Delaware limited liability company, whose address is 201 Prairie Heights Dr, Verona, WI 53593 (the "Contractor" or "Naviant"), individually a "Party" and jointly "the Parties."

RECITALS

WHEREAS, the City awarded this Agreement to the Contractor through a competitive selection for the purchase of software licensing, implementation, and support of the Hyland On-Base records request platform.

NOW, THEREFORE, in consideration of the mutual covenants and agreements hereinafter set forth and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the Parties incorporate the recitals set forth above agree as follows:

1. **COORDINATION AND LIAISON**: The Contractor shall fully coordinate all Work performed under this Agreement with the City's Chief Information Officer ("CIO"); with other personnel formally designated by the Department of Technology Services ("TS"); or, if applicable, with a representative from another City agency, as may be expressly designated by the CIO to act on behalf of the City for purposes of this Agreement. If a third party is designated by the CIO to serve as a liaison or coordinating entity on behalf of the City, the Contractor shall also coordinate its Work with such third party in the same manner and to the same extent as it would with City personnel.

2. **DEFINITIONS**

2.1. "**City Data**" means all data processed, stored, generated, collected, or transmitted on computers or other electronic media by or on behalf of the City, or provided to the Contractor for such processing, storage, generation, collection, or transmission, as well as any derivative data produced therefrom. City Data includes, but is not limited to: (i) information originally in physical format (including paper or other non-electronic media) that is subsequently digitized, scanned, or otherwise converted to electronic format; (ii) information provided to the Contractor by the City, authorized users, or third parties acting on the City's behalf; and (iii) confidential or sensitive information, financial data, public records, and any other regulated data, regardless of source, including but not limited to data from the City's employees, citizens, and contractors.

2.2. "**D(d)ata**" means information, regardless of form, that can be read, transmitted, or processed.

2.3. "**Deliverable(s)**" means a tangible object, SaaS, or On-Premise Software that is provided to the City by the Contractor under this Agreement.

2.4. "**Effective Date**" means the date on which this Agreement is approved and signed by the City as shown on the City's signature page.

2.5. "**Exhibits**" means the exhibits and attachments included with this Agreement.

2.6. "**On-Premise Software**" means software that the Contractor provides for the City's use that is installed and operated on City premises. For the avoidance of doubt, On-Premise Software does not include SaaS, though On-Premise Software may interface with SaaS.

2.7. "**SaaS**" means a software-as-a-service that the Contractor hosts (directly or indirectly) for the City's use. For the avoidance of doubt, SaaS does not include Services or On-Premise Software.

2.8. "**Service(s)**" means the technology related professional services to be performed by the Contractor as set forth in this Agreement and shall include any services or support provided by the Contractor under this Agreement.

2.9. "**Specifications**" refers to such technical and functional specifications for On-Premise Software, SaaS, and/or Deliverables included or referenced in an Exhibit.

2.10. "**Subcontractor**" means any third party engaged by the Contractor to aid in performance of the Work.

2.11. "**Task Order**" means a document issued in accordance with this Agreement that specifically describes the Work to be performed.

2.12. "**Work**" means any and all On-Premise Software, SaaS, Services, hardware, Deliverables, intellectual property, documentation, materials, labor, support, maintenance, training, updates, configurations, customizations, and other outputs and outcomes provided and/or performed by the Contractor pursuant to this Agreement, whether explicitly identified in this Agreement or reasonably necessary to fulfill the Contractor's obligations hereunder.

3. SOFTWARE AS A SERVICE, SUPPORT, AND SERVICES TO BE PERFORMED: As the City directs, the Contractor shall diligently undertake, perform, and make available the technology related Work set forth in the Exhibits to the City's satisfaction. The City shall have no liability to compensate the Contractor for Work that is not specifically authorized by this Agreement. The Work shall be provided and performed as stated herein and shall conform to the Specifications. The Contractor is ready, willing, and able to provide the Work required by this Agreement. The Contractor shall perform any Services in accordance with the standards of care, skill, training, diligence, and judgment provided by highly competent individuals performing services of a similar nature to those described in this Agreement and in accordance with the terms of this Agreement.

4. TASK ORDERS FOR ADDITIONAL PRODUCTS AND SERVICES

4.1. To initiate a Task Order, the City will provide a request to the Contractor describing the general scope and intent of the Work it desires the Contractor to perform under that Task Order. The Contractor shall submit a proposal, which shall include a quote, to the City in response to the City's request. All Task Orders, signed by the Parties, shall be issued in accordance with this Agreement using the rates contained therein. Each Task Order shall include a detailed scope of Services, level of effort, timeline for completion, rates or fixed fee pricing, and payment schedule, including a "not to exceed" amount, specific to each Task Order. Task Orders shall be construed to be in addition to, supplementary to, and consistent with the provisions of this Agreement. In the event of a conflict between a particular provision of any Task Order and a provision of this Agreement, this Agreement shall take precedence. A Task Order may be amended by the Parties by a written instrument prepared by the Parties jointly and signed by their authorized representatives.

4.2. The City is not required to execute any minimum number of Task Orders under this Agreement, and the City reserves the right to execute Task Orders with the Contractor at its sole discretion. The City shall have no liability to compensate the Contractor for any Work not specifically set forth in this Agreement or a properly executed Task Order. In no event shall a Task Order term extend beyond the Term unless the City has specifically agreed in writing. If this Agreement is terminated for any reason, each Task Order hereunder shall also terminate unless the City has specifically directed otherwise in writing. Task Orders may also be terminated in accordance with this Agreement's termination provisions. The Contractor agrees to fully coordinate its provision of Services with any third party under contract with the City relevant to the Contractor's performance hereunder.

4.3. The Contractor represents and warrants that all Services under a Task Order will be performed by qualified personnel in a professional and workmanlike manner, consistent with industry standards; all Services and/or Deliverables will conform to applicable, agreed upon specifications, if any; and, it has the requisite ownership, rights and licenses to perform its obligations under this Agreement fully as contemplated hereby free and clear from any and all liens, adverse claims, encumbrances and interests of any third party.

4.4. All Services and/or Deliverables will be performed in accordance with Exhibit A, any Task Orders issued hereunder, and the incorporated Software Support Level Agreement.

5. <u>TERM</u>: This Agreement will commence on October 1, 2025, and will expire, unless sooner terminated, on October 1, 2030 (the "Term"). Subject to the City's prior written authorization, the Contractor shall complete any work in progress as of the expiration date and the Term will extend until the work is completed or earlier terminated by the City.

6. END OF TERM EXTENSION: If this Agreement approaches the end of its Term, the City, at its discretion and upon written notice to the Contractor as provided herein, may unilaterally extend the Term for a period not to exceed six months (an "End of Term Extension). The provisions of this Agreement and the pricing in effect when such notice is given shall remain in effect during the End of Term Extension. The End of Term Extension shall automatically terminate upon execution of a replacement contract or modification extending this Agreement. To facilitate any agreed upon extensions in a timely manner, the Contractor shall negotiate any extension of this Agreement in good faith and provide the City all required order forms and updated pricing information to the City no later than one hundred twenty (120) days prior to the expiration of the Term. If the Contractor does not intend to extend the Term of this Agreement, the Contractor shall provide prompt notice to the City but not later than one hundred eighty (180) days prior to the expiration of the Term of its intent to let this Agreement lapse without an extension or replacement contract. The Contractor's obligation to facilitate a timely renewal under this Section is a material part of this Agreement.

7. COMPENSATION AND PAYMENT

7.1. Fees: The City shall pay, and the Contractor shall accept as the sole compensation for Services rendered and costs incurred under this Agreement the fees described in the attached Exhibits. Amounts billed may not exceed rates set forth in the Exhibits and will be made in accordance with any agreed upon payment milestones.

7.2. Reimbursement Expenses: There are no reimbursable expenses allowed under this Agreement. All the Contractor's expenses are contained in the budget as described in the Exhibits. The City will not be obligated to pay the Contractor for any other fees, costs, expenses, or charges of any nature that may be incurred and paid by the Contractor in performing their obligations under this

Agreement including but not limited to personnel costs, benefits, contract labor, overhead, administrative costs, operating costs, supplies, equipment, and out-of-pocket expenses.

7.3. Invoicing: The Contractor must submit an invoice which shall include the City contract number, clear identification of the Work that has been completed or delivered, and other information reasonably requested by the City. Payment on all uncontested amounts shall be made in accordance with the City's Prompt Payment Ordinance, §§ 20-107, *et seq.*, D.R.M.C, and no Exhibit or order form shall modify the City's statutory payment provisions.

7.4. Maximum Contract Amount

7.4.1. Notwithstanding any other provision of this Agreement, the City's maximum payment obligation will not exceed One Million Two Hundred Twenty-Six Thousand Thirty-Four Dollars ($1,226,034.00) (the "Maximum Agreement Amount"). The City is not obligated to execute an Agreement or any amendments for any further Work, including any Services performed by the Contractor beyond that specifically described in the attached Exhibits. Any Work performed beyond those in the attached Exhibits are performed at the Contractor's risk and without authorization under this Agreement.

7.4.2. The City's payment obligation, whether direct or contingent, extends only to funds appropriated annually by the Denver City Council, paid into the Treasury of the City, and encumbered for the purpose of this Agreement. The City does not by this Agreement irrevocably pledge present cash reserves for payment or performance in future fiscal years. This Agreement does not and is not intended to create a multiple-fiscal year direct or indirect debt or financial obligation of the City.

8. TAXES, CHARGES AND PENALTIES: The City shall not be liable for the payment of taxes, late charges, or penalties of any nature other than the compensation stated herein, except for any additional amounts which the City may be required to pay under D.R.M.C. § 20-107 to § 20-115.

9. STATUS OF CONTRACTOR: The Contractor is an independent contractor retained to perform professional or technical services for limited periods of time. Neither the Contractor nor any of its employees are employees or officers of the City under Chapter 18 of the Denver Revised Municipal Code, or for any purpose whatsoever. Nothing contained in this Agreement shall be construed as creating any agency, partnership, joint venture, or other form of joint enterprise, or employment relationship between the Parties.

10. TERMINATION

10.1. Either Party may terminate this Agreement, and the City may terminate a product under this Agreement, for the other Party's material breach by written notice specifying in detail the nature of the breach, effective in thirty (30) days unless the other Party first cures such breach, or effective immediately if the breach is not subject to cure.

10.2. The City has the right to terminate this Agreement or a product under this Agreement without cause upon thirty (30) days prior written notice to the Contractor. Nothing gives the Contractor the right to perform under this Agreement beyond the time when its Work becomes unsatisfactory to the City. Notwithstanding anything to the contrary contained in this Agreement, if the City terminates this Agreement without cause, the City shall be under no obligation to make further payment(s) for any remaining subscription years, licensing fees, or support costs as outlined in the attached Exhibits once the then current annual term expires; provide that, the City shall not be entitled to any refund, unless stated otherwise in the Exhibits, for the remainder of the prepaid annual term then in effect at the time of this Agreement's early termination without cause.

10.3. Notwithstanding the preceding paragraph, the City may terminate this Agreement if the Contractor or any of its officers or employees are convicted, plead nolo contendere, enter into a formal agreement in which they admit guilt, enter a plea of guilty or otherwise admit culpability to criminal offenses of bribery, kickbacks, collusive bidding, bid-rigging, antitrust, fraud, undue influence, theft, racketeering, extortion or any offense of a similar nature in connection with the Contractor's business. Termination for the reasons stated in this paragraph is effective upon receipt of notice.

10.4. Upon termination of this Agreement, with or without cause, the Contractor shall have no claim against the City by reason of, or arising out of, incidental or relating to termination, except for compensation for work duly requested and satisfactorily performed. Upon The City's request or upon termination, the Contractor shall return to the City all property placed in the Contractor's possession or control pursuant to this Agreement.

10.5. The City is entering into this Agreement to serve the public interest of the City as determined by its governing bodies. If this Agreement ceases to further the public interest of the City, or if the City fails to appropriate the necessary funding to continue this Agreement, the City, in its discretion, may terminate this Agreement in whole or in part. A determination that this Agreement should be terminated in the public interest or for lack of appropriation shall not be equivalent to a City right to terminate for convenience or without cause. This Subsection shall not apply to a termination of this Agreement by the City for a breach of contract by the Contractor. If the City terminates this Agreement in the public interest or for lack of appropriation, the City shall pay the Contractor an amount equal to the percentage of the total reimbursement payable under this Agreement that corresponds to the percentage of Work satisfactorily delivered or completed and accepted, as determined by the City, less payments previously made.

11. <u>EXAMINATION OF RECORDS AND AUDITS</u>: Any authorized agent of the City, including the City Auditor or his or her representative, has the right to access, and the right to examine, copy and retain copies, at City's election in paper or electronic form, any pertinent books, documents, papers and records related to the Contractor's performance pursuant to this Agreement, provision of any goods or services to the City, and any other transactions related to this Agreement. The Contractor shall cooperate with City representatives and City representatives shall be granted access to the foregoing documents and information during reasonable business hours and until the latter of three (3) years after the final payment under this Agreement or expiration of the applicable statute of limitations. When conducting an audit of this Agreement, the City Auditor shall be subject to government auditing standards issued by the United States Government Accountability Office by the Comptroller General of the United States, including with respect to disclosure of information acquired during the course of an audit. No examination of records and audits pursuant to this paragraph shall require the Contractor to make disclosures in violation of state or federal privacy laws. The Contractor shall at all times comply with D.R.M.C. 20-276.

12. **WHEN RIGHTS AND REMEDIES NOT WAIVED**: In no event shall any action by either Party hereunder constitute or be construed to be a waiver by the other Party of any breach of covenant or default which may then exist on the part of the Party alleged to be in breach, and the non-breaching Party's action or inaction when any such breach or default shall exist shall not impair or prejudice any right or remedy available to that Party with respect to such breach or default; and no assent, expressed or implied, to any breach of any one or more covenants, provisions or conditions of this Agreement shall be deemed or taken to be a waiver of any other breach.

13. **INSURANCE**

13.1. **General Conditions**: The Contractor agrees to secure, at or before the time of execution of this Agreement, the following insurance covering all operations, goods or services provided pursuant to this Agreement. The Contractor shall keep the required insurance coverage in force at all times during the term of this Agreement, including any extension thereof, and during any warranty period. The required insurance shall be underwritten by an insurer licensed or authorized to do business in Colorado and rated by A.M. Best Company as "A-VIII" or better. Each policy shall require notification to the City in the event any of the required policies be canceled or non-renewed before the expiration date thereof. Such written notice shall be sent to the parties identified in the Notices Section of this Agreement. Such notice shall reference the City contract number listed on the signature page of this Agreement. Said notice shall be sent thirty (30) days prior to such cancellation or non-renewal unless due to non-payment of premiums for which notice shall be sent ten (10) days prior. If such written notice is unavailable from the insurer, the Contractor shall provide written notice of cancellation, non-renewal and any reduction in coverage to the parties identified in the Notices Section by certified mail, return receipt requested within three (3) business days of such notice by its insurer(s) and referencing the City's contract number. The Contractor shall be responsible for the payment of any deductible or self-insured retention. The insurance coverages specified in this Agreement are the minimum requirements, and these requirements do not lessen or limit the liability of the Contractor. The Contractor shall maintain, at its own expense, any additional kinds or amounts of insurance that it may deem necessary to cover its obligations and liabilities under this Agreement.

13.2. **Proof of Insurance**: The Contractor may not commence services or work relating to this Agreement prior to placement of coverages required under this Agreement. The Contractor certifies that the certificate of insurance attached as **Exhibit C**, preferably an ACORD form, complies with all insurance requirements of this Agreement. The City requests that the City's contract number be referenced on the certificate of insurance. The City's acceptance of a certificate of insurance or other proof of insurance that does not comply with all insurance requirements set forth in this Agreement shall not act as a waiver of the Contractor's breach of this Agreement or of any of the City's rights or remedies under this Agreement. The City's Risk Management Office may require additional proof of insurance, including but not limited to policies and endorsements.

13.3. **Additional Insureds**: For Commercial General Liability, Auto Liability and Excess Liability/Umbrella (if required), the Contractor and Subcontractor's insurer(s) shall include the City and County of Denver, its elected and appointed officials, employees, and volunteers as additional insured.

13.4. **Waiver of Subrogation**: For all coverages required under this Agreement, with the exception of Professional Liability – if required, the Contractor's insurer shall waive subrogation rights against the City.

13.5. **Subcontractors and Subconsultants**: The Contractor shall confirm and document that all Subcontractors and subconsultants (including independent contractors, suppliers or other entities providing goods or services required by this Agreement) procure and maintain coverage as approved by the Contractor and appropriate to their respective primary business risks considering the nature and scope of services provided.

13.6. **Workers' Compensation and Employer's Liability Insurance**: The Contractor shall maintain the coverage as required by statute for each work location and shall maintain Employer's Liability insurance with limits of $100,000 per occurrence for each bodily injury claim, $100,000 per occurrence for each bodily injury caused by disease claim, and $500,000 aggregate for all bodily injuries caused by disease claims.

13.7. **Commercial General Liability**: The Contractor shall maintain a Commercial General Liability insurance policy with minimum limits of $1,000,000 for each bodily injury and property damage occurrence, $2,000,000 products and completed operations aggregate (if applicable), and $2,000,000 policy aggregate.

13.8. **Automobile Liability**: The Contractor shall maintain Automobile Liability with minimum limits of $1,000,000 combined single limit applicable to all owned, hired, and non-owned vehicles used in performing services under this Agreement.

13.9. **Cyber Liability**: The Contractor shall maintain Cyber Liability coverage with minimum limits of $1,000,000 per occurrence and $1,000,000 policy aggregate covering claims involving privacy violations, information theft, damage to or destruction of electronic information, intentional and/or unintentional release of private information, alteration of electronic information, extortion and network security. If Claims Made, the policy shall be kept in force, or a Tail policy placed, for three (3) years.

13.10. **Technology Errors & Omissions**: The Contractor shall maintain Technology Errors and Omissions insurance including network security, privacy liability and product failure coverage with minimum limits of $1,000,000 per occurrence and $1,000,000 policy aggregate. The policy shall be kept in force, or a Tail policy placed, for three (3) years.

14. DEFENSE AND INDEMNIFICATION

14.1. The Contractor hereby agrees to defend, indemnify, reimburse and hold harmless City, its appointed and elected officials, agents and employees for, from and against all liabilities, claims, judgments, suits or demands for damages to persons or property arising out of, resulting from, or relating to the work performed under this Agreement ("Claims") to the extent such Claims arise out of or result from the fault of the Contractor.

14.2. The Contractor's duty to defend and indemnify City shall arise at the time written notice of the Claim is first provided to City regardless of whether Claimant has filed suit on the Claim. The Contractor's duty to defend and indemnify City shall arise even if City is the only party sued by claimant and/or claimant alleges that City's negligence or willful misconduct was the sole cause of claimant's damages.

14.3. The Contractor will defend any and all Claims which may be brought against City and will pay on behalf of City any expenses incurred by reason of such Claims including, but not limited to, court costs and attorney fees incurred in defending and investigating such Claims or seeking to enforce this indemnity obligation. Such payments on behalf of City shall be in addition to any other legal remedies available to City and shall not be considered City's exclusive remedy.

14.4. Insurance coverage requirements specified in this Agreement shall in no way lessen or limit the liability of the Contractor under the terms of this indemnification obligation. The Contractor shall obtain, at its own expense, any additional insurance that it deems necessary for the City's protection.

14.5. The Contractor shall indemnify, save, and hold harmless the indemnified parties, against any and all costs, expenses, claims, damages, liabilities, and other amounts (including attorneys' fees and costs) incurred by the indemnified parties in relation to any claim that any Work provided by the Contractor under this Agreement (collectively, "IP Deliverables"), or the use thereof, infringes a patent, copyright, trademark, trade secret, or any other intellectual property right. The Contractor's obligations hereunder shall not extend to the combination of any IP Deliverables provided by the Contractor with any other product, system, or method, unless the other product, system, or method is (i) provided by the Contractor or the Contractor's subsidiaries or affiliates; (ii) specified by the Contractor to work with the IP Deliverables; (iii) reasonably required in order to use the IP Deliverables in its intended manner and the infringement could not have been avoided by substituting another reasonably available product, system, or method capable of performing the same function; or (iv) is reasonably expected to be used in combination with the IP Deliverables.

14.6. The Contractor shall indemnify, save, and hold harmless the indemnified parties against all costs, expenses, claims, damages, liabilities, court awards and other amounts, including attorneys' fees and related costs, incurred by the indemnified parties in relation to the Contractor's failure to comply with §§ 24-85-101, *et seq*., C.R.S., or the *Accessibility Standards for Individuals with a Disability* as established pursuant to § 24-85-103 (2.5), C.R.S. This indemnification obligation does not extend to the City's generated content using the Contractor's software, including any configuration or customization of the Contractor's software by the City.

14.7. This defense and indemnification obligation shall survive the expiration or termination of this Agreement.

15. LIMITATION OF THE CONTRACTOR'S LIABILITY: To the extent permitted by law, the liability of the Contractor, its Subcontractors, and their respective personnel to the City for any claims, liabilities, or damages relating to this Agreement shall be limited to damages, including but not limited to direct losses, consequential, special, indirect, incidental, punitive or exemplary loss, loss or unauthorized disclosure of City Data, not to exceed two (2) times the Maximum Agreement Amount payable by the City under this Agreement, subject to the following exceptions: (a) the Contractor's indemnification obligations to the City under this agreement shall be limited to a maximum of Five Million Dollars ($5,000,000.00); and (b) no limitation on the Contractor's liability to the City under this Section shall limit or affect (i) claims or damages arising out of bodily injury, including death, or damage to tangible property of the City; or (ii) claims or damages resulting from the recklessness, bad faith, or intentional misconduct of the Contractor or its Subcontractors.

16. COLORADO GOVERNMENTAL IMMUNITY ACT: The Parties hereto understand and agree that the City is relying upon, and has not waived, the monetary limitations and all other rights, immunities and protection provided by the Colorado Governmental Act, § 24-10-101, *et seq*., C.R.S.

17. COMPLIANCE WITH APPLICABLE LAWS AND POLICIES: The Contractor shall comply with all applicable laws, rules, regulations and codes of the United States, the State of Colorado; and with the Charter, ordinances, rules, regulations, public health orders, and Executive Orders of the City and County of Denver that are applicable to the Contractor's performance hereunder. These laws, regulations, and other authorities are incorporated by reference herein to the extent that they are applicable. Any of the Contractor's personnel visiting the City's facilities will comply with all applicable City policies regarding access to, use of, and conduct within such facilities. The City will provide copies of such policies to the Contractor upon request.

18. COMPLIANCE WITH DENVER WAGE LAWS: To the extent applicable to the Contractor's provision of Services hereunder, the Contractor shall comply with, and agrees to be bound by, all rules, regulations, requirements, conditions, and City determinations regarding the City's Minimum Wage and Civil Wage Theft Ordinances, Sections 58-1 through 58-26 D.R.M.C., including, but not limited to, the requirement that every covered worker shall be paid all earned wages under applicable state, federal, and city law in accordance with the foregoing D.R.M.C. Sections. By executing this Agreement, the Contractor expressly acknowledges that the Contractor is aware of the requirements of the City's Minimum Wage and Civil Wage Theft Ordinances and that any failure by the Contractor, or any other individual or entity acting subject to this Agreement, to strictly comply with the foregoing D.R.M.C. Sections shall result in the penalties and other remedies authorized therein.

19. DATA PROTECTION: The Contractor recognizes and agrees that: (i) City Data is valuable property of the City; (ii) City Data may include Confidential Information, protected or regulated data, and trade secrets of the City; and (iii) the City has dedicated substantial resources to collecting, managing, protecting, and compiling City Data. The Contractor recognizes and agrees that City Data may contain personally identifiable information or other sensitive information, even if the presence of such information is not labeled or disclosed. If the Contractor receives access to City Data, the Contractor shall comply with all applicable data protection laws, including the Colorado Consumer Protection Act and the Colorado Privacy Act, to the extent applicable. Other such obligations may arise from the Health Information Portability and Accountability Act (HIPAA), IRS Publication 1075, Payment Card Industry Data Security Standard (PCI-DSS), and the FBI Criminal Justice Information Service Security Addendum. At a minimum, the Contractor shall implement and maintain all appropriate administrative, physical, technical, and procedural safeguards necessary and appropriate to ensure compliance with the standards and guidelines applicable to the Contractor's performance under this Agreement. The Contractor shall also comply with the terms and conditions in the attached **Exhibit D**, Information Technology Provisions. Any Exhibit or external term hereto may not waive or modify the Contractor's legal obligations to protect City Data in compliance with applicable law under this Agreement.

20. <u>SAFEGUARDING PERSONAL INFORMATION</u>: "PII" means personally identifiable information including, without limitation, any information maintained by the City about an individual that can be used to distinguish or trace an individual's identity, including, but not limited to, first and last name, residence or other physical address, banking information, electronic mail address, telephone number, credit card information, an official government-issued driver's license or identification card number, social security number or tax identification number, date and place of birth, mother's maiden name, or biometric records. PII includes, but is not limited to, all information defined as personally identifiable information in §§ 24-73-101, C.R.S. "PII" shall also include "personal information" as defined in § 24-73-103(1)(g), C.R.S. If the Contractor or any of its Subcontractors receives PII under this Agreement, the Contractor shall provide for the security of such PII, in a manner and form acceptable to the City, including, without limitation, non-disclosure requirements, use of appropriate technology, security practices, computer and data access security, data storage and transmission encryption, security inspections, and audits. As applicable, the Contractor shall be a "Third-Party Service Provider" as defined in § 24-73-103(1)(i), C.R.S., and shall maintain security procedures and practices consistent with §§ 24-73-101, *et seq.*, C.R.S. In addition, as set forth in § 28-251, D.R.M.C., the Contractor, including, but not limited to, the Contractor's employees, agents, and Subcontractors, shall not collect or disseminate individually identifiable information about the national origin, immigration, or citizenship status of any person, over and above the extent to which the City is required to collect or disseminate such information in accordance with any federal, state, or local law.

21. <u>SECURITY BREACH AND REMEDIATION</u>

21.1. **<u>Security Breach</u>**: If the Contractor becomes aware of a suspected or unauthorized acquisition or disclosure of unencrypted data, in any form, that compromises the security, access, confidentiality, or integrity of City Data (a "Security Breach"), the Contractor shall notify the City in the most expedient time and without unreasonable delay. A Security Breach shall also include, without limitation, (i) attempts to gain unauthorized access to a City system or City Data regardless of where such information is located; (ii) unwanted disruption or denial of service; (iii) the unauthorized use of a City system for the processing or storage of data; or (iv) changes to the City's system hardware, firmware, or software characteristics without the City's knowledge, instruction, or consent. Any oral notice of a Security Breach provided by the Contractor shall be immediately followed by a written notice to the City.

21.2. **<u>Remediation</u>**: The Contractor shall implement and maintain a program for managing actual or suspected Security Breaches. In the event of a Security Breach, the Contractor shall cooperate with the City and law enforcement agencies, when applicable, to investigate and resolve the Security Breach, including, without limitation, providing reasonable assistance to the City in notifying third parties. The Contractor shall provide the City prompt access to such records related to a Security Breach as the City may reasonably request; provided such records will be the Contractor's Confidential Information, and the Contractor will not be required to provide the City with records belonging to, or compromising the security of, its other customers. The provisions of this Subsection do not limit the City's other rights or remedies, if any, resulting from a Security Breach. In addition, unless the Security Breach resulted from the City's sole act or omission, the Contractor shall promptly reimburse the City for reasonable costs incurred by the City in any investigation, remediation or litigation resulting from any Security Breach, including but not limited to providing notification to third parties whose data was compromised and to regulatory bodies, law-enforcement agencies, or other entities as required by law or contract; establishing and monitoring call center(s), and credit monitoring and/or identity restoration services to assist each person impacted by a Security Breach in such a fashion that, in the City's sole discretion, could lead to identity theft; and the payment of reasonable legal fees and expenses, audit costs, fines and penalties, and other fees imposed by regulatory agencies, courts of law, or contracting partners as a result of the Security Breach attributable to the Contractor or its Subcontractors.

22. ACCESSIBILITY AND ADA WEBSITE COMPLIANCE

22.1. **Compliance**: The Contractor shall comply with, and the Work provided under this Agreement shall be in compliance with, all applicable provisions of §§ 24-85-101, *et seq*., C.R.S., and the *Accessibility Standards for Individuals with a Disability*, as established pursuant to Section § 24-85-103 (2.5), C.R.S. (collectively, the "Guidelines"), to the extent required by law. The Contractor shall also comply with Level AA of the most current version of the Web Content Accessibility Guidelines (WCAG), incorporated in the State of Colorado technology standards.

22.2. **Testing**: The City may require, at the City's expense, the Contractor's compliance to be determined by a third party selected by the City to attest that the Contractor's has performed all obligations under this Agreement in compliance with §§ 24-85-101, *et seq.,* C.R.S., and the Accessibility Standards for Individuals with a Disability as established pursuant to § 24-85-103 (2.5), C.R.S.

22.3. **Validation and Remediation**: The Contractor agrees to promptly respond to and resolve any instance of noncompliance regarding accessibility in a timely manner and shall remedy any noncompliant Work at no additional cost to the City. If the City reasonably determines accessibility issues exist, the Contractor shall provide a "roadmap" for remedying those deficiencies on a reasonable timeline to be approved by the City. Resolution of reported accessibility issue(s) that may arise shall be addressed as high priority, and failure to make satisfactory progress towards compliance with the Guidelines, as agreed to in the roadmap, shall constitute a breach of contract and be grounds for termination or non-renewal of this Agreement.

23. CONFIDENTIAL INFORMATION

23.1. "Confidential Information" means all information or data, regardless of form, not subject to disclosure under the Colorado Open Records Act, §§ 24-72-201, *et seq*., C.R.S. ("CORA"), and is marked or identified at the time of disclosure as being confidential, proprietary, or its equivalent. Each of the Parties may disclose (a "Disclosing Party") or permit the other Party (the "Receiving Party") access to the Disclosing Party's Confidential Information in accordance with the following terms. Except as specifically permitted in this Agreement or with the prior express written permission of the Disclosing Party, the Receiving Party shall not: (i) disclose, allow access to, transmit, transfer or otherwise make available any Confidential Information of the Disclosing Party to any third party other than its employees, Subcontractors, agents and consultants that need to know such information to fulfill the purposes of this Agreement, and in the case of non-employees, with whom it has executed a non-disclosure or other agreement which limits the use, reproduction and disclosure of the Confidential Information on terms that afford at least as much protection to the Confidential Information as the provisions of this Agreement; or (ii) use or reproduce the Confidential Information of the Disclosing Party for any reason other than as reasonably necessary to fulfill the purposes of this Agreement. This Agreement does not transfer ownership of Confidential Information or grant a license thereto. The City will retain all right, title, and interest in its Confidential Information.

23.2. The Contractor shall provide for the security of Confidential Information and information which may not be marked but constitutes personally identifiable information or other federally or state regulated information ("Regulated Data") in accordance with all applicable laws and regulations. If the Contractor receives Regulated Data outside the scope of this Agreement, it shall promptly notify the City.

23.3. Disclosed information or data that the Receiving Party can establish: (i) was lawfully in the Receiving Party's possession before receipt from the Disclosing Party; or (ii) is or becomes a matter of public knowledge through no fault of the Receiving Party; or (iii) was independently developed or discovered by the Receiving Party; or (iv) was received from a third party that was not under an obligation of confidentiality, shall not be considered Confidential Information under this Agreement. The Receiving Party will inform necessary employees, officials, Subcontractors, agents, and officers of the confidentiality obligations under this Agreement, and all requirements and obligations of the Receiving Party under this Agreement shall survive the expiration or earlier termination of this Agreement.

23.4. Nothing in this Agreement shall in any way limit the ability of the City to comply with any laws or legal process concerning disclosures by public entities. The Parties understand that all materials exchanged under this Agreement, including Confidential Information, may be subject to CORA. In the event of a request to the City for disclosure of possible confidential materials, the City shall advise the Contractor of such request to give the Contractor the opportunity to object to the disclosure of any of its materials which it marked as, or otherwise asserts is, proprietary or confidential. If the Contractor objects to disclosure of any of its material, the Contractor shall identify to the City the legal basis under CORA for any right to withhold. In the event of any action or the filing of a lawsuit to compel disclosure, the Contractor agrees to intervene in such action or lawsuit to protect and assert its claims of privilege against disclosure of such material or waive the same. If the matter is not resolved, the City will tender all material to the court for judicial determination of the issue of disclosure. The Contractor further agrees to defend, indemnify, and save and hold harmless the City, its officers, agents, and employees, from any claim, damages, expense, attorneys' fees, or costs arising out of the Contractor's intervention to protect and assert its claim of privilege against disclosure under this Section.

24. <u>CRIMINAL JUSTICE INFORMATION</u>: The Contractor shall comply with all applicable standards of the Criminal Justice Information Services ("CJIS") Security Policy, attached hereto and incorporated herein as **Exhibit E** and all other requirements issued by the Federal Bureau of Investigation ("FBI"). The Contractor shall ensure that any Work provided under this Agreement protects the confidentiality, integrity, and availability of criminal justice information ("CJI") from unauthorized access, use, or disclosure. The Contractor shall ensure its responsibilities related to CJIS compliance are appropriately assigned and maintained and shall cooperate with any audits or inspections conducted by the City, the Colorado Bureau of Investigations, or the FBI to verify compliance with the CJIS Security Policy. The Contractor shall promptly report any breaches or incidents involving CJI to the City and take appropriate remedial actions. Contractors with direct access or indirect access to CJI shall handle all CJI following the CJIS Security Policy and Title 28, Code of Federal Regulations, Part 20 (relevant standards). Contractors supporting systems which provide direct access to CJI shall also follow the regulations listed in the laws, polices, and manuals incorporated into this agreement: NCIC Operating Manual, CCIC Training Manual, Interstate Identification Index / National Fingerprint File Operational and Technical Manual, and Title 28, Code of Federal Regulations, Part 23. Contractors who perform criminal justice functions and have access to CJI shall meet the same training and certification criteria required of governmental agencies performing a similar function and are subject to audit to the same extent as local agencies. Before receiving access to CJI or Federal Criminal History Record Information ("CHRI"), the Contractor and its individual employees must complete the attached CJIS Security Addendum certification attached hereto. The Contractor shall maintain signed CJIS Security Addendum certification pages for its personnel and shall provide copies to the City upon request.

25. <u>ASSIGNMENT; SUBCONTRACTING</u>: Except with regard to third party software providers utilized under this Agreement, the Contractor shall not sell, transfer, assign, subcontract performance obligations, or otherwise dispose of this Agreement or any portion thereof, including any right, title, or interest therein, without the City's prior written consent. The City shall not unreasonably withhold approval of an assignment when the Contractor is in full compliance with this Agreement and the proposed assignee, in the City's opinion, possesses sufficient business experience, aptitude, and financial resources to perform its obligations under this Agreement. The City may, at its reasonable discretion, approve the assignment, subcontract, or transfer in writing, deny it, or refer the matter to the City's governing bodies for approval. The City may execute its written approval of assignment through a signed consent letter without requiring a formal amendment to this Agreement, provided such consent letter explicitly references this Agreement. Any approved assignee shall be subject to all terms and conditions of this Agreement and other supplemental contractual documents; however, no approval by the City shall obligate the City beyond the provisions of this Agreement. Any assignment or subcontracting without the City's consent shall be ineffective and void and shall constitute grounds for termination of this Agreement by the City. Should unauthorized assignment or subcontracting occur, the Contractor shall remain responsible to the City, and no contractual relationship shall be created between the City and any subcontractor or assignee. This provision shall also apply to any reassignment of this Agreement due to change in ownership of the Contractor, and the Contractor shall notify the City in writing of any assignment due to change in ownership within thirty (30) days of such change.

26. **NO THIRD-PARTY BENEFICIARY**: Enforcement of the terms of this Agreement and all rights of action relating to enforcement are strictly reserved to the Parties. Nothing contained in this Agreement gives or allows any claim or right of action to any third person or entity. Any person or entity other than the City or the Contractor receiving services or benefits pursuant to this Agreement is an incidental beneficiary only.

27. **NO AUTHORITY TO BIND CITY TO CONTRACTS**: The Contractor lacks any authority to bind the City on any contractual matters. Final approval of all contractual matters that purport to obligate the City must be executed by the City in accordance with the City's Charter and the Denver Revised Municipal Code.

28. **AGREEMENT AS COMPLETE INTEGRATION-AMENDMENTS**: Except for the functional requirements provided in response to a request for proposal and/or any subsequent enhancement of the SOW or other implementation documentation that may be developed after execution of this Agreement, this Agreement is the complete integration of all understandings between the Parties as to the subject matter of this Agreement. No prior, contemporaneous, or subsequent addition, deletion, or other modification has any force or effect, unless embodied in this Agreement in writing. No oral representation by any officer or employee of the City at variance with the terms of this Agreement or any written amendment to this Agreement will have any force or effect or bind the City.

29. **SEVERABILITY**: Except for the provisions of this Agreement requiring appropriation of funds and limiting the total amount payable by the City, if a court of competent jurisdiction finds any provision of this Agreement or any portion of it to be invalid, illegal, or unenforceable, the validity of the remaining portions or provisions will not be affected, if the intent of the Parties can be fulfilled.

30. **CONFLICT OF INTEREST**: No employee of the City shall have any personal or beneficial interest in the Services or property described in this Agreement. The Contractor shall not hire, or contract for services with, any employee or officer of the City that would be in violation of the City's Code of Ethics, D.R.M.C. § 2-51, *et seq*. or the Charter §§ 1.2.8, 1.2.9, and 1.2.12. The Contractor shall not engage in any transaction, activity or conduct that would result in a conflict of interest under this Agreement. The Contractor represents that it has disclosed any and all current or potential conflicts of interest. A conflict of interest shall include transactions, activities or conduct that would affect the judgment, actions or work of the Contractor by placing the Contractor's own interests, or the interests of any party with whom the Contractor has a contractual arrangement, in conflict with those of the City. The City, in its sole discretion, will determine the existence of a conflict of interest and may terminate this Agreement in the event it determines a conflict exists, after it has given the Contractor written notice describing the conflict.

31. **NOTICES**: All notices required by the terms of this Agreement must be hand delivered, sent by overnight courier service, mailed by certified mail, return receipt requested, electronic mail with read receipt requested, or mailed via United States mail, postage prepaid, if to the Contractor at the

aforementioned address, and if to the City at: Chief Information Officer, Denver Technology Services, 201 West Colfax Avenue, Dept. 301, Denver, Colorado 80202; with a copy to: Denver City Attorney's Office, 1437 Bannock St., Room 353, Denver, Colorado 80202. Unless otherwise provided in this Agreement, notices shall be effective upon delivery of the written notice. Notices sent by certified mail are effective upon receipt. Notices sent by mail are effective upon deposit with the U.S. Postal Service. If a Party delivers a notice through email and the email is undeliverable, then, unless the Party has been provided with an alternate email contact, the Party delivering the notice shall deliver the notice by certified or registered mail to the addresses set forth herein. The Parties may designate electronic and substitute addresses where or persons to whom notices are to be mailed or delivered. However, these substitutions will not become effective until actual receipt of written notification.

32. DISPUTES: All disputes between the City and the Contractor arising out of or regarding this Agreement will be resolved by administrative hearing pursuant to the procedure established by D.R.M.C. § 56-106(b)-(f). For the purposes of that administrative procedure, the City official rendering a final determination shall be the CIO as defined in this Agreement. In the event of a dispute between the Parties, the Contractor will continue to perform its obligations under this Agreement during the resolution of the dispute until this Agreement is terminated in accordance with its terms.

33. GOVERNING LAW; VENUE: This Agreement will be construed and enforced in accordance with applicable federal law, the laws of the State of Colorado, and the Charter, Revised Municipal Code, ordinances, regulations and Executive Orders of the City and County of Denver, which are expressly incorporated into this Agreement. Unless otherwise specified, any reference to statutes, laws, regulations, charter or code provisions, ordinances, executive orders, or related memoranda, includes amendments or supplements to same. Venue for any legal action relating to this Agreement will be in the District Court of the State of Colorado, Second Judicial District (Denver District Court).

34. NO DISCRIMINATION IN EMPLOYMENT: In connection with the performance of work under this Agreement, the Contractor may not refuse to hire, discharge, promote, demote, or discriminate in matters of compensation against any person otherwise qualified, solely because of race, color, religion, national origin, ethnicity, citizenship, immigration status, gender, age, sexual orientation, gender identity, gender expression, marital status, source of income, military status, protective hairstyle, or disability. The Contractor shall insert the foregoing provision in all subcontracts.

35. LEGAL AUTHORITY: The Contractor represents and warrants that it possesses the legal authority, pursuant to any proper, appropriate, and official motion, resolution or action passed or taken, to enter into this Agreement. Each person signing and executing this Agreement on behalf of the Contractor represents and warrants that he has been fully authorized by the Contractor to execute this Agreement on behalf of the Contractor and to validly and legally bind the Contractor to all the terms, performances and provisions of this Agreement. The City shall have the right, in its sole discretion, to either temporarily suspend or permanently terminate this Agreement if there is a dispute as to the legal authority of either the Contractor or the person signing this Agreement to enter into this Agreement.

36. LITIGATION REPORTING: If the Contractor is served with a pleading or other document in connection with an action before a court or other administrative decision making body, and such pleading or document relates to this Agreement or may affect the Contractor's ability to perform its obligations under this Agreement, the Contractor shall, within 10 days after being served, notify the City of such action and deliver copies of such pleading or document, unless protected by law, to the City.

37. **LICENSES, PERMITS, AND OTHER AUTHORIZATIONS:** The Contractor shall secure, prior to the Term, and shall maintain, at its sole expense, all licenses, certifications, rights, permits, and other authorizations required to perform its obligations under this Agreement. This Section is a material part of this Agreement.

38. **NO CONSTRUCTION AGAINST DRAFTING PARTY**: The Parties and their respective counsel have had the opportunity to review this Agreement, and this Agreement will not be construed against any party merely because any provisions of this Agreement were prepared by a particular party.

39. **ORDER OF PRECEDENCE**: In the event of any conflicts between the provisions in the body of this Agreement, the Exhibits, or any other attachment hereto, the provisions in the body of this Agreement shall control. For the avoidance of doubt, no terms within any subsequent order form, invoice, or quote issued by the Contractor to the City shall be binding on the City or take precedence over the terms of the body of this Agreement regardless of any term contained therein to the contrary, unless a subsequent agreement is made in writing signed by both parties wherein a contrary term to this Agreement is specifically agreed upon.

40. **SURVIVAL OF CERTAIN PROVISIONS**: The terms of this Agreement, including any Exhibits and attachments, that by reasonable implication contemplate continued performance, rights, or compliance beyond the expiration or termination of this Agreement shall survive such expiration or termination and shall remain enforceable. Without limiting the foregoing, the Contractor's obligations to provide insurance coverage and to indemnify the City shall survive for a period equal to the duration of all applicable statutes of limitation, plus any additional time reasonably necessary to resolve any claims, disputes, or legal proceedings initiated within that period. Any grant of property rights or intellectual property rights to the City that, by its terms, extends beyond the term of this Agreement shall remain in effect after expiration or termination, except in the event of termination due to the City's breach of its payment obligations. Any warranties made available to the City, whether provided under this Agreement or otherwise, shall survive expiration or termination of this Agreement for the full duration specified in the warranty documentation or as permitted by applicable law. Upon expiration or termination of this Agreement, in whole or in part, the Contractor shall promptly return to the City all City Data and any other materials or information provided by the City, in the format reasonably requested by the City, and shall permanently delete or destroy all remaining copies thereof.

41. **INUREMENT**: The rights and obligations of the Parties herein set forth shall inure to the benefit of and be binding upon the Parties hereto and their respective successors and assigns permitted under this Agreement.

42. **TIME IS OF THE ESSENCE**: The Parties agree that in the performance of the terms, conditions, and requirements of this Agreement, time is of the essence.

43. **FORCE MAJEURE**: Neither Party shall be responsible for failure to fulfill its obligations hereunder or liable for damages resulting from delay in performance as a result of war, fire, strike, riot or insurrection, natural disaster, unreasonable delay of carriers, governmental order or regulation,

complete or partial shutdown of manufactures, unreasonable unavailability of equipment or software from suppliers, default of a Subcontractor or vendor (if such default arises out of causes beyond their reasonable control), the actions or omissions of the other Party and/or other substantially similar occurrences beyond the Party's reasonable control ("Excusable Delay"). In the event of any such Excusable Delay, time for performance shall be extended for as may be reasonably necessary to compensate for such delay.

44. PARAGRAPH HEADINGS: The captions and headings set forth herein are for convenience of reference only and shall not be construed to define or limit the terms and provisions hereof.

45. CITY EXECUTION OF AGREEMENT: This Agreement is expressly subject to and shall not be or become effective or binding on the City until it has been fully executed by all signatories of the City and County of Denver.

46. ADVERTISING AND PUBLIC DISCLOSURE: The Contractor shall not include any reference to this Agreement or to Services performed pursuant to this Agreement in any of the Contractor's advertising or public relations materials without first obtaining the City' written approval. Any oral presentation or written materials related to Services performed under this Agreement will be limited to Services that have been accepted by the City. The Contractor shall notify the City in advance of the date and time of any presentation. Nothing in this provision precludes the transmittal of any information to City officials.

47. EXTERNAL TERMS AND CONDITIONS DISCLAIMER: Notwithstanding anything to the contrary herein, the City shall not be subject to any provision including any terms, conditions, or agreements, and links thereto, appearing on the Contractor's or a Subcontractor's website, forms, or any provision incorporated into any click-through or online agreements related to the Work unless that provision is specifically incorporated into this Agreement.

48. PROHIBITED TERMS: Any term included in this Agreement that requires the City to indemnify or hold the Contractor harmless; requires the City to agree to binding arbitration; limits the Contractor's liability for damages resulting from death, bodily injury, or damage to tangible property; requires payment for any obligation where there has not been an appropriation; requires venue and jurisdiction outside of the Colorado; or seeks to modify the order of precedence, as stated in the main body of this Agreement; or that conflicts with this provision in any way shall be *void ab initio*. All contracts entered into by the City, except for certain intergovernmental agreements, shall be governed by Colorado law notwithstanding any term or condition to the contrary.

49. USE, POSSESSION OR SALE OF ALCOHOL OR DRUGS: To the extent applicable, the Contractor shall cooperate and comply with the provisions of Executive Order 94 and Attachment A thereto concerning the use, possession or sale of alcohol or drugs. Violation of these provisions or refusal to cooperate with implementation of the policy can result in the City barring the Contractor from City facilities or participating in City operations.

50. COUNTERPARTS OF THIS AGREEMENT: This Agreement may be executed in counterparts, each of which shall be deemed to be an original of this Agreement.

51. ELECTRONIC SIGNATURES AND ELECTRONIC RECORDS: The Contractor consents to the use of electronic signatures by the City. This Agreement, and any other documents requiring a signature hereunder, may be signed electronically by the City in the manner specified by the City. The Parties agree not to deny the legal effect or enforceability of this Agreement solely because it is in electronic form or because an electronic record was used in its formation. The Parties agree not to object to the admissibility of this Agreement in the form of an electronic record, or a paper copy of an electronic document, or a paper copy of a document bearing an electronic signature, on the ground that it is an electronic record or electronic signature or that it is not in its original form or is not an original.

52. **ATTACHED EXHIBITS INCORPORATED**: The following attached exhibits are hereby incorporated into and made a material part of this Agreement: **Exhibit A**, Statement of Work; **Exhibit B**, Cloud Service Agreement; **Exhibit C**, Certificate of Insurance; **Exhibit D**, Information Technology Provisions; and **Exhibit E**, Criminal Justice Information Services Security Addendum.

REMAINDER OF PAGE INTENTIONALLY LEFT BLANK

Contract Control Number: TECHS-202580661-00
Contractor Name: NAVIANT, LLC

IN WITNESS WHEREOF, the parties have set their hands and affixed their seals at Denver, Colorado as of:

SEAL

ATTEST:

____

CITY AND COUNTY OF DENVER:

By: ______________________________

APPROVED AS TO FORM:

Attorney for the City and County of Denver

By: ______________________________

REGISTERED AND COUNTERSIGNED:

By: ______________________________

By: ______________________________

Contract Control Number: TECHS-202580661-00
Contractor Name: NAVIANT, LLC

By: DocuSigned by: Jason Bruner
343AB47C5BBD461...

Name: Jason Bruner
(please print)

Title: CFO
(please print)

ATTEST: [if required]

By: ______________________________

Name: ______________________________
(please print)

Title: ______________________________
(please print)

DENVER
THE MILE HIGH CITY

Exhibit A Statement of Work

Planning & Implementation Phase

Public Records Request Platform

Prepared For

Read, Bierbach, Lifecycle Management Program Manager
City and County of Denver

Prepared By

Alex DeLaura, Sales Executive
Jeff Comer, Sales Engineer Manager
Bob Dunn, SVP
Naviant, Inc.

25 July 2025

NAVIANT®

201 Prairie Heights Drive | Verona, WI 53593 · 888.686.4624 · naviant.com
naviant.com/blog Naviant Inc. @NaviantInc Naviant Inc Naviant Inc.

TABLE OF CONTENTS

PROJECT SCOPE

Introduction/Business Problem

Naviant, LLC ("Naviant") has engaged in preliminary discussions with City and County of Denver ("Customer"/CCD) to discuss options and best practices for optimizing Customer's processes via Content Services such as content management, case management, process management, records management, and/or other automation technologies. The current APEX records system used by Denver Police Department (DPD) and Denver Sherriff Department (DSD) for handling records requests is outdated and no longer meets necessary legal and security requirements.

As a result of these discussions, City and County of Denver has requested that Naviant provide solution planning, implementation and/or support services as defined by this Statement of Work (sometimes referred to as a "SOW"). The SOW will reflect the results of the Vendor Risk Assessment (VRA) conducted by CCD's Information Security team. Further, the solution will also go through CCD's Technology Architecture Review (TAR) where the vendor will be required to respond to specific architecture questions and review and scoring of nonfunctional and technical requirements. This SOW will provide a detailed overview of the project elements necessary for this endeavor to be successful. These include but are not limited to the following areas:

- Objectives
- Implementation Schedule
- Key Participants
- Project Approach
- Assumptions and Dependencies
- Requirements
- Risks and Issues
- Deliverables with Acceptance Criteria

Solution planning for this project will be provided through a Planning Phase to define initial requirements, identify design options, and provide a Planning Phase Report. Planning will validate business process options, software licensing, and professional services required to deliver and implement the solution.

Based on preliminary requirements provided by Customer to date, this SOW provides software licenses, related maintenance/support, and professional services estimates for the Customer-requested solution at this time. Upon completion of the Planning Phase, Future State software and professional services will be validated and a mutually-executed upon Change Order may be executed as appropriate.

An overview of the Naviant Methodology is provided in Appendix A of this SOW.

Technology Overview

The software being proposed as a public records request platform is Hyland's OnBase content services platform (https://www.hyland.com/en/government) with a certified-Hyland technology partner, JADU Central, constituent facing landing page (https://www.jadu.net/central) for initiation of the public records request and payment processing. via a centralized shopping cart. This payment functionality is custom programming required by the City and County of Denver (CCD), other efforts associated with this implementation are deemed configuration or out of the box) (OOB) as defined in the requirements traceability matrix (RTM). (Appendix XXX). If Additional custom programming is required, this will be agreed by both parties and documented in the form of a change order.

OnBase

OnBase is a leading platform for government entities that streamlines paper-based processes across the enterprise with a proven solution for each level of government, helping each meet the challenges of smaller budgets and staffs while laying the foundation for simplified, efficient, and mobile government information technology. As the industry-leading solution to government and their constituents, OnBase provides an extensive breadth of solutions including Public Records Request Management, Finance & Administration, Housing & Human Services, Justice & Public Safety, Planning

& Public Works, and Integrations to departmental/agency government applications like Accela, Cityworks, ESRI, and more. OnBase is enterprise-class, content management (ECM) and business process management (BPM) software that combines workflow, document management, imaging, optical character recognition (OCR), case management, and enterprise report management technologies in a single database application. By dynamically organizing and controlling the capture of documents and by interactively managing the business processes in which these documents are used, OnBase enables organizations to streamline their operations and share information among their employees, partners, and customers.

Naviant's dedicated Government solutions (https://naviant.com/solutions/government/) aligns the enterprise flexibility and digital transformation benefits of OnBase with the experience from Naviant's public sector customer partners. Naviant's specialized experiences within the government sector has evolved to provide "OnBase Solutions by Naviant" within the Hyland Platform for federal, state, local, and tribal government streamlining paper-based processes across the enterprise with proven solutions for each level of government, helping each meet the challenges of smaller budgets and staffs while laying the foundation for simplified, efficient, and mobile government information technology.

OnBase is a premier, Tier 1 solution offering the management of virtually every kind of document images, host generated reports, application files, electronic forms, emails, video clips, etc. as well as every stage of the document lifecycle creation/input, storage, retrieval, revision, and distribution. While other software systems take a toolkit approach providing a set of "building blocks" that may include a common front end for interfacing with several separate software packages, OnBase, by contrast, is a single software application that utilizes a single SQL database, a single configuration utility, and a single customizable user interface for all capture, storage, retrieval, processing, management, and security. This unparalleled level of integration enables OnBase to provide an exhaustive amount of out-of-the-box functionality to support the most sophisticated document, content, and workflow management solutions.

OnBase is point-and-click configurable, enabling the rapid deployment of sophisticated solutions without the need for expensive, time-consuming programming or ongoing support complexities. In designing solutions to meet their own unique requirements, customers can select from over 300 OnBase capabilities that provide specialized input, management, processing, and output capabilities. OnBase customers are encouraged to invest in the solution they need today and then incrementally and cost-effectively expand at the appropriate time in the future.

JADU

JADU is a comprehensive, low-code Web Experience Management platform designed to help organizations create and manage accessible, user-centric websites and online forms with accessible designs adhering to WCAG 2.1 AA standards, ensuring inclusivity across devices. It integrates web content management, form building, and customer engagement tools into a unified system, streamlining digital service delivery with a seamless and certified integration to Hyland OnBase.

JADU Central includes a flexible form builder that allows users to create online forms with branching rules and data capture capabilities. These forms can integrate with payment systems, facilitating seamless transactions. The platform emphasizes accessibility, providing fully responsive and accessible site templates and also incorporates robust security measures to protect user data and ensure reliable service delivery.

Naviant has worked with Hyland and JADU to develop a custom JADU integration to Hyland OnBase. In addition, JADU has the capability to integrate with various third-party services, including Office 365 Calendars, Brightly asset management solutions, and ESRI ArcGIS maps, enhancing its functionality and adaptability.

Project Objectives

The following business objectives were defined:

- **Enhance efficiency:** Automates processes, reduces manual work, and speeds up request handling.
- **Boost constituent satisfaction:** Simplifies request submissions and improves communication.
- **Faster implementation:** Quick deployment and setup reduce disruption and deliver rapid value opposed to complete custom solution.

- **Increase transparency:** Provides real-time visibility and reporting for improved compliance and trust.
- **Scalability:** Adapts easily to growing volumes and organizational changes.
- **Improve security:** Strengthens data protection and compliance with regulatory standards.
- **Manage all document requests:** The system will handle requests from both DPD and DSD, replacing our current outdated system.
- **Provide a user-friendly interface:** Citizens will be able to easily submit requests and make payments through a "shopping cart" style front end.
- **Securely process payments:** The system will integrate with Euna Payments using the city's enterprise integration system and the approved payment provider, to ensure all payments and financial information are handled securely.

Scope of Work

Customer and Naviant have identified the following high-level Future State objectives for the Implementation Phase of this project, which may include an applicable Change Order Authorization based on the findings from the Planning Phase.

- Front end shopping cart functionality will be designed and implemented in the vendors solution for DPD and DSD. The ECS project team will provide support on all required integrations between the new solution and EUNA payments.
- Backend request system will be configured for DPD and DSD workflows in OnBase. Implementing all necessary business requirements to meet the current system functionality
- Design and implementation of DSD frontend and backend configurations utilizing the previously completed work for DPD. The initial implementation will be specific to DPD, DSD will follow after the implementation for DPD.
- CJIS Compliance- content that requires CJIS compliance will not be stored in OnBase.It will go through redaction and the unredacted version will be deleted in OnBase. The public facing redacted portion will be stored in OnBase.
- Out of scope: Any vendor involvement with Apex legacy data.
- Out of scope: Microsegmentation for Apex Replacement.

Planning Phase high-level activities will include:

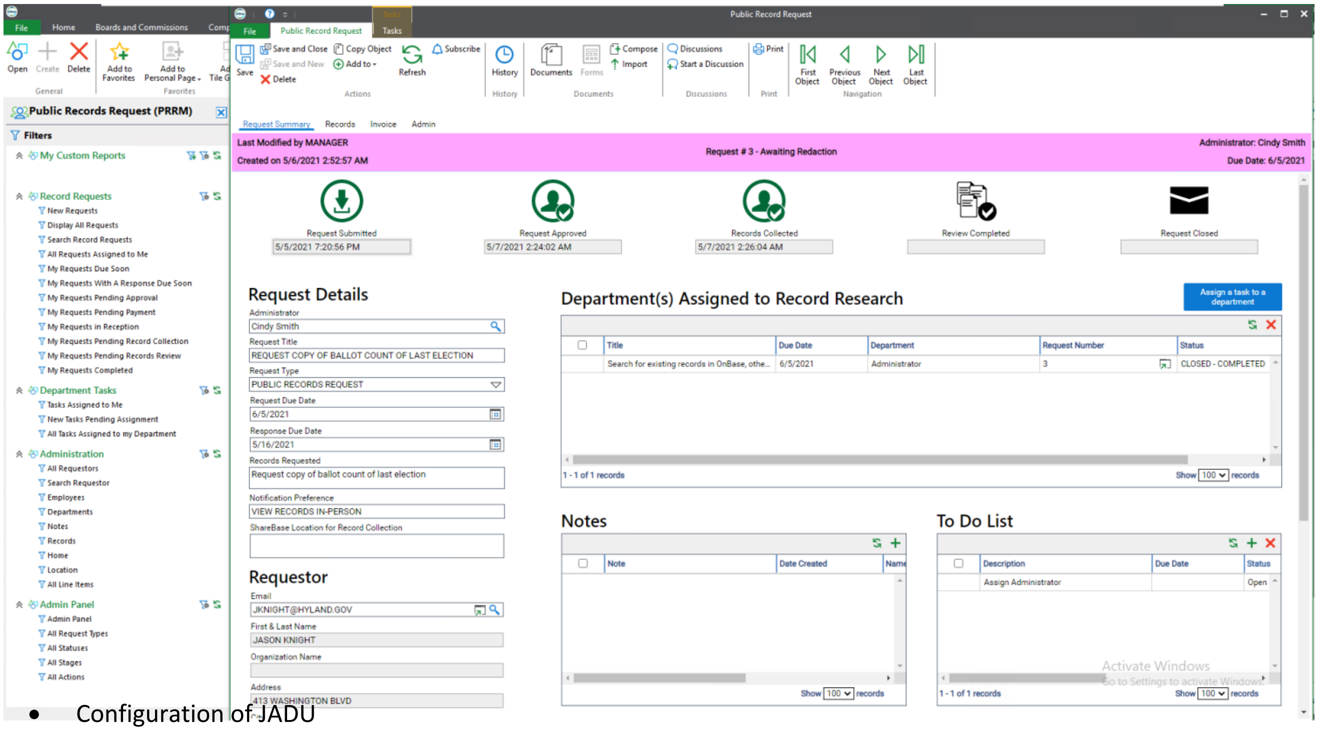
- **Analysis**: Review current state documentation and processes end to end
  - System context diagrams for future state (created collaboratively)
  - Logical Diagrams for Denver Sheriff Department (DSD) and Denver Police Department (DPD) (created collaboratively)
  - Types of documents and data that are being received. for DSD and DPD.
  - Payment Processing Integration options through Mulesoft.
  - Source of content and data for processing including protected data.
  - Identify record request types:
    - 911 Recording
    - Computer Aided Dispatch (CAD) Report
    - Premise History
    - Person Hardcopy
    - Investigation Report
    - Audio- Video Recording, Including Bodycam
    - DUI Room Video
    - HALO/Traffic Cam Video
  - User access, interactions, and security with documents
  - Network infrastructure and technical architecture
  - Integration with Denvergov
  - Integration with email

  - Integration with Federated Authentication, MFA, logging, etc.
  - Requestor document retrieval from OnBase via JADU or email,

- **Design:** Conduct Joint Application Design (JAD) session to validate the future state solution design.
  - Review future state vision considering content services best practices.
  - Review future state configuration and design objectives.
    - Capture (scanning, email)
    - Retrieval (custom queries, Microsoft Outlook)
    - Storage (document type groups, document types, keywords, user groups)
  - Future state solution design
    - Records retention
    - Document reporting requirements (OnBase OOB and OnBase API)
- Validate future state hardware/software requirements and implementation estimates based on Planning Phase
- Prepare Planning Report deliverable.

The following capabilities will be **considered within the scope** of this Implementation estimate, subject to Planning Phase design validation activities:

- Configuration of OnBase's Public Records Request concept solution depicted below
- Development of OnBase Unity form(s) for exposure to Public for new Record Requests
- Implementation of Standard Mailbox Importer functionality
- Workflow/Workview configuration for Records Request (Base Concept Solution):
  - Request Payment Processing Integration (pre-paid or upon completion of request)
  - New Request: Sample Actions (Acknowledge/Deny)
  - Awaiting Assignment: (Assign Department/Assignments Complete)
  - Department Processing: (Send Reminder/Reassign/Request Complete)
  - Compile Results: (Create PDF)
  - Awaiting Information: Waiting for customer supplied information.
  - Deliver Response:(Email Response/Print Response)
  - Recently Completed: (Reuse for new request)



Last Modified by MANAGER

Created on 5/6/2021 2:52:57 AM

Request # 3 - Awaiting Redaction

Administrator: Cindy Smith

Due Date: 6/5/2021

Request Submitted	Request Approved	Records Collected	Review Completed	Request Closed
5/5/2021 7:20:56 PM	5/7/2021 2:24:02 AM	5/7/2021 2:26:04 AM		

Request Details

Administrator: Cindy Smith

Request Title: REQUEST COPY OF BALLOT COUNT OF LAST ELECTION

Request Type: PUBLIC RECORDS REQUEST

Request Due Date: 6/5/2021

Response Due Date: 5/16/2021

Records Requested: Request copy of ballot count of last election

Notification Preference: VIEW RECORDS IN-PERSON

ShareBase Location for Record Collection:

Requestor

Email: JKNIGHT@HYLAND.GOV

First & Last Name: JASON KNIGHT

Organization Name:

Address: 413 WASHINGTON BLVD

Department(s) Assigned to Record Research

☐	Title	Due Date	Department	Request Number	Status
	Search for existing records in OnBase, othe...	6/5/2021	Administrator	3	CLOSED - COMPLETED

1 - 1 of 1 records Show 100 records

Notes

☐	Note	Date Created	Name

Show 100 records

To Do List

☐	Description	Due Date	Status
	Assign Administrator		Open

1 - 1 of 1 records Show 100 records

- Configuration of JADU

  - Link to Existing Website
  - OnBase Integration
  - Payment Workflow to Customer's Payment Processing Platform (EUNA)
  - Form / Path creation - up to ten (10) forms
- Testing / Training
  - Create test plan to include:
    - Unit Testing
    - System/Integration Testing
    - User Acceptance Testing
  - Create training plan
- Communication/Change Management Process (collaboratively)
  - Create communication plan
  - Create change management plan

Naviant has the ability and willingness to utilize the service, functions, and components of the City's Enterprise Cashiering System (ECS) to process user payments via API integration. This means that all payment processing will be handled by CCD's payment platform. Naviant affirms that with access to Customer's ECS expertise for co-development of the integration, their software can support this requirement.

Note: A change order will be required for work effort associated with the updates to the base concept solution and additional JADU customizations.

Project Deliverables

The following are project deliverables that are provided to the Customer during the phases outlined below:

Planning Phase

Agenda for Kickoff Meeting

Planning Phase Project Plan

Planning Phase Report

Implementation Phase

- Agenda for Kickoff Meeting
- Implementation Phase Project Plan
- Functional Specifications
- Solution Demonstration
- Train-the-trainer materials & training
-

Assumptions

- CCD, Vendor, and any necessary contractors/contingency workers will have the availability, skills, and tools necessary to deliver the scope of this project within the estimated duration outlined in the approved, baselined project schedule.
- CCD, Vendor, and any necessary contractors/contingency workers will deliver a high-quality Solution integrated application that meets or exceeds CCD's requirements and the objectives outlined in this SOW, the Solution Design Document as well as any supporting project documents.
- During User Acceptance Testing CCD agency users will competently execute the test cases they are assigned and be responsible for approving or reporting defects and re-testing all assigned test cases.
- The following CCD agencies are expected to use the Solution integrated application:
  - Department of Safety (Denver Police Department and Street Enforcement Team and Denver Sherriff Department)

Dependencies

- ECS team and EUNA systems.

- Solution training alone will not necessarily support proper use of the new application.
- Organization Change Management activities will be required by the CCD agencies using Solution to ensure the application is embraced and properly used by the end users.

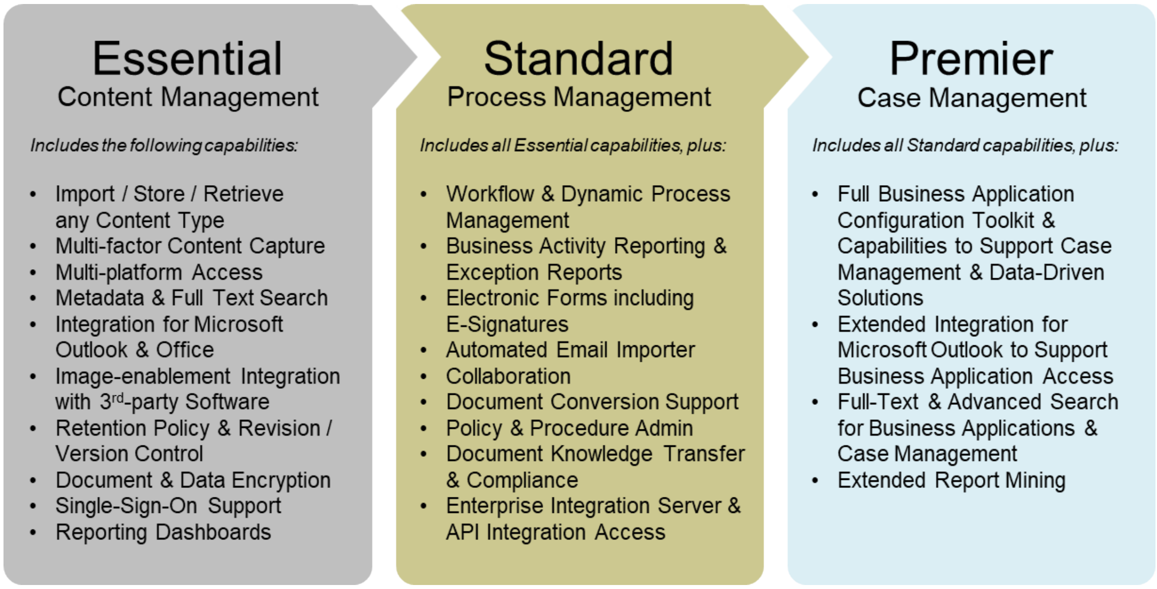
OnBase Simplified Subscription Licensing

The OnBase Simplified Subscription Licensing option provides Simplified Base Packages (Essential, Standard, and Premier) which contain universal licenses to align with industry-leading solutions and to serve as a foundation of this platform. As an annual subscription model, these Packages are tiered functionally in a "good, better, best" structure, and Customers are entitled to purchase the quantity of users they need from any combination of the Package tiers.

- **Essential** provides all of the essential content management capabilities, perfect for anyone interacting with content as part of their daily work
- **Standard** provides everything in Essential, plus workflow and other process management capabilities
- **Premier** provides everything in Standard, plus business applications and case management capabilities

In addition to Full-Time Named User licenses, Concurrent User licenses are available for users that will access the platform on a less frequent or shared basis. Concurrent Users maintain full Package functionality and provide use of the platform through a pool of licenses shared across a group of potential users.

In addition to the Simplified Base Packages, Add-On Packages are available for common Horizontal and Industry-Specific capabilities such as Advanced Capture, Document Composition, and Agenda Management, including Purpose-Built, certified integration capabilities such as SAP, Oracle, Workday, DocuSign, Esri, and others.



Essential
Content Management

Includes the following capabilities:

- Import / Store / Retrieve any Content Type
- Multi-factor Content Capture
- Multi-platform Access
- Metadata & Full Text Search
- Integration for Microsoft Outlook & Office
- Image-enablement Integration with 3rd-party Software
- Retention Policy & Revision / Version Control
- Document & Data Encryption
- Single-Sign-On Support
- Reporting Dashboards

Standard
Process Management

Includes all Essential capabilities, plus:

- Workflow & Dynamic Process Management
- Business Activity Reporting & Exception Reports
- Electronic Forms including E-Signatures
- Automated Email Importer
- Collaboration
- Document Conversion Support
- Policy & Procedure Admin
- Document Knowledge Transfer & Compliance
- Enterprise Integration Server & API Integration Access

Premier
Case Management

Includes all Standard capabilities, plus:

- Full Business Application Configuration Toolkit & Capabilities to Support Case Management & Data-Driven Solutions
- Extended Integration for Microsoft Outlook to Support Business Application Access
- Full-Text & Advanced Search for Business Applications & Case Management
- Extended Report Mining

Hyland Cloud

The Hyland Cloud (https://www.hyland.com/en/innovation/hyland-cloud) a secure, privately managed cloud platform that is custom-designed to host Hyland content services solutions. Leveraging a sophisticated multi-cloud architecture, the Hyland Cloud delivers multi-instance and/or multi-tenant SaaS solutions that are administered, governed, and supported by expert Hyland engineers and available globally. Through strategic collaboration with Amazon Web Services (AWS), Hyland Cloud customers receive enhanced infrastructure backed by innovative technologies and industry-leading security-driven policies to environments in North America on the appropriate AWS region.

Hyland delivers Hyland Cloud solutions through co-located data centers or accredited public data centers, which both meet the highest security standards. Data is protected at every stage – at rest, in use, and in transit ensuring security in every phase of data usage. The Hyland Cloud aligns to leading compliance and security standards including SOC 2, ISO 27001, PCI DSS, and NIST 800-53.

The Hyland Cloud offering includes one (1) User Test Lite environment and one (1) Disaster Recovery environment at no additional cost. Customers may purchase additional User Test Lite environments if required. One (1) TB of storage is the initial allocation for new customers, reported off the Production environment only. Additional storage allocation is purchased as an annual subscription. Please reference the Service Classes Manual for information regarding the three (3) service class options (Gold, Platinum, and Double-Platinum).

Change Orders

This SOW has been prepared in accordance with Naviant's understanding of Customer requirements and the “Project Scope” based on the information provided by Customer to Naviant at this time. Although Naviant makes reasonable attempts to provide accurate estimates, estimates may change as further details of the solution are identified and the final Solution Design is developed. In the event that additional products and/or services beyond those outlined in this SOW are required, a “Change Order Authorization” will be generated outlining the details, as well as time and cost estimates, of the modifications to this SOW. A Change Order Authorization must be authorized, approved, and executed by Naviant and Customer in order for the modifications to be incorporated into the SOW.

In order to ensure that assignments are carried out in a timely manner so as not to impact the project schedule, Customer is responsible for directing the work assigned to its staff and 3rd party service providers. In the event that the SOW project schedule is delayed or needs to be extended due to a failure of Customer’s staff and/or 3rd party service providers to complete assigned work in a timely manner, Naviant shall be entitled to an extension of time and/or cost impact as set forth in a Change Order Authorization.

PROJECT PRICING

Year 1 Pricing:

Software Subscription & Support			
Description	**Part # / Notes**	**Qty**	**Total**
OnBase Premier Named User License	ONB-SAAS-KW-GL	25	$48,000
Hyland Cloud Storage	HYCLD-STRG-TB	1 TB	$1,800
OnBase Integration for Hyland Content Portal for Local Government - Mega Jurisdiction - Up to 10 Forms	HCPLGI1-MG_SAAS		$32,900
Hyland Content Portal for Local Government - Mega Jurisdiction - Up to 10 Forms	HCPLG1-MG_SAAS		$57,200
Hyland Content Portal Payment Connector	HCPPC1_SAAS		$6,700
Software Support Level Agreement	SLA		$17,592
Subtotal			**$164,192**

Professional Services			
Description	**Days Low**	**Days High**	**Total**
Professional Services	89	112	$156,120 - $196,360
Post-Production Monitoring & Assistance	5	7	$12,320 - $17,600
Subtotal			**$168,480 - $213,960**

Years 2-5 Pricing:

	Year 2	Year 3	Year 4*	Year 5*
OnBase / JADU Subscription	$157,595	$169,414.63	$182,120.72	$195,779.76
Support Level Agreement	$18,911.40	$20,329.76	$21,854.49	$23,493.57
Total	**$176,506.40**	**$189,744.38**	**$203,975.21**	**$219,273.35**

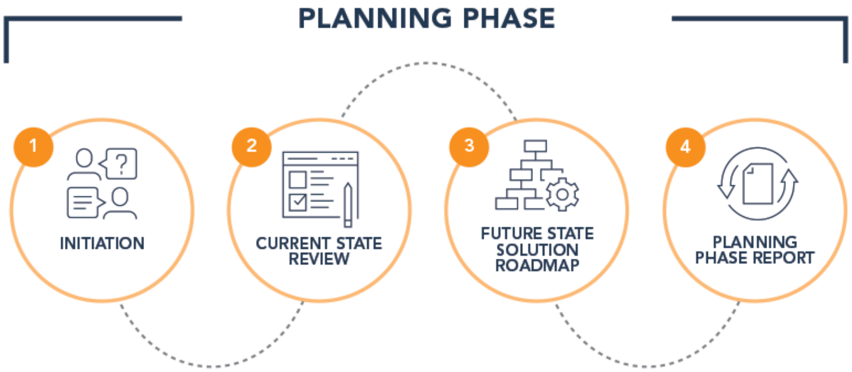
*Years 4& 5 outside standard term and are listed as optional renewals

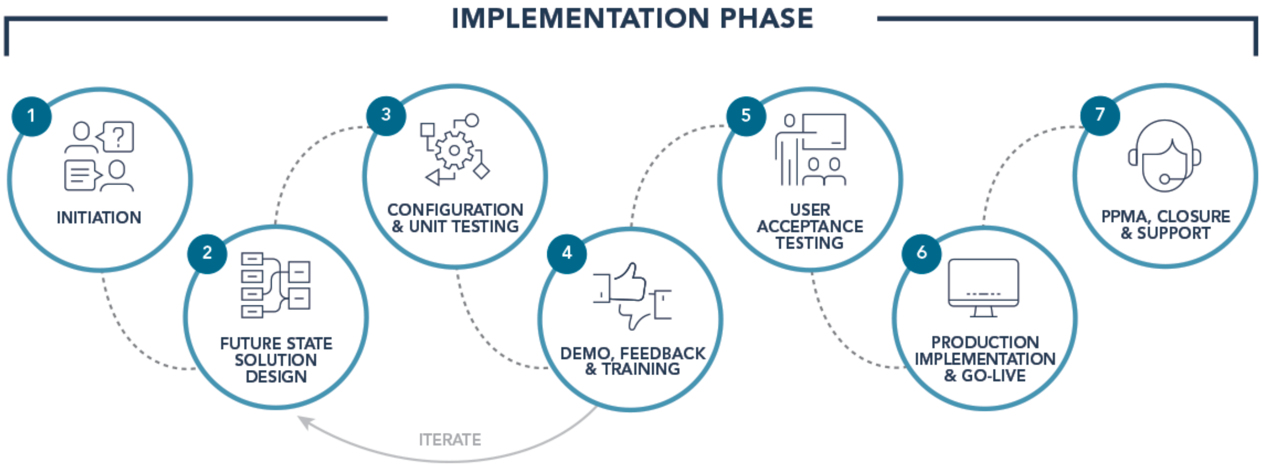
1. Software Subscription & Support will be invoiced upon receipt of Customer-executed SOW, and if applicable, Customer-required Purchase Order, with payment terms consistent with the Master Terms & Agreement.
2. For new Customers, the Software Subscription & Support term will start upon receipt of Customer-executed SOW and End User License Agreement ("EULA"), and if applicable, Customer-required Purchase Order.
3. City and County of Denver's performance and obligation to pay under this Contract is contingent upon an annual appropriation by the Legislature.
4. Please note, subtotals do not include applicable sales tax. If applicable, sales tax will be assessed during the course of the project and/or on the final invoice.
5. Customer agrees to abide by the provisions set forth in the Software Support Level Agreement (SLA Provisions).

APPENDIX A – NAVIANT PROJECT METHODOLOGY

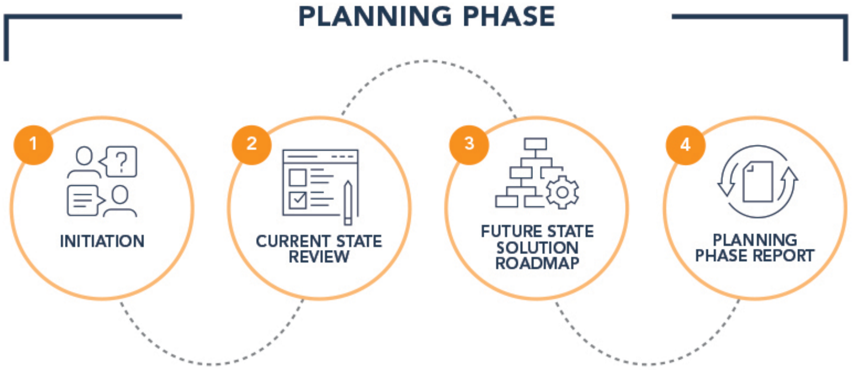
Naviant Methodology Overview

The Naviant Methodology consists of two phases, the Planning Phase and the Implementation Phase. It is designed to ensure timely and effective delivery of Content Services solutions that meet our Customer's requirements and are aligned with their strategy, vision, and objectives.




IMPLEMENTATION PHASE
1
INITIATION
2
FUTURE STATE SOLUTION DESIGN
3
CONFIGURATION & UNIT TESTING
4
DEMO, FEEDBACK & TRAINING
ITERATE
5
USER ACCEPTANCE TESTING
6
PRODUCTION IMPLEMENTATION & GO-LIVE
7
PPMA, CLOSURE & SUPPORT

Planning Phase



The Planning Phase (sometimes referred to as "Discovery") is generally a relatively short engagement consisting of four (4) primary steps designed to gain a high-level understanding of the project objectives, requirements, and costs. This information is documented in a Planning Phase Report deliverable to present a common vision of the final project to all stakeholders and also serves both as a financial decision point as well as the primary input into the Implementation Phase.

Overall Planning Phase Responsibilities

Naviant

- Identify Naviant Planning Phase Team and commit resources.
- Work with the Customer Project Manager to develop the Planning Phase Project Plan.
- Prepare the Planning-Phase Onsite Agenda and deliver to Customer in advance of the Kickoff Meeting.

Customer

- **Identify the Project Sponsor** - The Project Sponsor is the individual that has ultimate authority over the project, is involved in the project, and is the final escalation point for all issues, scope changes, and decisions. The Project Sponsor also provides project funding, approves major deliverables, and provides high-level direction. This person will champion the project with internal and external stakeholders and ensure that the appropriate personnel are made available to execute the project successfully.
- **Identify the Project Lead -** The Project Lead is the individual that is responsible for project management activities including:
    - Working with Naviant's Project Manager to develop the Planning Phase Project Plan.
    - Coordinating project activities with the Naviant Project Manager and/or the Lead Naviant Consultant.
    - Ensuring Customer resource availability.
    - Tracking of Customer-assigned tasks.
    - Managing of Customer communication and status reporting.
    - Coordinate logistics for Naviant and other non-Customer team members (meeting rooms, remote access, etc.).
    - Create all Customer required documentation and ensure timely internal signoffs.
    - Commit and confirm that Project Team resources (Project Sponsor, Project Lead, Subject Matter Experts (SMEs), IT resources) will be available as needed for project sessions and activities.
    - Ensure CCD PMO phase gates and deliverables and change management are met.
- Secure meeting rooms for all onsite Planning Phase activities. Meeting rooms should be large enough for all onsite attendees and include the following:
    - Available telecommunications equipment as needed for remote attendees.
    - A projector or television monitor.
    - A whiteboard that may be used in addition to any projection equipment.

Initiation

Pre-Engagement Questionnaire

Prior to the Project Kickoff Meeting, Naviant may provide Customer with a Pre-Engagement Questionnaire. This questionnaire may be used to establish an understanding of the current work environment prior to onsite sessions and may include the following areas of focus:

- Processes & Procedures
- Business Challenges & Risks
- Key Process Measures & Metrics
- Relevant Organizational Charts
- User Population & Distribution
- IT Infrastructure
- Test Environment Requirements
- Other, TBD

Note: The Pre-Engagement Questionnaire is only used for certain projects. The Naviant Project Manager will advise if a questionnaire is required.

Pre-Engagement Questionnaire Responsibilities (if utilized)

Naviant

- Prepare and provide the questionnaire to the Customer.
- Review completed questionnaire in advance of the Kickoff Meeting.

Customer

- Assign responsibility, complete the questionnaire, and return to Naviant prior to the Kickoff Meeting.

Planning Phase Kickoff Meeting

A formal Planning Phase Kickoff Meeting will be held and usually takes anywhere between thirty (30) minutes to two (2) hours, depending on the project complexity. The topics for the meeting may vary but typically include the following:

- Project Team Member Introductions & Roles
- Review of the Statement of Work
- Confirmation of Project Objectives & Timelines
- Communication Planning
- Planning Phase Logistics

Planning Phase Kickoff Meeting Responsibilities

Naviant

- Ensure that relevant Naviant team members attend the Kickoff Meeting.
- Facilitate the meeting.

Customer

- Ensure that the Project Sponsor, Project Lead, and all other relevant Customer Project Team Members attend the Kickoff Meeting.

2 CURRENT STATE REVIEW

Current State Review

In order to design a Future State solution based on each Customer's needs and objectives, it is necessary to gain a thorough understanding of the Current State environment. This is accomplished through a series of working sessions with various Subject Matter Experts (SMEs) including process owners and knowledge workers. Various techniques may be utilized to gather information including verbal descriptions, Customer-generated documentation, and/or live walk-throughs. Information on Current State systems' architecture/infrastructure will also be collected in this step, as appropriate.

Current State Review Responsibilities

Naviant

- Review any Current State process documentation prepared and/or submitted by Customer in advance of the onsite activities.
- Facilitate the Current State Review session(s).
- Capture relevant Current State details for inclusion in the Planning Phase Report.
- Capture thoughts and ideas for consideration in the Future State Solution Roadmap

Customer

- Provide relevant Current State process documentation.
- Assign appropriate SMEs to attend and present relevant Current State information.
- Be prepared to discuss any business challenges and opportunities for consideration in the Future State Solution Roadmap.

3 FUTURE STATE SOLUTION ROADMAP

Future State Solution Roadmap

Future State Solution Roadmap is accomplished through Naviant-facilitated Joint Application Design (JAD) sessions with relevant project team participants including the Project Sponsor, Project Lead, Subject Matter Experts, Process Managers, IT Resources, and/or other resources as appropriate.

The primary objectives of this step include:

- Providing the Customer with an overview and understanding of the technology platforms that may be included as part of the solution.
- Identifying process automation opportunities and documenting the solution scope.
- Defining a list of Use Cases (both Primary and Alternate) to be included in the solution scope.
- Discussing and capturing sufficient requirements detail to estimate the Implementation Phase work effort as accurately as possible. *Note: A detailed solution design may be deferred until the Implementation Phase.*

Future State Solution Roadmap Responsibilities

Naviant

- Facilitate the Future State Solution Roadmap session(s).
- Provide technology overviews and/or demos, as appropriate.

- Capture identified Future State Use Cases, Requirements, Risks, Action Items, and other notes during the session(s).

Customer

- Ensure appropriate Customer resources are available to participate in the session(s) with minimal interruptions.
- Ensure Customer attendees individually or collectively have Future State decision making authority.
- Provide any additional information/documentation as requested/required for Future State needs.

4

PLANNING PHASE REPORT

Planning Phase Report

The final step of the Planning Phase is the creation, delivery, review, and finalization of the Planning Phase Report. A draft of the report will be delivered to the Customer in PDF format. After an appropriate review period, a review meeting will be conducted (normally via remote web conference) to review any Customer feedback and/or questions. Naviant will then update the report with any required changes and deliver a final copy of the Planning Phase Report to the Customer.

While the content may vary based on the project scope and requirements, a typical Planning Phase Report may include the following:

- An overview of the project, scope, and Planning Phase participants.
- A summary of the Current State information relevant to the Future State solution.
- A high-level Future State Solution Roadmap containing the defined Use Cases as well as any requirements gathered during the Planning Phase.
- A list of the software/modules required for the Future State solution.
- Estimated project pricing including professional services and any required software and/or hardware.
- A Work Breakdown Structure (WBS) identifying the tasks required to successfully implement the project (as applicable)

Planning Phase Report Responsibilities

Naviant

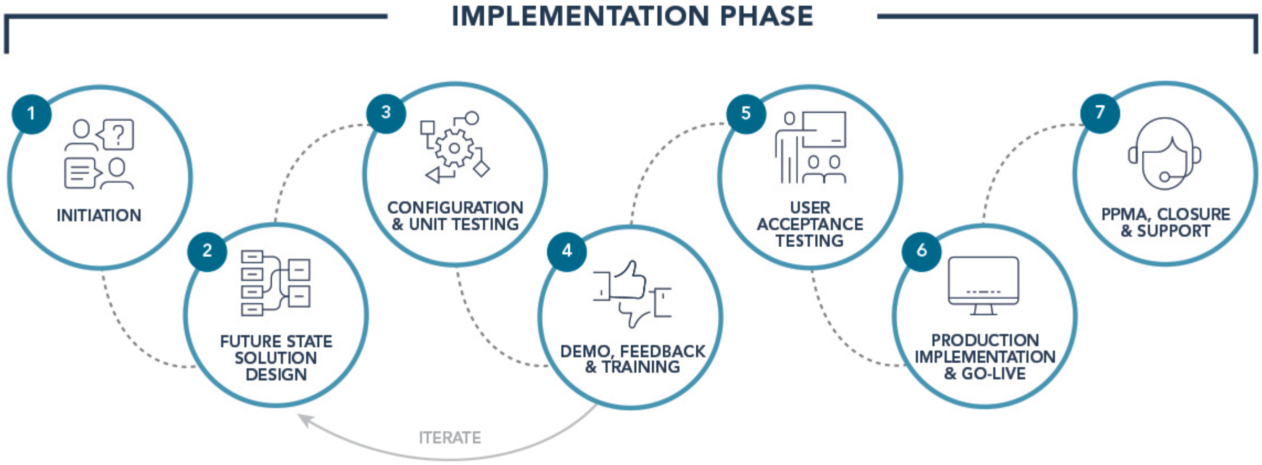
- Create and deliver to Customer a draft copy of the Planning Phase Report.
- Work with Customer to schedule the Planning Phase Report Review Meeting.
- Facilitate the Planning Phase Report Review Meeting.
- Update the Planning Phase Report as appropriate based on the outcomes of the Planning Phase Report Review Meeting.
- Deliver a final copy of the Planning Phase Report.

Customer

- Work with Naviant to schedule the Planning Phase Report Review Meeting.
- Review the draft copy of the Planning Phase Report and be prepared to discuss any questions/feedback in the Planning Phase Report Review Meeting.
- Sign-off on the Planning Phase Report.

Delivery of the final copy of the Planning Phase Report by Naviant to the Customer marks the formal end of the Planning Phase.

Implementation Phase


IMPLEMENTATION PHASE
1
INITIATION
2
FUTURE STATE SOLUTION DESIGN
3
CONFIGURATION & UNIT TESTING
4
DEMO, FEEDBACK & TRAINING
5
USER ACCEPTANCE TESTING
6
PRODUCTION IMPLEMENTATION & GO-LIVE
7
PPMA, CLOSURE & SUPPORT
ITERATE

The Implementation Phase consists of seven (7) primary steps with multiple Iterations of design, configuration, and feedback (steps I2 through I4). This iterative model provides the stakeholders an understanding of the project deliverables and gives them an opportunity to provide feedback and request changes prior to User Acceptance Testing.

Overall Implementation Phase Responsibilities

Naviant

- Assign the Naviant Project Manager serving as the primary Customer contact with responsibilities:
  - Overall project management and execution.
  - Managing project budget, tasks, issues, and risks.
  - Coordinating meetings and status reports with Customer Project Lead.
  - Managing Naviant resources and schedules.
- Identify Naviant Implementation Phase Team and commit resources.
- Work with Customer Project Manager to develop the Implementation Phase Project Plan.
- Prepare the agenda(s) and deliver to Customer in advance of the Meetings.

Customer

- **Identify the Project Sponsor** - The Project Sponsor is the individual that has ultimate authority over the project, is involved in the project, and is the final escalation point for all issues, scope changes, and decisions. The Project Sponsor also provides project funding, approves major deliverables, and provides high-level direction. This person will champion the project with internal and external stakeholders and ensure that the appropriate personnel are made available to execute the project successfully.
- **Identify the Project Lead** - The Project Lead is the individual that is responsible for project management activities including:
  - Working with Naviant Project Manager to develop Implementation Phase Project Plan.
  - Coordinating project activities with the Naviant Project Manager and/or the Lead Naviant Consultant.
  - Ensuring Customer resource availability.
  - Tracking of Customer-assigned tasks.
  - Managing Customer communication and status reporting.
  - Coordinate logistics for Naviant and other non-Customer team members (meeting rooms, remote access, etc.).
  - Create all Customer required documentation and ensure timely internal signoffs.
  - Commit and confirm that Project Team resources (Project Sponsor, Project Lead, Subject Matter Experts (SMEs), IT resources) will be available as needed for project sessions and activities.

- **Identify the Project Champion** - The Project Champion is an advocate for the project that has direct lines of communication to the Project Sponsor and/or key stakeholders. This position provides oversight on the project by removing blockers and ensuring the Customer is in a position to take overall ownership of the solution. This resource would know the decisions made during the JAD sessions, and stays engaged during the entire project.
- **Identify the Integration Lead** - As needed, projects with multiple integrations benefit from a dedicated coordinator who manages development, unit testing and support during the project lifecycle.
- As part of the planning and initiative, review the Naviant Roles and Responsibility Matrix and identify additional lead roles as appropriate.
    - Testing Lead
    - Training Lead
    - Infrastructure Lead (network and workstation)
- Verify compliance with minimum server specifications for Development/Test Environments (if required) and Production Environment
- Secure meeting rooms for all onsite Implementation Phase activities. Meeting rooms should be large enough for all onsite attendees and include the following:
    - Available telecommunications equipment as needed for remote attendees.
    - A projector or television monitor.
    - A whiteboard that may be used in addition to any projection equipment.

Initiation

Implementation Phase Kickoff Meeting

A formal Implementation Phase Kickoff Meeting will be held and usually takes anywhere between thirty (30) minutes to two (2) hours, depending on the project complexity. The topics for the meeting may vary but typically include the following:

- Project Team Member Introductions & Roles
- Review of the Preliminary Pricing Estimate
- Review of the Planning Phase Report, as appropriate
- Confirmation of Project Objectives & Timelines
- Communication Planning
- Implementation Phase Logistics

Implementation Phase Kickoff Meeting Responsibilities

Naviant

- Ensure relevant Naviant team members attend the Kickoff Meeting.
- Facilitate the meeting.

Customer

- Ensure the Project Sponsor, Project Lead, and all other relevant Customer Project Team Members attend the Kickoff Meeting.

2 FUTURE STATE SOLUTION DESIGN

Future State Solution Design

Future State Solution Design is accomplished through Naviant-facilitated Joint Application Design (JAD) sessions with relevant project team participants including the Project Sponsor, Project Lead, Subject Matter Experts, Process Managers, IT Resources, and/or other resources as appropriate. This typically occurs onsite at the Customer location.

Similar to the JAD session(s) held in the Planning Phase, the Implementation Phase JAD sessions will focus on defining and documenting all remaining use case and requirements detail.

Primary Objectives

1. Finalizing the complete list of Use Cases (both Primary and Alternate) included in the solution scope for the current Iteration.
2. Finalizing and capturing all detailed and necessary requirements included in the solution scope for the current Iteration.
3. Creating and/or updating the Functional Specifications.

Future State Solution Design Responsibilities

Naviant

- Facilitate the Future State Solution Design session(s).
- Capture identified Future State Use Cases, Requirements, Risks, Action Items, and other notes during the session(s).
- Create and/or update the Functional Specifications.

Customer

- Ensure appropriate Customer resources are available to participate in the session(s) with minimal interruptions.
- Ensure that Customer attendees individually or collectively have Future State decision making authority.
- Provide any additional information/documentation as requested/required for Future State needs.

3 CONFIGURATION & UNIT TESTING

Configuration & Unit Testing

In this step, the Functional Specifications are used as input to architect and complete the technical design of the solution, as well as complete any configuration, development, and unit testing within scope for the current Iteration. Activities in this step are typically completed remote; however, resources may need to be onsite at Naviant's discretion.

Configuration & Unit Testing Responsibilities

Naviant

- Architect and complete the technical design of the solution based on the Functional Specifications.
- Configure, develop, and unit test solution components in scope for the current Iteration.

Customer

- Verify that basic equipment needs for deployment into Customer’s environment (development, test, and production) have been provided to Naviant (database server, file server with ample storage, web server if applicable, security, network’s ability to handle incoming traffic, Customer machines, etc.).
- Ensure that Naviant has remote access to the Customer development, test, and production environments, as appropriate.
- Ensure that SMEs are available to answer questions in a timely manner.
- Conduct, coordinate, and unit test any additional development efforts not being conducted by Naviant. This may include Integrations.

4 DEMO, FEEDBACK & TRAINING

Demo, Feedback & Training

Upon the completion of each Iteration (steps I2 through I4), Naviant will facilitate a demonstration of the solution components configured in the current Iteration. This session is critical to ensuring that stakeholders have a thorough understanding of the solution as well as an opportunity to provide feedback and request changes prior to User Acceptance Testing.

Naviant utilizes a train-the-trainer methodology to facilitate end user training. Once the Customer has identified the lead trainer and lead testers that will participate in the training session, Naviant will align expectations regarding the training materials and the audience for the train-the-trainer sessions. Prior to the scheduled training sessions, Naviant will provide training documentation for common functionality in addition to documentation created specifically for the Customer. Naviant will then lead a training session with the customer’s pre-identified team. This session will provide the Customer with hands on experience working through specific use cases and the opportunity to leverage training materials and ask questions. The training documentation can then be adapted and used by the Customer to train their end-users.

Prior to the training, an environment strategy should be finalized. Typically, multiple OnBase environments are utilized prior to production to allow for testing and training activities.

Demo, Feedback & Training Responsibilities

Naviant

- Prepare the demonstration script.
- Prepare the non-production environment for the demonstration.
- Facilitate the demonstration and Feedback Session.
- Capture any outcomes and update the Functional Specifications as appropriate.
- Prepare training materials for Customer lead trainers and testers.
- Conduct train-the-trainer session for Customer lead trainers and testers to Kickoff testing.

Customer

- Ensure that all appropriate Customer resources attend and participate in the demonstration and Feedback Session.
- Complete any follow-ups and/or action items that come out of the session in a timely manner.
- Define participants (Customer lead trainers and testers) for Naviant-led train-the-trainer sessions.
- Customer will be responsible for end-user training after User Acceptance Testing (Step I5).
- Customer will be responsible for the review, update, and distribution of training documentation.

User Acceptance Testing

User Acceptance Testing (UAT) is the responsibility of the Customer. During UAT, the Customer will fully test the system using defined Test Scripts with the objective of accepting the solution as ready for production implementation. Naviant and Customer will work together to facilitate testing and address any open issues.

Customer Training for end-users will take place towards the end of this phase. The Customer is responsible for delivering end-user training to their staff. The Customer is also responsible for updating and distributing training documentation provided by Naviant during the Demo, Feedback & Training (Step I4) for actual use within their environment during training.

User Acceptance Testing Responsibilities

Naviant

- Work with Customer to establish a Test Plan.
- Work with Customer to establish Issue Management Plan including:
    - Method of tracking and reporting on issues
    - Establish agreed upon timeline and method to track progress for Customer questions and issues
- Resolve issues identified as needing resolution prior to production implementation.

Customer

- Assign test team members.
- Develop a Test Plan to ensure proper end-to-end testing of the solution.
- Work with Naviant to:
    - Determine method of tracking and reporting on issues.
    - Establish agree upon timeline and method to track progress.
- Complete Quality Assurance and User Acceptance Testing (UAT) activities in a timely fashion and within the agreed-to timeline as indicated in the Project Plan.
- Report and document any issues found during testing.
- Work with Naviant to review issues and determine resolution.
- Provide solution acceptance (sign-off) indicating readiness for production.
- Customer will be responsible for end-user training prior to starting Production Implementation & Go-Live.
- Customer will be responsible for review, update, and distribution of training documentation from Demo, Feedback & Training.
- Customer will be responsible for reviewing Appendix B Training Resources for additional training opportunities.

Note: Issues are an inevitable part of implementing any solution, and typically, not all issues must be resolved before solution acceptance. Naviant and Customer will work together to review, categorize, and prioritize all issues to determine those that must be fixed before production vs. those that can be resolved in the future.

Production Implementation & Go-Live

Production Implementation encompasses the activities to deploy the solution and make it production-ready before Go-

Live. Activities in this step include defining and executing a production migration plan, ensuring desktop software is deployed on end-user workstations, and basic testing in the production environment to confirm that the migration was successful, and that the solution is fully functional.

Production Implementation Responsibilities

Naviant

- Work with Customer to create and review the Go-Live Plan.
- Migrate the solution from the previous environment into production.
- Work with Customer to validate production environment functionality.

Customer

- Work with Naviant to create and approve the Go-Live Plan.
- Ensure desktop software is deployed to all end-user workstations.
- Work with Naviant to validate production environment functionality.
- Coordinate the migration of any development not delivered by Naviant.

Production Go-Live

Production Go-Live is the point during which the solution is first utilized in a production capacity. The Naviant Project Team will provide a period of Go-Live Support during this phase. Naviant Go-Live Support is the stabilization period right before and immediately after project Go-Live which focuses on customer support, best practices, and system availability. The Naviant project team will provide technical and process support to the Customer's Go-Live project team. The team will leverage Business Process Management (BPM) and technical knowledge and experience from the Naviant deployment and support teams to answer all questions and resolve all issues in a timely and effective manner. Go-Live Support will aid the Customer's project team in technical issue resolution and system use.

The Implementation Plan will specify the timing of Go-Live activities, and how Go-Live is executed. Naviant and the Customer will work together to determine the best method for Go-Live, including the following considerations:

- Stages/phases of rollout (i.e. whether the entire solution Go-Live at one time, or implemented over time by process, user group, etc.)
- How in-process work/transactions will be managed (i.e. converted into the new solution or completed via the old process/solution.)

Production Go-Live Responsibilities

Naviant

- Naviant provide Go-Live support.

Customer

- Ensure that personnel are trained and ready to use the new solution.
- Execute any procedures to manage work-in-process (if Customer-responsibility).

7

PPMA, CLOSURE & SUPPORT

PPMA, Closure & Support

Post Production Maintenance Assistance ("PPMA") affords dedicated project hours that may be utilized to provide process enhancement and design changes that are requested by the Customer after Go-Live. Naviant will provide process, development and technical support to the Customer's project team. The overall objective of PPMA is to work with each Customer, onsite or remote as applicable, to provide an opportunity for continuous process improvement and to ensure that the solution will be utilized efficiently.

PPMA Responsibilities

Naviant

- Assign Project Team resources to work with Customer on any enhancements and design changes needed for effective use of the solution.

Customer

- Execute/utilize the full scope of the solution as timely as possible/appropriate.
- Provide feedback on the solution to Naviant, including aspects that may need enhancement during the PPMA period.

Closure & Support

Once the production environment is fully functional and stabilized, closure activities will occur, including the transition of the solution from the Project Team to the Naviant Support Team.

The Support Phase begins with a Support Kickoff Meeting facilitated by Naviant's Customer Success Team (CST) to review how Customer would engage Naviant for support-related issues. CST will review the different methods for contacting CST, support programs, review authorized support contacts approved by Customer, share issue tracking methodology, training, and learning opportunities.

Software Support Level Agreement (SLA)

Naviant's experienced support team maintains a dedicated help desk to provide the first line of support for all Content Service solution implementations. Naviant Customers are provided with a toll-free number to use when calling in for support and will be connected directly with the help desk technician and the call will be logged into the Naviant support service system. By utilizing this streamlined approach to support, each issue will be responded to and tracked in a timely and efficient way to minimize disruption to both system operation and work processes. Naviant is an industry leader in solutions support and is recognized by Hyland Software as a "Diamond Level Support" provider with a 95%+ customer retention rate for annual support renewals. The SLA provisions are attached herein as Appendix C.

Closure & Support Responsibilities

Naviant

- Project Team conduct a handoff meeting with the Support Team to review the overall solution and ensure support readiness.
- Accept the solution into support according to the Customer's SLA. Please reference Appendix C Naviant Support.
- Conduct the Support Kickoff Meeting.

Customer

- Provide final sign-off and solution acceptance, indicating readiness for the transition to support.
- Define and provide list of staff authorized to contact Naviant CST for support (Authorized Support Contacts).
- Participate in the Support Kickoff Meeting.

APPENDIX B – TRAINING RESOURCES

Naviant is committed to providing your team updates, information, and training in your Content Services solution. In addition to the training provided by the Naviant Implementation Phase team, Naviant recommends Customers to leverage the following additional Training Resources to promote self-sufficiency and encourage continued business and technical advancement. Customers will also receive a Naviant Welcome Guide which highlights the training opportunities provided by Naviant and Hyland Software.

Naviant Trainers

In addition to the train-the-trainer methodology outlined in “Demo, Feedback & Training”, Naviant offers enhanced implementation and configuration-specific training and testing support to help Customers kickstart the training and testing process for additional fees.

Hyland System Administrator Training

One element critical to the success of any solution is the users’ ability to effectively and efficiently work in the software on a daily basis. Hyland offers a wide array of Training courses designed to introduce end users to the basic features and technical resources to support the advanced functionality of a solution. Naviant recommends that at least one individual participate in the Hyland System Administration training class (typically $3,000 per attendee) prior to the system being installed or within six months of installation. The course is designed to introduce new and existing system administrators to the use, maintenance, and administration of Hyland software and provide in-depth, hands-on experience using actual business scenarios. The class also investigates technical support process, effective maintenance strategies, online documentation, and other resources available to Hyland system administrators.

Hyland CommunityLIVE Conference

Hyland's CommunityLIVE Conference (typically $3,000 per attendee for 5 days) will stretch your imagination to the limits as Hyland experts and users from around the globe demonstrate how to achieve more with your current system and how you can be the technology leader in your industry with the latest and greatest Hyland upgrades and enhancements. Innovation, collaboration, and learning opportunities abound within Hyland’s platform portfolio including OnBase, Brainware, ShareBase, Enterprise Search, Medical Imaging, and more! CommunityLIVE offers the following benefits:

- Industry expert led discussions focused on best practices & areas of concern
- 200+ educational sessions & training courses offered
- Over 2,500 attendees to share best practices
- Compelling keynote speakers & networking events

Naviant Summit

Naviant Customers are eligible for complimentary attendance at Naviant’s annual Summit (educational user conference). Naviant's nationally recognized Summit brings together customers, end-users, vendor partners, invited prospects, and Naviant resources to discuss industry trends, learn about new solution offerings, and recognize how to best leverage current investments in content management technologies. The annual Summit focuses on critical business issues, case studies, and solution/industry-focused educational sessions designed to bring increased value to your organization by improving the effectiveness and efficiency of your operations.

Hyland Community

As a Naviant Customer, the Hyland Community site (community.hyland.com) provides access to the global network of other customers, partners, and employees to share points of view, ask questions of subject matter experts, and research business and technical best practices. Resources include detailed product information, industry solutions & special interests, technical & administration content, user interest groups & member events, and more!

Hyland Online Training

As a Naviant Customer, the Hyland Training site (training.hyland.com) provides access to Hyland's Classroom and Online Training Schedules, plus an extensive collection of the industries-best training topics for end-users to explore including:

- New Courses – Latest & greatest training courses
- OnBase End Users – Learn the basics of OnBase customers
- Workflow – Workflow courses for new users & experts
- Brainware – Install & create Brainware projects
- Healthcare – Courses for healthcare solutions
- System Administration – Courses for new & existing system administrators
- WorkView – Case management courses for new users & experts
- Tech Support – Learn techniques for troubleshooting
- Forms – Design, create & manage forms
- Development – Courses for IS & API developers
- Installation – Design & implement Hyland solutions
- Premium Subscription – Optional fee-based online premium subscription to 200+ hours of technical training for your entire team including end users, support, new employees, and experts

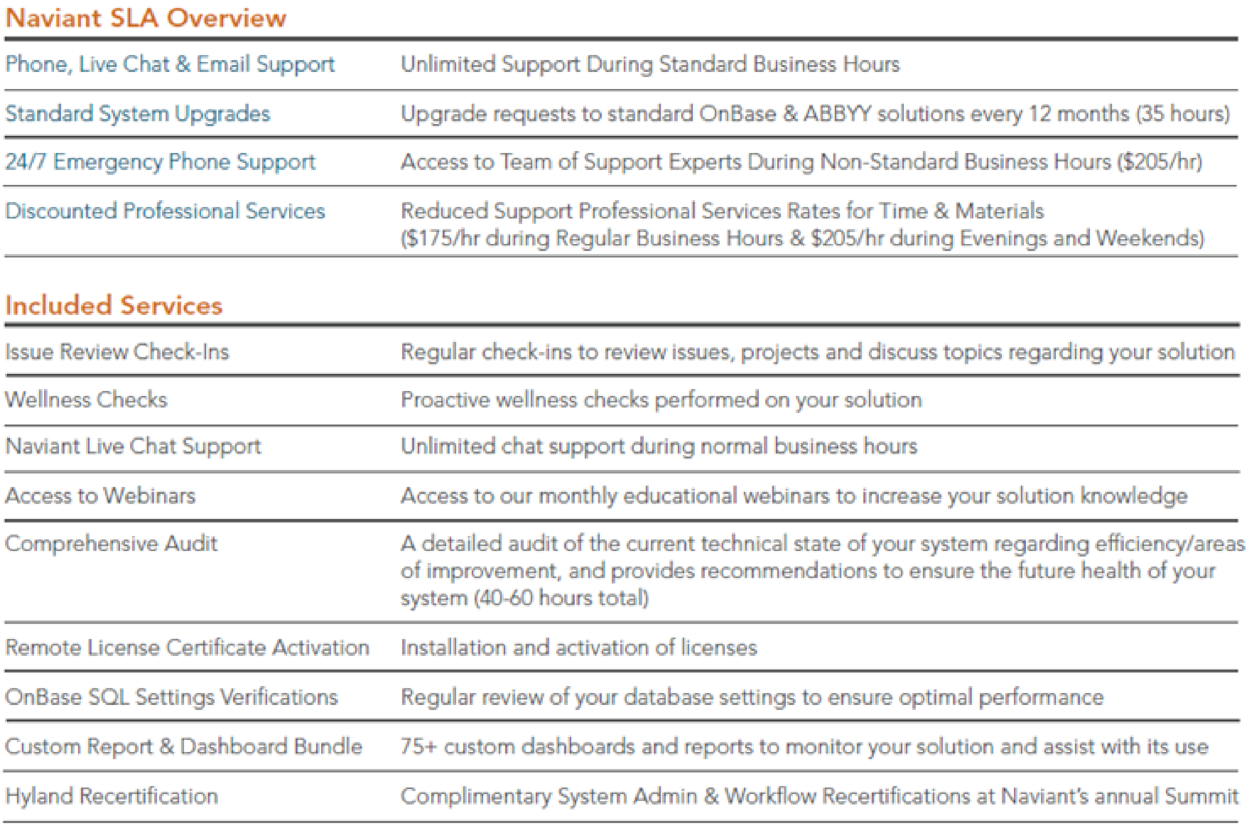
APPENDIX C – NAVIANT SUPPORT

Support Level Agreement

1. Naviant Software Support Level Agreement

Naviant, Inc. ("Naviant") agrees to provide and the Customer agrees to accept ongoing system support on the software products utilized in customer's system at the annual charges as invoiced, in accordance with the terms and conditions contained within these SLA Provisions. A Software Support Level Agreement will provide phone, remote access, and email support for issues related to the performance of the installed system. Naviant standard business hours are 7:00 AM – 7:00 PM CT Monday through Friday, excluding holidays observed by Naviant.

Naviant's Weekly Evening Hours are 7:00 PM – 7:00 AM CT Monday evening through Friday morning. Weekend Hours are 7:00 PM – 7:00 AM CT Friday evening through Monday morning. When Time & Materials billing is applicable, actual and reasonable travel expenses (mileage, transportation, lodging, and meals) will be charged per visit per Naviant resource to the customer as incurred, and Naviant will estimate such fee prior to dispatching onsite support. Naviant's Software Support Level Agreement is outlined below:



Naviant SLA Overview

Phone, Live Chat & Email Support	Unlimited Support During Standard Business Hours
Standard System Upgrades	Upgrade requests to standard OnBase & ABBYY solutions every 12 months (35 hours)
24/7 Emergency Phone Support	Access to Team of Support Experts During Non-Standard Business Hours ($205/hr)
Discounted Professional Services	Reduced Support Professional Services Rates for Time & Materials ($175/hr during Regular Business Hours & $205/hr during Evenings and Weekends)

Included Services

Issue Review Check-Ins	Regular check-ins to review issues, projects and discuss topics regarding your solution
Wellness Checks	Proactive wellness checks performed on your solution
Naviant Live Chat Support	Unlimited chat support during normal business hours
Access to Webinars	Access to our monthly educational webinars to increase your solution knowledge
Comprehensive Audit	A detailed audit of the current technical state of your system regarding efficiency/areas of improvement, and provides recommendations to ensure the future health of your system (40-60 hours total)
Remote License Certificate Activation	Installation and activation of licenses
OnBase SQL Settings Verifications	Regular review of your database settings to ensure optimal performance
Custom Report & Dashboard Bundle	75+ custom dashboards and reports to monitor your solution and assist with its use
Hyland Recertification	Complimentary System Admin & Workflow Recertifications at Naviant's annual Summit

If a Software Support Level Agreement is not purchased or kept in force, all support requests not covered by the Manufacturer Software Maintenance will be billed at Naviant's then prevailing Professional Services rates. Professional Services will be billed at ¼ hour increments.

2. Manufacturer Software Maintenance

In general, "Manufacturer Software Maintenance" provides access to product upgrades & enhancements, product error correction & fixes, technical documentation, and access to manufacturer escalated technical support facilitated through Naviant. When purchased, Manufacturer Software Maintenance provides Customer ongoing software support by the software manufacturer including commercially reasonable efforts to correct any properly reported errors in the software that are confirmed by the software manufacturer in the exercise of its commercially reasonable judgment. Access to Manufacturer Software Maintenance is provided by Naviant. Naviant will undertake to report to the software manufacturer for confirmation any reported errors promptly after receipt of proper notice from Customer, and will perform services in an effort to correct confirmed errors promptly after making such confirmation as directed by the software manufacturer. Manufacturer Software Maintenance provides software maintenance and troubleshooting for product error correction and related fixes coordinated or facilitated through Naviant via phone or email for issues not caused by Customer actions, inactions, hardware, or non-Naviant supplied or supported software. Requests for intervention from the software manufacturer will be at the discretion of Naviant.

3. SLA Upgrades

Customers who have a current SLA are eligible for a complimentary SLA upgrade of up to two versions of their OnBase or Abbyy solution once every twelve (12) months. This upgrade consists of one development environment, one testing environment, and one production environment (up to 35 hours of upgrade services). Customers can request an SLA upgrade during their contract term and Naviant will coordinate based on current project scheduling for Customer. Additional environments, environment refreshes, updates to custom/legacy forms, scripts and workflows are outside scope of this SLA upgrade. Upgrading greater than two versions may incur an additional charge. Additionally, products outside OnBase and Abbyy are excluded. Customer is responsible for all user/client/workstation upgrades, configuration changes, and/or installations as appropriate. Hours dedicated for SLA upgrade cannot be used for any other professional services.

4. Naviant Software Support Protocol

Naviant maintains a dedicated help desk to provide the first line of support to receive and resolve support inquiries for all software solution implementations. By utilizing this streamlined approach to support, Naviant ensures that each customer inquiry will be answered in a timely and efficient manner, minimizing disruption to both system operation and work processes, and that all issues are reported and tracked accordingly. Naviant customers are provided with a dedicated toll-free number to use when calling in for support, as well as a dedicated support email address to email support inquiries. When contacting Naviant Support, the Customer will be connected directly with a help desk technician, the issue will be logged into the Naviant's Support System, assigned a reference number, and the Customer will receive an email confirmation for tracking purposes. Naviant's standard response time objective is to respond to Customer support inquiries within one hour during Naviant standard business hours; however, Naviant's response time protocol is not to exceed three hours for either callback phone support or remote access to resolve the issue. If the issue requires further investigation, status updates will be provided in a timely manner until the issue is resolved.

5. Customer Responsibilities

A. *Onsite Support*. When support is required at Customer's premises, Customer shall ensure reasonable and safe access to the software and equipment in accordance with these SLA Provisions. Customer will be held accountable for any damages to persons or property resulting from non-compliance.

B. *Operating Environment*. Customer is responsible for maintaining the appropriate operating environment for their system, including but not limited to hardware, software, and disk space. Additionally, Customer must provide suitable electrical power and protective devices. If an inappropriate operating environment leads to system issues, Naviant will undertake a problem definition and resolution effort. Should system problems be resolved by recommending changes or upgrades to essential components, Customer will bear the cost of executing such upgrades. If the upgrade is not completed, Naviant reserves the right to terminate the Software Support Level Agreement. Any system (hardware) enhancements necessitated by a software upgrade must be acquired by Customer prior to installation. Customer acknowledges that Naviant requires online access to the software installed on Customer’s systems for maintenance purposes and support provision. Customer shall install and maintain, at their own expense, communications software approved by Naviant. Customer must establish and maintain an adequate or dedicated connection to facilitate Maintenance and Support Services, also at their own expense.

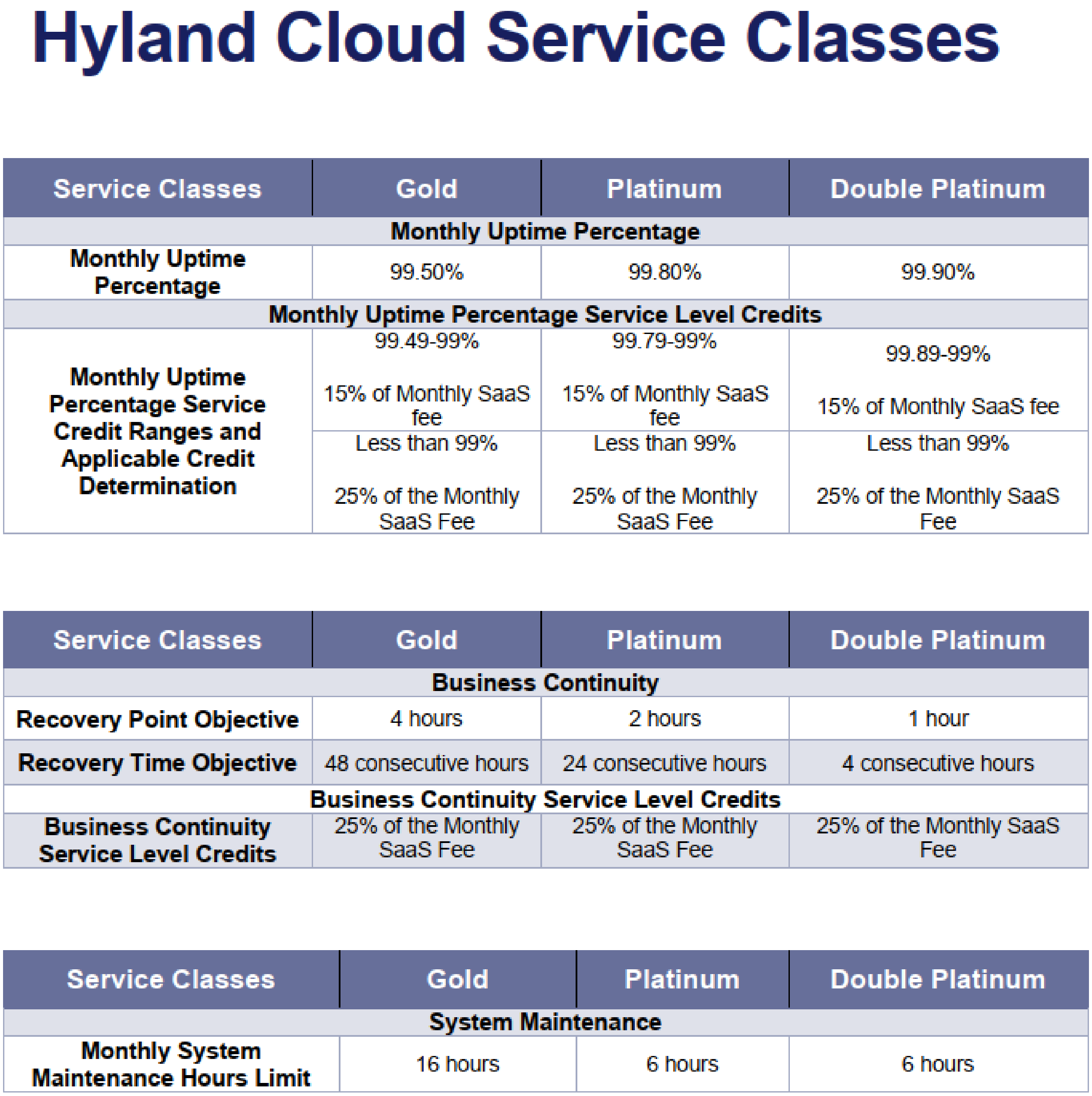
6. Products and Services Not Covered

Software Support Level Agreements do not cover installation fees for initial system configuration, expansion of the system in applications, enhanced functionality, or inclusion of additional users. Unless specifically agreed to in writing, Software Support Level Agreements shall not cover: (i) Support for scripting, API or workflow changes or additions by Customer; (ii) Customized application functions or device support for the software and/or the hardware utilized by the software; (iii) Conversions for the Customer, whether such conversion be to data or to programs; (iv) Onsite support, training, and implementation services beyond the terms specified; (v) Installation of software version upgrades; (vi) Annual system audits not outlined in Section 1; (vii) Support calls related to issues traced to a Customer action, inaction, non-Naviant supported hardware, or non-Naviant supplied or supported software not covered under these SLA Provisions.

Software Support Level Agreements do not provide support for any hardware or software not purchased from Naviant that is used with or attached to the system, or any hardware or software that is required to make the supported system work with excluded items. Any services provided by Naviant to provide compatibility with non-Naviant hardware and software and identify and resolve problems caused by these excluded items will be charged to Customer at Naviant's prevailing Professional Services Group rates. Naviant is not responsible for any damages resulting from Customer's improper use of the system, from the Customer's failure to follow standard back-up procedures, or from any consequences arising from failure of the various computer media used. The use of an unauthorized part, component, modification, or person to effect repairs or changes will cause the Software Support Level Agreement to be null and void at the option of Naviant. Software Support Level Agreements do not cover software reinstallations due to Customer computer moves, relocations, or replacements.

APPENDIX D – HYLAND CLOUD SERVICE CLASS

Customer is purchasing Hyland Cloud Service level gold for this engagement.



Hyland Cloud Service Classes

Service Classes	Gold	Platinum	Double Platinum
Monthly Uptime Percentage			
Monthly Uptime Percentage	99.50%	99.80%	99.90%
Monthly Uptime Percentage Service Level Credits			
Monthly Uptime Percentage Service Credit Ranges and Applicable Credit Determination	99.49-99% 15% of Monthly SaaS fee	99.79-99% 15% of Monthly SaaS fee	99.89-99% 15% of Monthly SaaS fee
	Less than 99% 25% of the Monthly SaaS Fee	Less than 99% 25% of the Monthly SaaS Fee	Less than 99% 25% of the Monthly SaaS Fee

Service Classes	Gold	Platinum	Double Platinum
Business Continuity			
Recovery Point Objective	4 hours	2 hours	1 hour
Recovery Time Objective	48 consecutive hours	24 consecutive hours	4 consecutive hours
Business Continuity Service Level Credits			
Business Continuity Service Level Credits	25% of the Monthly SaaS Fee	25% of the Monthly SaaS Fee	25% of the Monthly SaaS Fee

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

APPENDIX E – OBLIGATIONS & KEY ASSUMPTIONS

The following are key assumptions that impact the success of the solution, and are applicable for all Project Areas within this proposal:

1. Naviant's project implementation methodology will be executed by the project resources.
2. Services will be provided both onsite at one (1) End User location and remotely from Naviant offices.

3. To maintain anticipated timeframes, Customer will review deliverables in accordance to the agreed upon plan. Failure to respond where needed within the designated timelines may result in project delays, loss of resources, and the execution of a Change Order Authorization.
4. Naviant and Customer will review remaining work effort throughout the project. If at any time the number of hours required to complete a project phase exceeds the number of hours estimated by the project teams for that phase, then Naviant will execute a Change Order Authorization.
5. Customer will provide appropriate access to facilities and office space for all onsite or remote work. This includes, but is not limited to, work desks, networked computers, team meeting rooms, conference phones, whiteboards, the internet and VPN connection as dictated by Customer's reasonable security measures.
6. Customer will provide Subject Matter Experts (SMEs) who are thoroughly knowledgeable about the current business practices in their respective areas and who are capable of performing their assigned project roles.
7. Customer will make commercially reasonable efforts to maintain consistent project resources throughout the project.
8. Each deliverable created will use Naviant's standard deliverable templates. Customer requested changes to the deliverable template may increase project costs or introduce timeline delays.
9. Customer will include third-party vendors or subject matter/technical experts as required.
10. Customer will assign a Project Sponsor, who will be actively involved in the project and is the final escalation point for all issues and decisions. The project sponsor will also ensure that the appropriate personnel are made available to execute the project successfully.
11. Each project is intended to be implemented in a specified timeframe. Scheduling delays that impact the project timeline will result in changes to project cost.
12. While onsite, the Naviant personnel will work during normal operating hours generally between 8:00 AM and 5:00 PM, Monday through Friday in the Customer's local time zone. When providing remote services, Naviant and Customer will discuss generally acceptable working hours and take into consideration time zone differences. Issues deemed as non-critical will only be addressed during normal business hours.
13. The installation of this solution may require assistance from the Customer's IT staff to obtain access to the servers and network devices the solution may reside on; and thus, it is required that the Customer schedule their IT resource and customer personnel assigned to this project to be available within 30 minutes of Naviant being scheduled for installation. If Naviant personnel need to wait for longer than 30 minutes for an IT resource to be available for assistance with the installation, the Customer will be charged in ¼ hour increments at the prevailing rate for the time lost. Customer will be responsible for additional equipment cabling, except as specifically set forth to be provided by Naviant. In the event Customer will be required to provide specific additional equipment prior to installation, it is the responsibility of Customer to provide the necessary versions of network OS, server software, database, hardware, browsers, and desktop OS to work with the proposed solutions prior to the scheduled Project milestone or task requiring additional equipment, or costs may be incurred by the Customer. Customer will be responsible for the actual results with hardware operations (including among other aspects, network, server or scanner speeds; personnel requirements; and costs) and results may vary from those indicated due to overall network environment, volume estimates, personnel and other factors.

APPENDIX F- KEY PARTICIPANTS & DENVER PMO REQUIRED DELIVERABLES

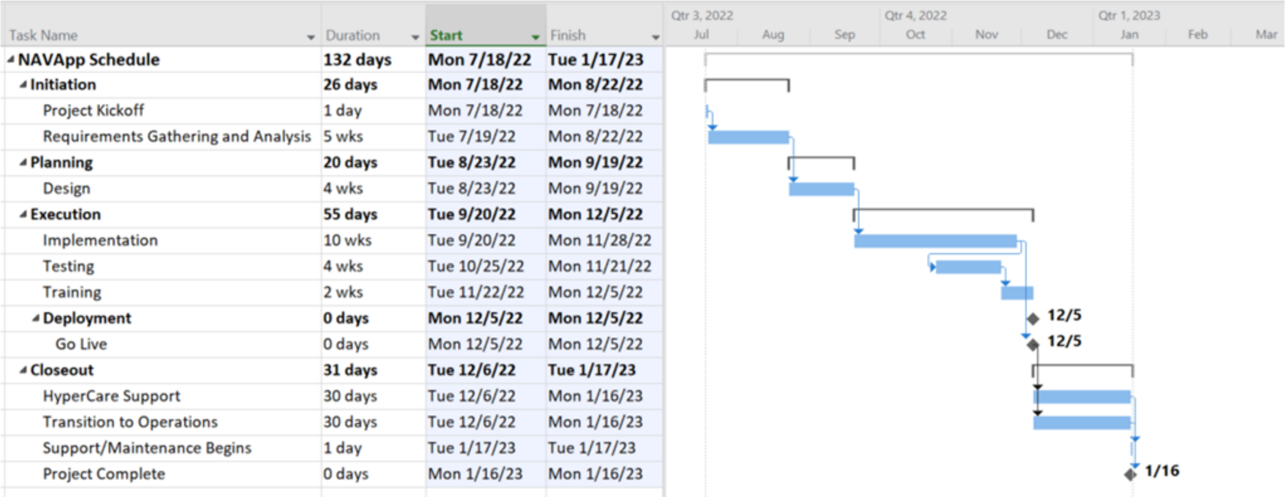
Key Participants

The following table lists the known and anticipated participants that will be involved in this project. List the names of the project teams here for both vendor and CCD.

Name	Agency | Company | Organization	Role
To be completed at initiation phase		

Pre Initiation Phase Sample Project Schedule

The following sample schedule is representative of this implementation project. A refined schedule will be developed based on the actual Project Kickoff and outcomes of the planning phase.



Task Name	Duration	Start	Finish
NAVApp Schedule	**132 days**	**Mon 7/18/22**	**Tue 1/17/23**
Initiation	**26 days**	**Mon 7/18/22**	**Mon 8/22/22**
Project Kickoff	1 day	Mon 7/18/22	Mon 7/18/22
Requirements Gathering and Analysis	5 wks	Tue 7/19/22	Mon 8/22/22
Planning	**20 days**	**Tue 8/23/22**	**Mon 9/19/22**
Design	4 wks	Tue 8/23/22	Mon 9/19/22
Execution	**55 days**	**Tue 9/20/22**	**Mon 12/5/22**
Implementation	10 wks	Tue 9/20/22	Mon 11/28/22
Testing	4 wks	Tue 10/25/22	Mon 11/21/22
Training	2 wks	Tue 11/22/22	Mon 12/5/22
Deployment	**0 days**	**Mon 12/5/22**	**Mon 12/5/22**
Go Live	0 days	Mon 12/5/22	Mon 12/5/22
Closeout	**31 days**	**Tue 12/6/22**	**Tue 1/17/23**
HyperCare Support	30 days	Tue 12/6/22	Mon 1/16/23
Transition to Operations	30 days	Tue 12/6/22	Mon 1/16/23
Support/Maintenance Begins	1 day	Tue 1/17/23	Tue 1/17/23
Project Complete	0 days	Mon 1/16/23	Mon 1/16/23

Pre Initiation Phase

- Complete SOW
- Confirmation of budget
- Contract reviewed and completed
- GRITS Phase Gate Approval to move to initiation
- Vendor Risk Assessment (VRA)
- Technical Architecture Review (TAR)
- Resource Plans (vendor and CCD)

- Charter
- Kickoff slide desk
- GRITS phase gate approval to move to planning phase

Initiation Phase

- Communication Plan
- Project Budget
- Ensure Risk and Issues are Documented in ServiceNow
- Completion of VRA
- Completion of TAR
- Project schedule
- Resources allocated (vendor and CCD)
- GRITS phase gate approval to move to execution
-

Execution Phase

- Maintain risks and issues
- Maintain project schedule
- Maintain resource plans
- Change management plan- Go Live
- Budget tracking
- Weekly status report

Execute to Go Live

Test plan

- Training plan
- UAT Sign Off
- Go Live Checklist- CAB Approval
- Complete Transition to Production
- Identify decommission objects

Monitoring and Control Phase

- Post mortem/lessons learned with vendor and CCD
- Complete transition to support documentation for help desk
- Postproduction warranty (30 days after each agency implementation)
- Complete GRITS Execute to close phase gate

APPENDIX G- HYLAND CONTENT PORTAL TERMS OF USER

HYLAND CONTENT PORTAL TERMS OF USE

These Hyland Content Portal Terms of Use (these “Terms of Use”) govern and control the Customer’s, including its End User’s, access and use of the Hosting Service as described herein.

These Terms of Use forms a part of the Contract Information, and amends that certain separate contract that governs the licenses to the Software previously procured by the Customer (such as an End User License Agreement (click through or written), Master

Software License, Services and Support Agreement, Software License and Services Agreement or other similar agreement addressing Software license terms) (the "Underlying Agreement"). The Underlying Agreement, as amended by these Terms of Use, shall be referred to herein as the Agreement.

For purposes of this Agreement, the terms "Customer", "User" "you" or "your" shall mean the person or entity set forth in the Contract Information.

Customer acknowledges that Jadu, Inc. requires that Customer agree to these Hyland Content Portal Terms of Use prior to Customer's use of the Hosting Service.

DEFINITIONS AND INTERPRETATION

The definitions and rules of interpretation in this clause apply in this Agreement and the schedules to it.

Applicable Law: applicable laws, statutes, common law, regulations, ordinances, codes, rules, guidelines, orders, permits, tariffs and approvals of any governmental authority that apply to the parties or the subject matter of this Agreement including any reference to that law as amended, extended, consolidated or re-enacted from time to time.

Business Day: a day (other than a Saturday, Sunday or any nationally recognized public holiday in the Territory referred to). Hours or minutes referred to in this Agreement in relation to Business Days shall be construed as being units of time within a Business Day.

Contract Information: the purchase table schedule included in the Underlying Agreement, an applicable order form, or other similar document for the purchase of Hosting Services and the corresponding invoice you have been provided with for which the terms of this agreement apply.

Charges: the charges payable for any Hosted Software as set out in the Contract Information.

Customer Data: all content, data, files, documents, links works and materials including those held within any system database used by the Service/Software that may be processed by us or Third Party Services in relation to this Agreement.

that is: uploaded to or stored on the Platform by End Users or integrated systems regarding End User data; transmitted by the Platform at your instigation; supplied by the End User to us for uploading to, transmission by, or storage on the Platform; or generated by the Platform as a result of the use of the Service/Software by the End User (but excluding analytics data relating to the use of the Platform and server log files).

Customer Data Incident meaning an unauthorized disclosure of Customer Data resulting from Hyland's failure to comply with the provisions of clause 4. 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/ Third Party Services 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).

End User: You, any of your organization's users, those users on behalf of whom you may have contracted, and the relevant third party end user using the Service/Software you have procured.

Environment: a single installation of the Service/Software (whether in a cloud based server, single server, virtual server or clustered server infrastructure) and where specifically referred to in the agreement as LIVE Environment (which is intended to provide content and software functionality to end users) or UAT Environment (which is for the purpose of conducting user acceptance testing by you before changes are made to a LIVE Environment).

Force Majeure Event: an event, or a series of related events, that is outside the reasonable control of the party affected including failures of the Internet or any public telecommunications network, cyber or hacker attacks, denial of service attacks, virus or other malicious software attacks or infections, power failures, industrial disputes affecting any third party, changes to the law, disasters including natural disasters, epidemics, pandemics, explosions, fires, floods, riots, terrorist attacks and wars.

Hosting Service or **Hosting Services:** the hosting service of the Platform to be provided by Hyland, or through Third Party Services, set out in the Contract Information including, where indicated, web performance, security or intrusion detection services to you as part of the Hosted Software. The Hosting Service also includes the hosting by Hyland or Third Party Services of the Hosted Software together with the provision of such server maintenance services, infrastructure, hardware and bandwidth as are necessary to provide such Third Party Services in relation to the Service/Software. Schedule 2 lists the subcontractors and data processors you approve for the delivery of the services to be delivered by Hyland under this Agreement.

For the avoidance of doubt, the Hosting Service does not include the Hyland Cloud Service or any services or software offered by Hyland that are not the Hyland Content Portal.

Hosted Software: the Hyland Content Portal Service/Software including all related Software Products indicated as hosted in the Contract Information.

For the avoidance of doubt, the Hosting Software does not include any services or software offered by Hyland that are not the Hyland Content Portal.

Hosting Support Service: the support service for hosting related issues to be provided by Hyland as part of the Hosting Service.

Inappropriate Content: any material which is unlawful, offensive, threatening, libellous, defamatory, pornographic, obscene or otherwise objectionable or violates any party's intellectual property or the terms of this Agreement.

Intellectual Property Rights: rights in patents, utility models, rights to inventions, copyright and related rights, trademarks and service marks, trade names and domain names, rights in get-up, goodwill and the right to sue for passing off or unfair competition, rights in designs, rights in computer software, database rights, moral rights, rights to preserve the confidentiality of information (including know-how and trade secrets) and any other intellectual property rights, including all applications for (and rights to apply for and be granted), renewals or extensions of, and rights to claim priority from, such rights and all similar or equivalent rights or forms of protection which subsist or will subsist, now or in the future, in any part of the world.

Software Products: Service/Software Enterprise products making up the Hyland Content Portal (CP).

For the avoidance of doubt, the Software Products does not include any services or software offered by Hyland that are not the Hyland Content Portal.

Platform: the platform managed by Hyland and used by Hyland to provide the Service/Software, including the application and database software for the Service/Software, the system and server software used to provide the Service/Software, and the computer hardware on which that application, database, system and server software is installed and all networking, storage, and related technology required to run the Service/Software.

Professional Services: professional services provided by Hyland or a Third Party Services provision of professional services at Hyland's request.

Release: an update of the Service/Software incorporating 'patches' where applicable which corrects faults, adds functionality (and may include new tools and resources) or otherwise amends or updates the Service/Software.

Service/Software: the service and any software (which includes Software Products) and associated media and any Documentation Hyland provides to you for the Service/Software or Release in either printed text or digital or machine-readable form, including any technical documentation, program specification and operations manual.

Where reference is made to a 'product' of the Service/ Software it refers to individual Service/ Software products rather than the totality of all Service/Software. The Hosting Service and Hosting Support Service in relation to the Service/Software does not include any templates, themes, forms, case types, portals or other presentation layer or content items designed to operate in conjunction with or to interface with the Service/Software and are not part of the Service/Software in this regard.

For the avoidance of doubt, the Service/Software does not include any services or software offered by Hyland that are not the Hyland Content Portal.

Support Portal: the on-line support and incident-reporting help desk system provided by Hyland as part of the Hosting Support Service.

Standard Support Hours: 8.00 am to 6.00 pm on Business Days in England in relation to the provision of the Hosting Support Service.

Territory: England, U.S or Canada according to the location of the respective party's principal place of business.

Third Party Services: any part of the Hosting Service or third party integrations provided by any third party, other than Jadu, Inc. in accordance with the terms of this Agreement.

1. DURATION.

1.1 Without limitation to clause 1.2, this Agreement will take effect as of and on the date that Customer has accepted this Agreement as described above (the "Commencement Date").

1.2 Subject to termination in accordance with the provisions of this Agreement, this Agreement shall continue for the Term Length indicated in the Contract Information.

1.3 Following expiry of this Agreement, any resumption of the Service/Software will require you to enter into a new agreement with Hyland and the payment by you of the prevailing Charges.

1.4 The Contract Information sets out details of the Hosted Software.

2. CHARGES.

2.1 In consideration of the provision of the Hosting Service, you shall pay the Charges. You shall pay the Charges annually in advance within thirty (30) days of the date of Hyland's invoice unless otherwise set out in the Contract Information.

2.2 Charges are non-refundable. For the avoidance of doubt there will be no refunds or credits where you have used the Hosted Software or any Third Party Services including where this has been for only part of the term indicated in the Contract Information or where there has been no use, or partial use of the Hosted Software, or any Third Party Services or where you have obtained an addition or reduction in the Service/Software and Hyland does not accept any liability whatsoever for any loss of applications, content, features or capacity caused as a result of a reduction of the Service/Software you have obtained.

2.3 Save where the Contract Information sets out the complete arrangements for the payment of Hyland expenses occasioned with the provision of Hyland services pursuant to this Agreement, you shall reimburse any of Hyland's reasonable expenses including travel, hotel costs, subsistence and any associated expenses where such expenses are incurred wholly and exclusively for the purpose of providing on-site support in respect of the provision of the Hosted Software, (and where Hyland has indicated in the Contract Information the use of Third Party Services, where the cost of services provided by such third parties and required by Hyland for the performance of the aforementioned service) provided any request for reimbursement is in the form of a proper invoice accompanied by appropriate receipts.

2.4 All amounts payable under this Agreement shall be exclusive of all applicable taxes and government charges (such as duties), all of which shall be paid by you (other than taxes on Hyland's income). In the event you are required by law to withhold taxes, you agree to furnish Hyland all required receipts and documentation substantiating such payment. If Hyland is required to remit any tax or government charge on behalf of (or on account of) you, you agree to reimburse Hyland within thirty (30) days after Hyland notifies you in writing of such remittance. You agree to provide Hyland with valid tax exemption certificates in advance of any remittance otherwise required to be made by Hyland on your behalf, where such certificates are applicable.

3. HOSTING SERVICE.
3.1 Where Hyland supplies the Hosting Service and you take and pay for Hosted Software the following provisions shall comprise the Hosting Service.

3.2 In relation to the Hosting Service:

(a) The Hosting Service shall include the hosting by Hyland or Third Party Services subcontractors set out in schedule 2 of the Hosted Software together with the provision of such server maintenance services, infrastructure, hardware and bandwidth as are necessary to provide such hosting. Without prejudice to your other obligations under this clause 3.2:

(i) you must ensure that you have in place the necessary contractual safeguards to ensure the transfer of relevant Customer Data to Hyland and a provider of Third Party Services for the Hosting Service is lawful;

(ii) you must ensure that you have in place the necessary contractual safeguards to ensure the use of relevant Customer Data by Hyland and a provider of Third Party Services Hosting Service is lawful;

(iii) you shall have the opportunity to consent to transfers of Customer Data to any Third Party Services Hosting Service operator and Hyland must ensure that such transfers shall not take place without your consent;

(iv) you hereby consent to the transfer of the Customer Data to the relevant Third Party Services Hosting Service subcontractors set out in schedule 2 (or agreed elsewhere in writing between the parties). This shall be for any such category of data that may reasonably be regarded by Hyland as required for the effective purpose of such Hosting Service or as otherwise stipulated in the schedule 2;

(v) you acknowledge that from time to time Hyland may substitute, replace or add a Third Party Services Hosting Service provider and in such event, Hyland shall seek your consent to do so;

(vi) you warrant to Hyland that the transfer of Customer Data by Hyland to a provider of Third Party Services in accordance with this clause 3.2 will not infringe any person's legal or contractual rights and will not put Hyland in breach of any Applicable Law; and

(vii) you acknowledge that the Hosting Service is designed to be compatible only with that software and those systems specified by Hyland in writing as compatible; and Hyland does not warrant or represent that the Service/Software will be compatible with any other software or systems and Hyland provides no warranties or representations in respect of any Third Party Services Hosting Service.

(b) Data storage for the Hosting Service is fully managed, with twenty four (24) hour seven (7) days a week monitoring and point-in-time recovery. Hyland will respond to any outage, technical issue or service interruption as soon as is reasonably practicable. Hyland may where necessary choose to restore any severely affected system from the latest backup**,** however you acknowledge that this process may overwrite the Customer Data stored on the Platform prior to the restoration point and Hyland will bring the Customer Data back into the Hosting Service as soon as reasonably practicable at no additional cost to you save where any loss or damage to data is caused by matters or circumstances beyond Hyland’s reasonable control (including but not limited to viruses, denial-of-service attacks or any other form of cyber-attack) in which case, any work in this regard shall involve Professional Services.

(c) You will use reasonable efforts to ensure any Customer Data submitted to Hyland or Third Party Services subcontractors via electronic media will be free of viruses and Hyland shall provide virus-checking of the Hosted Software from commencement of the Hosting Service. Hyland shall also provide firewall protection.

(d) Hyland shall provide such server monitoring, log file rotation, application of server operating system updates and patches and user account management services as Hyland reasonably considers necessary for the provision of a reliable and consistent Hosting Service.

(e) Save for immediately deployed emergency Releases required to urgently address security or performance / availability issues, Hyland may suspend for the purpose of repair, maintenance or improvement, part or all of the Hosting Service upon at least twenty four (24) hours’ notice to you and shall use reasonable endeavors to restore the Hosting Service as soon as is reasonably practicable following any such suspension.

(f) You shall follow reasonable instructions provided by Hyland in respect of the Hosting Service which Hyland considers necessary for safety or to maintain or improve the quality of the Hosting Service. This may include Hyland’s use of alternative Third Party Services subcontractors pursuant to this clause 3.2.

(g) Unless the parties have agreed otherwise in writing, your use of the Hosted Software shall be (i) limited to the bandwidth set out in the Contract Information in relation to the specific environment for Hyland Software Products. Any use over such limit shall be subject to additional bandwidth charges, in accordance with Hyland's rates advertised or notified to you from time to time (ii) 250 GB of storage for accounts of Software Products.

(h) You shall keep secure any usernames and passwords related to the Hosting Service and shall notify Hyland immediately of any known or suspected unauthorized use of the Hosted Software or breach of security, including loss, theft or unauthorized disclosure of one of your passwords or other security information.

(i) You shall observe all reasonable security and operational procedures Hyland may from time to time prescribe and you shall not use the Hosting Service in any way which could be detrimental to Hyland's other clients and customers.

(j) Hyland shall be entitled to update the technical specification of the Hosting Service for operational reasons. In order to allow Hyland to continually upgrade hosting facilities, Hyland may from time to time relocate your servers within Third Party Services data centers, make changes to the provision of the Hosting Service, URLs and Internet protocol (IP) addresses and establish new procedures for the use of the Hosting Service. Hyland will give you advance notice of any such change and endeavor to minimize the effect of any such changes on your use of the Hosting Service.

(k) You shall not conduct, or request that any other person conduct, any load testing or penetration testing on the Platform, Hosting Service or Service/Software without Hyland's prior written consent not to be unreasonably withheld or delayed.

(l) You shall not misuse the Service/Software by knowingly introducing viruses, trojans, worms, logic bombs or other material which is malicious or technologically harmful.

(m) You have sole responsibility for the accuracy, quality, content and legality of all Customer Data. You shall not upload, publish, post, link to or transmit any Inappropriate Content using the Service/Software and you accept that Hyland is not responsible for the content posted or otherwise appearing on the Service/Software and that End Users are exposed to the content of the Service/Software at their own risk. Hyland may, but have no obligation to remove content that Hyland determines in its sole discretion is Inappropriate Content.

(n) You shall not attempt to gain unauthorized access or make any alteration to the Platform, Service/Software, the server from which the Service/Software is provided or any other server, computer or database connected to the Service/Software. By breaching this provision, you may commit a criminal offence (in the United States under the computer fraud law (18 U.S.C. § 1030 contained in the Comprehensive Crime Control Act of 1984 or other Applicable Law). Hyland shall report any such breach to the relevant law enforcement authorities and will cooperate with those authorities by disclosing your identity to them if Hyland is required to do so. In the event of such a breach, your right to use the Service/Software will cease.

(o) Hyland is not responsible for providing, or obligated to provide, Hosting Support Service:

(i) 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 the Service/Software or from any error or defect in any configuration of any component of the Service/Software or Hosting Service, which activities in any such case were undertaken by any party other than Hyland or a Third Party Service supplier;
(ii) in connection with any error or defect or problem in any other component of the Service/Software or Hosting Service if Hyland has previously made available corrections for such error or defect which you fail to implement;
(iii) 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 Service/Software or the Hosting Service;
(iv) if any party other than Hyland or Third Party Services supplier, has provided any services in the nature of the Hosting Support Service to you with respect to the Service/Software or Hosting Service; or
(v) in connection with any questions related to the operation or use of the Service/Software application programming interfaces (APIs). Support relating to the operation or use of APIs may be provided, on a case-by-case basis, as mutually agreed to in an applicable Hyland proposal which outlines Professional Services for such support activities.

(p) The Service/Software and Hosting Service is not fault-tolerant and is not guaranteed to be error free or to operate uninterrupted. The Service/Software or Hosting Service is not designed or intended for use in any situation where failure or fault of any kind of the Service /Software or Hosting Service could lead to death or serious bodily injury to any person, or to severe physical or environmental damage ("High Risk Use"). You are not permitted to use the Service/Software or Hosting Service in, or in conjunction with, High Risk Use. High Risk Use is STRICTLY PROHIBITED. High Risk Use includes, for example, the following: aircraft or other modes of human mass transportation, nuclear or chemical facilities, life support systems, implantable medical equipment, motor vehicles, or weaponry systems. High Risk Use does not include utilization of the Service/Software or Hosting Service for administrative purposes, as an information resource for medical professionals, to store configuration data, engineering and/or configuration tools, or other non-control applications, the failure of which would not result in death, personal injury, or severe physical or environmental damage. These non-controlling applications may communicate with the applications that perform the control, but must not be directly or indirectly responsible for the control function. You agree not to use, distribute, license, or grant the use of the Service/Software or Hosting Service in, or in connection with, any High Risk Use."

3.3 Both parties shall take appropriate technical and organizational measures against unauthorized or unlawful processing of Customer Data or its accidental loss, destruction or damage. This may include pseudonymizing and encrypting Customer Data. Where requested by you or as otherwise authorized under this Agreement, the technical processing and transmission of the Service/Software in relation to the Hosting Service including your content, may be transferred unencrypted and involve:

(a) transmissions over various networks and in this regard, Hyland are not responsible for any delays, delivery failures, or any other loss or damage resulting from the transfer of data over communications networks and facilities, including the Internet, and you acknowledge that the Service/Software may be subject to limitations, delays and other problems inherent in the use of such communications facilities;

(b) changes to conform and adapt to technical requirements of connecting networks or mobile devices;

(c) temporary return of encrypted data to an unencrypted format for the effective operation of the intrusion detection system forming part of the Hosting Services; and

(d) in the event of a support or security issue with the Hosting Services access to data to perform required investigation and resolution of any such issue.

3.4 All interactions with the Hosted Software, whether via the administration user interfaces that Hyland provides or via the API for systems integrations, data will be transmitted over an HTTPS (TLS) connection.

3.5 Without limitation to clauses 3.3 and 3.4, Software Product form data captured is stored at rest using AES encryption.

3.6 You are exclusively responsible for the selection, use of and results obtained from any other programs, materials or services used in conjunction with the Service/Software.

3.7 You shall provide Hyland staff and all other persons duly authorized by Hyland with full, safe and uninterrupted access (including remote access with sufficient network connectivity speed) to your premises, systems, facilities and the Service/Software as may reasonably be required for the purpose of performing Hyland's service obligations under this Agreement, such access, except in the case of emergency or agreed out-of-hours downtime, to be within the Standard Support Hours. Where Hyland's service obligations are to be performed at any of your premises, you shall provide adequate working space and office facilities (including telephone) for use by Hyland staff and take reasonable care to ensure their health and safety.

4. CUSTOMER DATA.

4.1 You hereby grant to Hyland a non-exclusive license to copy, reproduce, store, distribute, publish, export, adapt, edit and translate the Customer Data to the extent reasonably required for the performance of Hyland's obligations and the exercise of Hyland rights under this Agreement. You also grant to Hyland the right to sub-license these rights to Hyland's Third Party Services providers, subject to any express restrictions elsewhere in this Agreement.

4.2 You warrant to Hyland that the Customer Data will not infringe the Intellectual Property Rights or other legal rights of any person, and will not breach the provisions of any law, statute or regulation, in any jurisdiction and under any Applicable Law.

4.3 Details of data storage for the Hosting Service are set out at clause 3.2 (b) of this Agreement.

4.4 You warrant to Hyland that you have the legal right to disclose all Customer Data that you do in fact disclose to Hyland under or in connection with this Agreement.

4.5 You shall only supply to Hyland, and Hyland shall only process, in each case under or in relation to this Agreement:

(a) the Customer Data of data subjects falling within the categories specified in the table in schedule 3 or such other categories as may be agreed by the parties in writing; and

(b) Customer Data of the types specified in schedule 3 or such other types as may be agreed by the parties in writing.

4.6 Hyland shall only process the Customer Data for the purposes specified in table in schedule 3. In the event that no detail is set out in that table. Hyland is permitted to process Customer Data as Hyland sees fit (acting reasonably and in good faith) in accordance with the provision of the Service/Software and in accordance with Hyland's obligations under this Agreement.

4.7 Hyland shall only process the Customer Data during the duration of this Agreement and for not more than thirty (30) days or such other time period as agreed between the parties following the termination of the agreement, subject to the other provisions of this clause 4.

4.8 Hyland shall only process the Customer Data on your documented instructions (including with regard to transfers of the Customer Data to any place outside your Territory), as set out in this Agreement or as otherwise agreed in writing between the parties.

4.9 You hereby authorize Hyland to make the following transfers of Customer Data:

(a) Hyland may transfer the Customer Data internally to its own employees, offices and facilities in the Hyland Group of companies, provided such transfers must be protected by appropriate safeguards including reasonable appropriate technical and organizational measures against unauthorized or unlawful processing of Customer Data or its accidental loss, destruction or damage;

(b) Hyland may transfer the Customer Data to Hyland's Third Party Services subcontractors identified as providing the relevant services to Hyland as set out in schedule 2, provided such transfers must be protected by appropriate safeguards including reasonable appropriate technical and organizational measures against unauthorized or unlawful processing of Customer Data or its accidental loss, destruction or damage; and

(c) Hyland or its Third Party Services subcontractors identified in schedule 2 may process the Customer Data in a country, territory or sector only to the extent required to ensure effective service (including Hosting Support Service) provision provided always that Hyland or its Third Party Services subcontractors ensure the adequate level of protection for Customer Data in accordance with industry standard, internationally recognized data processing agreements.

4.10 Notwithstanding any other provision of this Agreement, Hyland may process the Customer Data if (and only to the extent that) Hyland is required to do so by Applicable Law. In such a case, Hyland shall inform you of the legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

4.1 Hyland shall ensure that persons authorized to process the Customer Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

4.12 Both parties shall each implement appropriate technical and organizational measures to ensure an appropriate level of security for the Customer Data, including those measures specified in schedule 3.

4.13 Hyland must not engage any third party to process the Customer Data without your prior written consent. Accordingly, Hyland shall inform you at least thirty (30) days in advance of any intended changes concerning the addition or replacement of any Third Party Services Hosting Service provider. If you object to any such changes before their implementation, then you may terminate this Agreement on seven (7) days' written notice to Hyland, provided such notice must be given within the period of seven (7) days following the date that Hyland informed you of the intended changes. Hyland shall ensure that each Third Party Services Hosting Service provider is subject to similar legal obligations as those imposed on Hyland by this clause 4.

4.14 As at the Commencement Date, Hyland is hereby authorized by you to engage as sub-processors with respect to Customer Data, the relevant Third Party Services subcontractors identified in schedule 2.

4.15 Hyland shall, insofar as possible, and taking into account the nature of the processing, take appropriate technical and organizational measures to assist you through the provision of Professional Services (unless the parties otherwise agree in writing) with the fulfilment of your obligation to respond to requests exercising a data subject's rights under Applicable Law.

4.16 Hyland shall assist you through the provision of Professional Services (unless the parties otherwise agree in writing) in ensuring compliance with the obligations relating to the security of processing of Customer Data; the notification of Customer Data breaches to the supervisory authority; the communication of Customer Data breaches to the data subject; data protection impact assessments and prior consultation in relation to high-risk processing under the Applicable Law. Where any such Customer Data breach is caused by matters or circumstances beyond Hyland's reasonable control (including but not limited to viruses, denial-of-service attacks or any other form of cyber-attack) Hyland may be able to assist you with any remedial work you require to be undertaken through the provision of Professional Services. Hyland shall not be liable for any such loss or damage caused by any third party except those Third Party Services contracted by Hyland to perform the Hosting Service.

4.17 Hyland will notify you of any Customer Data breach affecting the Customer Data without undue delay and, in any case, not later than thirty six (36) hours after Hyland becomes aware of the breach. You will alert Hyland without undue delay as soon as you become aware of any such breach.

4.18 Hyland shall make available to you, information necessary to demonstrate Hyland's compliance with its obligations under this clause 4. Hyland can assist you through the provision of Professional Services (unless the parties otherwise agree in writing) with any work to be performed by Hyland at your request pursuant to this clause 4.18, provided no such Professional Service charges shall be levied with respect to the completion by Hyland (at your reasonable request, not more than once per calendar year).

4.19 Upon written request by you to Hyland, 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 or Third Party Service data-centers, including all replicated copies

4.20 You acknowledges that the integration of Third Party Services may entail the transfer of Customer Data from the Service/ Software to the relevant Third Party Services; and Hyland has no control over, or responsibility in respect of any disclosure, modification, deletion or other use of Customer Data resulting from any integration with any Third Party Services and you must ensure that you have in place the necessary contractual safeguards to ensure that both: the transfer of relevant Customer Data to a provider of Third Party Services application is lawful; and the use of relevant Customer Data by a provider of Third Party Services application is lawful.

4.21 You acknowledge full responsibility in relation to the lawful transfer, use, handling, storage, deletion or return of the same in relation to any Customer Data integrated with or through Third Party Services applications.

4.22 Hyland shall allow for and contribute to audits, including inspections, conducted by you or another auditor mandated by you in respect of the compliance of Hyland's processing of Customer Data pursuant to this clause 4. Hyland can assist you through the provision of Professional Services (unless the parties otherwise agree in writing) with any work performed by Hyland at your request pursuant to this clause 4.22, provided that no such charges shall be levied where the request to perform the work arises out of any breach by Hyland of this Agreement or any security breach affecting a Platform.

4.23 If any changes or prospective changes to the Applicable Law result or will result in one or both parties not complying with the Applicable Law in relation to the processing of Customer Data carried out under this Agreement, then the parties shall use their best endeavors promptly to agree such variations to this Agreement as may be necessary to remedy such non-compliance.

4.24 You agree that, for Hyland's research and development purposes and to allow Hyland to continually improve Hyland's quality and user experience, Hyland may automatically collect and store the following information from you each time you or your authorized users access the Service/Software interfaces:

(a) technical information as stored within a combination of the Service/Software or supporting log files, including the Internet Protocol (IP) address of your computer, your login identifier, browser type and version, time zone setting, operating system and platform date/time access; and

(b) other information about your use of the Service/Software as stored within Hyland's managed Google Analytics account, including the modules of the Service/Software that you have used and how you have used them, the date and time, page response times, length of visits to certain pages, page interaction information (such as scrolling, clicks, and mouse-overs) and methods used to browse away from certain pages.

4.25 You agree that Hyland may use the information collected pursuant to clause 4.24 in order to contact you with useful and relevant advice or information relating to the Service/Software.

5. LIMITATION OF LIABILITY AND INDEMNITIES.

5.1 EXCEPT FOR THE WARRANTIES PROVIDED BY HYLAND AS EXPRESSLY SET FORTH IN THIS AGREEMENT, HYLAND AND ITS THIRD PARTY SERVICES SUPPLIERS MAKE NO WARRANTIES OR REPRESENTATIONS REGARDING ANY SERVICE (INCLUDING IN RELATION TO THE SERVICE/SOFTWARE, PLATFORM, HOSTED SOFTWARE, HOSTING SERVICE, HOSTING SUPPORT SERVICE, PROFESSIONAL SERVICES AND THIRD PARTY SERVICES) OR ANY OTHER SERVICES PROVIDED UNDER THIS AGREEMENT OR ANY SERVICES PROPOSAL. HYLAND AND ITS THIRD PARTY SERVICES 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 THIRD PARTY SERVICES SUPPLIERS DO NOT WARRANT THAT ANY MAINTENANCE AND SUPPORT, HOSTING SERVICE, PROFESSIONAL SERVICES, SERVICE/SOFTWARE PROVIDED WILL SATISFY YOUR REQUIREMENTS OR ARE WITHOUT DEFECT OR ERROR, OR THAT THE OPERATION OF ANY SOFTWARE/SOFTWARE, HOSTING SERVICE, ADD-ON SERVICES, OR ANY WORK PRODUCTS PROVIDED UNDER THIS AGREEMENT WILL BE UNINTERRUPTED. EXCEPT AS EXPRESSLY STATED IN THIS AGREEMENT, HYLAND DOES NOT ASSUME ANY LIABILITY WHATSOEVER WITH RESPECT TO ANY THIRD PARTY HARDWARE, FIRMWARE, SOFTWARE OR SERVICES.

5.2 YOU SPECIFICALLY ASSUME RESPONSIBILITY FOR THE SELECTION OF THE SERVICE/SOFTWARE, MAINTENANCE AND SUPPORT, HOSTING SERVICES AND PROFESSIONAL SERVICES TO ACHIEVE YOUR BUSINESS OBJECTIVES.

5.3 HYLAND MAKES NO WARRANTIES WITH RESPECT TO ANY SERVICE/SOFTWARE, OR HOSTING SERVICES, IN ANY NON-PRODUCTION SYSTEM AND PROVIDES ANY SUCH SERVICE/SOFTWARE, HOSTING SERVICE, "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.

5.5 NEITHER PARTY NOR ANY OF ITS AFFILIATES (AND IN THE CASE OF HYLAND, ITS THIRD PARTY SERVICES SUPPLIERS) SHALL BE LIABLE, WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE), OR ANY OTHER LEGAL OR EQUITABLE THEORY, FOR ANY INDIRECT, INCIDENTAL, SPECIAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES, OR ANY LOSS OF REVENUE, GOODWILL, SAVINGS OR PROFITS (EXCLUDING FEES DUE UNDER THIS AGREEMENT), LOSS OR CORRUPTION OF DATA OR PROGRAMS, COSTS OF REPLACEMENT OR THE REMEDY OF COVER, OR BUSINESS INTERRUPTION DAMAGES, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, LOSSES, EXPENSES OR COSTS.

5.6 HYLAND'S (INCLUDING ITS AFFILIATES AND THIRD PARTY SERVICES SUPPLIERS) TOTAL, CUMULATIVE LIABILITY ARISING OUT OF OR RELATED TO THIS AGREEMENT OR THE PRODUCTS OR SERVICES PROVIDED UNDER IT, WHETHER IN CONTRACT OR TORT (INCLUDING NEGLIGENCE), OR ANY OTHER LEGAL OR EQUITABLE THEORY, SHALL IN NO EVENT EXCEED THE TOTAL AMOUNTS ACTUALLY PAID TO HYLAND BY YOU (LESS ANY REFUNDS OR CREDITS) FOR THE USE OF THE PRODUCTS OR PROVISION OF THE SERVICES GIVING RISE TO THE CLAIM DURING THE TWELVE (12) MONTH PERIOD IMMEDIATELY PRECEDING THE FIRST EVENT GIVING RISE TO SUCH CLAIM. WITH RESPECT TO ANY PRODUCTS OR SERVICES PROVIDED TO YOU FREE OF CHARGE (SUCH AS EVALUATION SOFTWARE OR SERVICES), NEITHER HYLAND NOR ANY OF ITS AFFILIATES OR THIRD PARTY SERVICES SUPPLIERS WILL BE LIABLE FOR DIRECT DAMAGES.

5.7 THE LIMITATIONS IN SECTIONS 5.5 AND 5.6 SHALL NOT APPLY TO THE EXTENT SUCH LIMITATIONS ARE PROHIBITED BY LAW.

5.9 You acknowledge that Hyland uses Third Party Services to provide the Hosting Service of the Platform and the only representation as to service levels and uptime are in accordance with the service levels set out in schedule 1. Without prejudice to any other provision of this Agreement, Hyland's total liability to you in respect of such services levels and uptime shall in no circumstances exceed a sum equivalent to the service credits set out in schedule 1.

5.10 NOTWITHSTANDING ANYTHING TO THE CONTRARY, IN THE CASE OF A CUSTOMER DATA INCIDENT THE FOLLOWING SHALL APPLY: THE MAXIMUM LIABILITY OF HYLAND (INCLUDING ITS THIRD PARTY SERVICES) ARISING OUT OF OR RELATED TO THIS AGREEMENT OR THE PRODUCTS OR SERVICES PROVIDED UNDER IT FOR A CUSTOMER DATA INCIDENT (AS DEFINED IN THIS AGREEMENT), WHETHER IN CONTRACT OR TORT (INCLUDING NEGLIGENCE), OR ANY OTHER LEGAL OR EQUITABLE THEORY, SHALL IN NO EVENT EXCEED, IN THE AGGREGATE, ALL FEES AND CHARGES ACTUALLY PAID BY YOU TO HYLAND (LESS ANY REFUNDS OR CREDITS) UNDER THIS AGREEMENT DURING THE TWELVE (12) MONTH PERIOD IMMEDIATELY PRECEDING THE CUSTOMER DATA INCIDENT MULTIPLIED BY TWO (2).

6. TERMINATION.

6.1 Without prejudice to any rights that have accrued under this Agreement or any of its rights or remedies and unless the parties have otherwise agreed in writing, either party may at any time terminate this Agreement with immediate effect by giving written notice to the other party if:

(a) the other party fails to pay any amount due under this Agreement on the due date for payment and remains in default not less than fourteen (14) days after being notified in writing to make such payment;

(b) the other party commits a material breach of any term of this Agreement (other than failure to pay any amounts due under this Agreement) which is irremediable or (if such breach is remediable) the other party fails to remedy that breach within a period of thirty (30) days after being notified in writing to do so;

(c) the other party repeatedly breaches any of the terms of this Agreement in such a manner as to reasonably justify the opinion that its conduct is inconsistent with it having the intention or ability to give effect to the terms of this Agreement;

(d) the other party suspends, or threatens to suspend, payment of its debts or is unable to pay its debts as they fall due or admits inability to pay its debts or is deemed unable to pay its debts within the meaning in the Uniform Commercial Code 1952 (as revised), or is insolvent within the meaning of Title 11 of the United states Code (Bankruptcy Code).

6.2 Without limiting Hyland's other rights or remedies and unless the parties have otherwise agreed in writing, Hyland may terminate this Agreement (or at Hyland's option suspend any Hosted Software under it) with immediate effect by giving written notice to you if you fail to pay any amount due (pursuant to clause 6.1(a); or if you or any agent acting on your behalf interferes with or repeatedly fails to implement the advice given in respect of the Hosted Software inhibiting or preventing Hyland from performing its service obligations under this Agreement or if your staff are abusive or behave unreasonably to Hyland staff.

6.3 Other than as set out in this Agreement, neither party shall have any further obligation to the other under this agreement after its termination.

6.4 On termination of this Agreement for any reason, your right to use the Hosted Software shall cease automatically along any Hosting Service.

6.5 On termination of this Agreement for any reason, you shall immediately pay any outstanding unpaid invoices due to Hyland.

7. NON-SOLICITATION.

7.1 You shall not, for the duration of this Agreement, and for a period of six months following termination, directly induce or attempt to induce any of Hyland's employees who have been engaged in the provision or management of the Hosting Service or otherwise in connection with this Agreement to leave Hyland's employment.

8. GENERAL.
8.1 Save where specifically agreed in writing between the parties, neither of the parties shall be liable to the other as a result of any delay or failure to perform its obligations (save for its obligation to pay Charges and any professional Services charges where relevant) under this Agreement as a result of a Force Majeure Event. In the event that either party is delayed or prevented from performing their obligations under this Agreement, that party shall:

(a) give notice in writing of such delay or prevention to the other party as soon as reasonably possible, stating the effective date and extent of such delay or prevention, the cause thereof and its estimated duration;

(b) use reasonable endeavors to mitigate the effects of such delay or prevention of performance of its obligations under this Agreement; and

(c) resume performance of its obligations under this Agreement as soon as reasonably possible after the removal of the cause of the delay or prevention.

8.2 Any notice to be served in respect of this Agreement must be in writing and must be served by hand or registered post or recorded delivery and in the case of a company must be served at its registered office for the time being. In any other case notice may be served at any address for the time being of the person to be served. Such service shall take effect, if given by hand, on the date of delivery. If given by post, it shall take effect two (2) Business Days after posting.

8.3 Hyland's waiver of any right under this Agreement is only effective if it is in writing and shall not be deemed to be a waiver of any subsequent breach or default. No failure or delay by Hyland in exercising any right or remedy under this Agreement or by law shall constitute a waiver of that or any other right or remedy, nor preclude or restrict its further exercise.

8.4 Except as expressly provided in this Agreement, the rights and remedies provided under this Agreement are in addition to, and not exclusive of, any rights or remedies provided by law.

8.5 If a court or any other competent authority finds that any provision of this Agreement (or part of any provision) is invalid, illegal or unenforceable, that provision or part-provision shall, to the extent required, be deemed deleted, and the validity and enforceability of the other provisions of this Agreement shall not be affected. If any invalid, unenforceable or illegal provision of this Agreement would be valid, enforceable and legal if some part of it were deleted, the provision shall apply with the minimum modification necessary to make it legal, valid and enforceable.

8.6 Nothing in this Agreement is intended to, or shall be deemed to constitute a partnership or joint venture of any kind between the parties, nor constitute either party the agent of another party for any purpose. Neither party shall have authority to act as agent for, or to bind the other in any way.

8.7 Neither party shall assign, transfer, mortgage, charge, subcontract, declare a trust over or deal in any other manner with any or all of its rights or obligations under this Agreement without the other party's consent not to be unreasonably withheld or delayed.

8.8 Except as set out in these terms and conditions, no variation of this Agreement, including the introduction of any additional terms and conditions, shall be effective unless it is agreed in writing and signed by the parties.

8.9 No person who is not a party to this Agreement shall acquire any rights under it or be entitled to benefit from any of its terms even if that person has relied on any such terms or has indicated to any party to this Agreement its assent to any such terms.

8.10 This Agreement, and any dispute or claim arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims), shall be governed by, and construed in accordance with the laws of the State of Kansas and the parties irrevocably submit to the exclusive jurisdiction of the courts of the State and Federal courts of Kansas.

8.11 To the extent of any conflicting terms, conditions or stipulations contained or referenced in any other agreement, including the Underlying License Agreement or Contract Information, the terms and conditions of this Agreement shall control as it relates to the Hosting Services. For the avoidance of doubt, the parties acknowledge and agree that, except for the Hyland Content Portal, the terms of this Agreement shall not apply to any other software or services provided by Hyland to Customer

Schedule 1

Details of Hosting Support Service, service levels and service credits
Hosting Support Service for Service/Software:
Due to the varying types of Hosting Support Service issues and the dependency on both your and Hyland's Third Party Services (hosting provider's) interaction, Hyland does not offer a "resolution target" for Hosting Support Service issues.
Response and resolution times depend on the nature and severity of the Hosting Support Service issues reported. The following response and approximate resolution times represent 'worst case scenarios' for the most complex Hosting Support Service issues rather than being targets for all Hosting Support Service issues and Hyland would expect to be well within these times for most Hosting Support Service issues.

The date and time at which a Hosting Support Service issue is raised is considered to be the date and time at which it is entered into the Support Portal. Any Hosting Support Service issues raised by your staff or agents via telephone call will be logged on their behalf within the Support Portal. Where Hosting Support Service issues are raised by telephone call then a first response target will be deemed to have been met by the interaction within said call. For the purposes of the audit trail and any subsequent reports the times will be taken from the date and time the Hosting Support Service issues were logged in the Support Portal.
Hyland will respond to Hosting Support Service tickets within Standard Support Hours within the following response times:

Priority of Hosting Support Service Issue:	First Response (as set out above) within:	Feedback frequency:	Approximate resolution for Hosting Support Service issue, Platform or Release update, temporary fix or workaround and where applicable, available for you to test:
Priority 1 - Customers WITH a DR Environment A Hosted Software issue which is a complete unavailability of Service/Software and Hosting Service for a period of 5 minutes or more	30 minutes ***** for Hyland Software Products.	Every hour *****	1 hour *****(or sooner for temporary fix) to provide a fix or to switch to DR site (subject to terms and conditions of DR service) for Hyland Software Products

** Business Day, hour(s) or other specified unit of time.*

Service/Software Uptime SLA - Service Credits for Hyland Software Products:

Service Hours	Measurement Period	Uptime	Service Credit **(**)**
24 x 7	Annually	Between 99.9% and 99.00%	3% of Hyland's annual Charge to you for the applicable Hosting Service.
24 x 7	Annually	Between 98.99% and 97.50%	6% of Hyland's annual Charge to you for the applicable Hosting Service.
24 x 7	Annually	Below 97.49%	10% of Hyland's annual Charge to you for the applicable Hosting Service.

(**) Service Credits shall be exclusive the financial remedy for failure to meet the KPIs in the table above and will take the form of a credit note to be offset against future Charges. Service Credits shall only be paid as a refund if the agreement is terminated or expires and the Supported Service is not renewed. The measurement of determining Service Credits shall be based on a calendar year and accordingly shall commence from your first full calendar month using the Service/Software.
Service credits are only payable on the applicable Uptime banding and not applied cumulatively. Scheduled Downtime and emergency maintenance as referred to in this Agreement is excluded from the calculation of Uptime.

"Uptime"

Uptime is defined as the percentage availability of the Hosting Service over the current calendar year excluding Scheduled Downtime.

"Scheduled Downtime"

Scheduled Downtime is planned routine maintenance for the deployment of Releases of the Service/Software to the Hosting Service or regular maintenance activities such as scheduled Hosting Service patching.

Hyland Disaster Recovery Environment ('DR Environment') provision operates as follows:

Backups are taken every 24 hours (overnight) In relation to the LIVE Environment of your LAMP based Hyland Software Products and used to refresh your DR Environment. The DR Environment for your Hyland Software Products is available during a LIVE Environment disaster event subject to DNS changes initiated and managed by you. The declaration of the disaster and the initiating of a switch to the DR Environment is subject to agreement between you and Hyland and will take place at an agreed time.
Any third-party integrations (including those in relation to Third Party Services) requiring special connectivity arrangements (VPN, IP whitelisting, etc.) will not work unless previously configured on both sides by the initiator (DR Environment) and the receiver (third party integration end-point) following prior cooperation between the parties of this Agreement for such arrangements and any such services shall be delivered (by Hyland or by its subcontractors) at Hyland's Professional Services rates.
During usage of the DR Environment, content changes can be made to the DR Environment by you but those changes will not be replicated back to the LIVE Environment when it is restored unless such a service has been agreed between the parties as an additional Professional Service.

Schedule 2

Subcontractors

The Hosting Service shall include the hosting by Hyland or Hyland's Third Party Services subcontractors of the Hosted Software together with the provision of such server maintenance services, infrastructure, hardware and bandwidth as are necessary to provide such Third Party Services in relation to the Service/Software. The following are a list of approved subcontractors and data processors Hyland may use. Hyland will notify you of any other alternative or additional third parties in writing:

Company Registration Number	Full name and trading name where applicable	Registered Address	Where data is stored	Purpose (in relation to products and services taken and paid for)
880665542	Amazon Web Services Inc ("AWS")	410 Terry Avenue North Seattle, WA 98109 United States	US	(1) Hosting for Service/Software and/or (2) Disaster Recovery site hosting for Hyland Software Products
4890547	Jadu Inc.	Jadu, Inc. 12022 Blue Valley Parkway, Overland Park, KS 66213, United States	Data remains stored in US	Support of the Service/Software

Please note that if the Contract Information indicates that this is a renewal of the Hosting Service and Hyland has previously provided such services using other third parties, those third parties will also remain as approved subcontractors.

Schedule 3

Customer Data processed in relation to the Agreement:

Description	Details
Subject matter of the processing	**Example:** Hosting Service and Hosting Support Service for (i) the Hyland Software Product Content Portal (CP); and (ii) your website(s) including subscription preferences for targeted email alerts.
Duration of the processing	**Example:** Commencement Date to any such time as the agreement is terminated.
Nature and purpose of the processing	**Example:** Provision of Hosting Service and Hosting Support Service of the products /services listed in "Subject matter of the processing" above. The nature of the processing generally relates to data hosting, system maintenance and upgrades but includes any operation such as, recording, storing, adapting, altering, retrieving, using, disclosing, disseminating, restricting, erasing, destroying or otherwise processing data held within the ICT systems. In terms of any Customer Data integrated with or through Third Party Services applications, you acknowledge full responsibility in relations to the lawful transfer, use, handling and storage of the same. Where Hyland transfers Customer Data on your behalf in pursuance of this Agreement, you have consented to the same as indicated in the agreement.

Type of Customer Data	**Example:** Examples include but are not limited to; name, address, email address, date of birth, contact details.
Categories of Data Subject	**Example:** Examples include but are not limited to; staff (including volunteers, agents, and temporary workers), customers/ clients, members of the public, website users.
Plan for return and destruction of the data once the processing is complete unless requirement under union or member state law to preserve that type of data	**Example:** At the end of the agreement instructions shall be issued defining the requirement to return and/or destruct data.

Exhibit B HYLAND CLOUD SERVICE AGREEMENT

As of the Effective Date, following attached schedules are a part of the Cloud Service Agreement and apply to the provision of the applicable products or services:

☒ General Terms Schedule
☒ Software-as-a-Service Schedule (includes Acceptable Use Policy Attachment and SAAS Security Attachment)

All products or services related to the cloud services which may be licensed or purchased by Customer from Naviant from time to time under a schedule shall be governed by this Cloud Service Agreement. Customer specifically represents and warrants to Naviant that Customer has read and understands all of the terms and conditions contained herein prior to entering into the Cloud Service Agreement.

GENERAL TERMS SCHEDULE

This General Terms Schedule ("General Terms" or "General Terms Schedule") will apply to the Hyland Cloud Service purchased from Naviant under this CSA. If there is a conflict between the terms of this General Terms Schedule and any other Schedule of this CSA, the other Schedule shall control with respect to the subject matter of such Schedule. In the event the same topic is addressed in both the General Terms Schedule and any other Schedule but the terms do not conflict, the terms of both the General Terms Schedule and the Schedule shall apply. Capitalized terms used in this General Terms Schedule may be defined within this Schedule or within other Schedules to which they are applicable.

1. DEFINED TERMS.

The defined terms below shall have the meaning ascribed to them below as used throughout the CSA.

"Consumption Fees" means the amounts payable by Customer for storage of data and information in the Hyland Cloud Service in excess of the data storage allocation set forth in the initial Statement of Work for the Hyland Cloud Service.

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

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

"Effective Date" means the date this CSA is signed by the last party that signs this CSA, as determined based upon the dates set forth after their respective signatures.

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

"Host Vendor" means Hyland Software, Inc. or one of its affiliates, and its successors and assigns. For clarity, the term "Hyland" as used in the SaaS Security Attachment means Host Vendor as defined herein.

"Hyland Cloud Service Support" means the services described in Section 5 of this Schedule.

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

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

"Hyland Cloud Service" means the Host Vendor's provision of Software and the Hyland Cloud Platform for use by Customer in accordance with the CSA, including this SaaS Schedule.

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

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

"Resolution" means Naviant provides Customer with a reasonable workaround, correction, or modification that solves or mitigates a reported Hyland Cloud Service issue or error.

"SaaS Fees" means the amounts invoiced by Naviant to Customer and payable by Customer to Naviant for the use of the Hyland Cloud Service. The initial SaaS Fees are set forth in the initial Statement of Work

“Service Class” means the service level commitment included as part of Hyland Cloud Service, as described in the Service Class Manual, and purchased by Customer as part of the Hyland Cloud Service**.**

“Service Class Manual” means the latest version of the manual describing any available Service Classes, as provided by Naviant from time to time.

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

“Statement of Work” means a statement of work entered into and executed by the parties describing the Software and professional services to be provided by Naviant to Customer.

“Testing Environment” means a separate instance of the Hyland Cloud Service (including Customer Data) hosted by Host Vendor, 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 and Hosted 3rd Party Software included in the Hyland Cloud Service.

“Testing Lite Environment” means a separate instance of the Hyland Cloud Service (including Customer Data) hosted by Host Vendor, 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 and Hosted 3rd Party Software included in the Hyland Cloud Service.

“Upgrades and Enhancements” means any and all new versions, improvements, modifications, upgrades, updates, fixes and additions to Software that Host Vendor makes available to Customer or to Host Vendor’s end users generally during the term of this 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, re-platformed Software or the professional services required to implement the change. Naviant 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 for Software, if and when released during the term of this CSA. Upgrades and Enhancements are not available for retired Software.

“Users” means Customer’s employees that access and use the Hyland Cloud Service.

2. TERM AND TERMINATION; CERTAIN EFFECTS OF EXPIRATION OR TERMINATION.

2.1 Naviant’s rights

3. PAYMENT TERMS.

3.1

5. OWNERSHIP AND PROHIBITED CONDUCT.

5.1 Ownership. Host Vendor and its suppliers own the Software, Documentation, and all components of the Hyland Cloud Services, 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 all components of the Hyland Cloud Services, are protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. No ownership rights in the Software, Documentation, or components of the Hyland Cloud Services are transferred to Customer. Customer agrees that nothing in this CSA or associated documents gives it any right, title or interest in the Software, any component of the Hyland Cloud Service or Documentation, except for the limited express rights granted in this CSA. Customer acknowledges and agrees that Host Vendor has the right, at any time, to change the specifications and operating characteristics of the Software and Hyland Cloud Service, and Host Vendor’s policies respecting Upgrades and Enhancements (including but not limited to its release process). THIS CSA IS NOT A WORK-FOR-HIRE AGREEMENT. At no time shall Customer file or obtain any lien or security interest in or on any components of the Software, Hyland Cloud Service or Documentation.

5.2 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, Documentation, Hyland Cloud Services or Hosted 3rd Party Software documentation; (b) sell, transfer, rent, lease or sub-license the Software, Documentation, Hyland Cloud Service or Hosted 3rd Party Software documentation to any third party; (c) alter or modify the Software, Hyland Cloud Services, Documentation or Hosted 3rd Party Software documentation; (d) reverse engineer, disassemble, decompile or attempt to derive source code from the Software, Documentation, Hyland Cloud Service or Hosted 3rd Party Software documentation, or prepare derivative works therefrom; or (e) use the Hyland Cloud Service or permit it to be used in violation of Host Vendor's Acceptable Use Policy in effect from time to time a copy of the current form of which is attached hereto as SaaS Security Attachment or for the purposes of evaluation, benchmarking, or other comparative analysis intended for external publication without Naviant or Host Vendor's prior written consent.

6. DISCLAIMER OF WARRANTIES.

6.1 EXCEPT FOR THE WARRANTIES PROVIDED BY NAVIANT AS EXPRESSLY SET FORTH IN THE SCHEDULES MADE PART OF THIS CSA, NAVIANT, HOST VENDOR AND ITS SUPPLIERS MAKE NO WARRANTIES OR REPRESENTATIONS REGARDING ANY SOFTWARE, DOCUMENTATION, OR ANY COMPONENT OF THE HYLAND CLOUD SERVICE (INCLUDING ANY SOFTWARE OR HARDWARE), PROVIDED UNDER THIS CSA. NAVIANT, HOST VENDOR 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. NAVIANT, HOST VENDOR AND ITS SUPPLIERS DO NOT WARRANT THAT ANY SOFTWARE, DOCUMENTATION, OR ANY COMPONENT OF THE HYLAND CLOUD SERVICE PROVIDED WILL SATISFY CUSTOMER'S REQUIREMENTS OR ARE WITHOUT DEFECT OR ERROR, OR THAT THE OPERATION OF ANY SOFTWARE, DOCUMENTATION, OR ANY COMPONENT OF THE HYLAND CLOUD SERVICE PROVIDED UNDER THIS CSA WILL BE UNINTERRUPTED. EXCEPT AS EXPRESSLY STATED IN THIS CSA, NAVIANT AND HOST VENDOR DO NOT ASSUME ANY LIABILITY WHATSOEVER WITH RESPECT TO ANY THIRD PARTY HARDWARE, FIRMWARE, SOFTWARE OR SERVICES.

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

6.3 Naviant AND HOST VENDOR MAKE NO WARRANTIES WITH RESPECT TO ANY SOFTWARE OR HYLAND CLOUD SERVICE USED IN ANY NON-PRODUCTION SYSTEM AND PROVIDES ANY SUCH SOFTWARE AND HYLAND CLOUD SERVICE "AS IS."

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

7. LIMITATIONS OF LIABILITY.

7.1 IN NO EVENT SHALL NAVIANT OR ITS DIRECT OR INDIRECT SUPPLIERS' (INCLUDING HOST VENDOR'S) AGGREGATE LIABILITY ARISING OUT OF OR IN CONNECTION WITH THIS CSA OR IN CONNECTION OR ANY USE OR INABILITY TO USE THE SOFTWARE OR HYLAND CLOUD SERVICE EXCEED THE AMOUNT OF THE FEES AND CHARGES ACTUALLY PAID BY CUSTOMER TO NAVIANT UNDER THIS CSA DURING THE 12-MONTH PERIOD IMMEDIATELY PRECEDING THE EVENT GIVING RISE TO SUCH LIABILITY. IN NO EVENT WILL NAVIANT OR ITS DIRECT OR INDIRECT SUPPLIERS (INCLUDING HOST VENDOR) BE LIABLE FOR ANY INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL OR PUNITIVE DAMAGES OR OTHER PECUNIARY LOSS, INCLUDING WITHOUT LIMITATION, LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF DATA OR INFORMATION OR THE COST OF RECOVERING SUCH DATA OR INFORMATION, THE COST OF SUBSTITUTE SOFTWARE, HARDWARE OR SERVICES, OR CLAIMS BY THIRD PARTIES, ARISING OUT OF OR IN CONNECTION WITH THIS CSA OR ANY USE OR INABILITY TO USE THE SOFTWARE OR HYLAND CLOUD SERVICE, EVEN IF NAVIANT OR SUCH SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITIES OF SUCH DAMAGES.

7.2 IF CUSTOMER USES THE SOFTWARE IN A CLINICAL SETTING, CUSTOMER ACKNOWLEDGES THAT THE SOFTWARE DOES NOT OFFER MEDICAL INTERPRETATIONS OF DATA, DIAGNOSE PATIENTS, OR RECOMMEND THERAPY OR TREATMENT; THE SOFTWARE IS AN INFORMATION RESOURCE AND IS NOT A

SUBSTITUTE FOR THE SKILL, JUDGMENT AND KNOWLEDGE OF THE CUSTOMER'S USERS OF THE SOFTWARE IN THE PROVISION OF HEALTHCARE SERVICES. IN ADDITION TO THE LIMITATIONS OF LIABILITY PROVIDED HEREIN, NAVIANT AND HOST VENDOR SHALL NOT HAVE ANY LIABILITY FOR ANY ASPECT OF CUSTOMER'S SERVICES PROVIDED IN CONJUNCTION WITH ITS USE OF THE SOFTWARE.

7.3 Force Majeure. No failure, delay or default in performance of any obligation of a party to this CSA (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 6 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 CSA 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 CSA.

8. GENERAL PROVISIONS.

8.2 Interpretation. The headings used in this CSA 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 CSA 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 CSA.

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 CSA, including any and all exhibits and schedules referred to herein or order form referencing this CSA, 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. Customer acknowledges and agrees in entering into the CSA and its purchases hereunder are not contingent on the availability of any future functionality, features, programs, or services. This CSA may only be modified by a written document signed by duly authorized representatives of the parties. This CSA shall not be supplemented or modified by any course of performance, course of dealing or trade usage. Customer and Naviant specifically acknowledge and agree that any other terms varying from or adding to the terms of this CSA, whether contained in any purchase order or other electronic, written or oral communication made from Customer to Naviant are rejected and shall be null and void and of no force or effect, unless expressly agreed to in writing by both parties. This CSA will prevail over any conflicting stipulations contained or referenced in any other document.

8.9 Export. Regardless of any disclosure made by Customer to Naviant of an ultimate destination of any components of the Hyland Cloud Service, 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 Hyland Cloud Service 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 Hyland Cloud Service (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 Hyland Cloud Service (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.

8.10 Injunctive Relief. The parties to this CSA recognize that a remedy at law for a breach of the provisions of this CSA 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 of this CSA.

8.11 Counterparts. This CSA may be executed in one or more counterparts, all of which when taken together shall constitute one and the same instrument.

8.12 Expenses. Except as otherwise specifically provided herein, each party shall bear and pay its own expenses incurred in connection with this CSA and the transactions contemplated hereby.

8.13 Third Parties. 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 CSA; provided, however, that third party suppliers of software products bundled with the Software are third party beneficiaries to this CSA as it applies to their respective software products.

SOFTWARE-AS-A-SERVICE SCHEDULE

As of the Effective Date, this Schedule ("SaaS Schedule") is part of the Cloud Service Agreement (CSA) entered into between Customer and Naviant.

1. HYLAND CLOUD SERVICE

1.1 General. During the term of this CSA, (a) Naviant will make the Hyland Cloud Service available to Customer pursuant to this SaaS Schedule, the SaaS Security Attachment, Documentation and the applicable Service Class Manual; and (b) Naviant and Host Vendor will only use Customer Data to provide, develop, and improve the Hyland Cloud Service and other services, to prevent or address service or technical problems, or in accordance with Customer's instructions.

Customer acknowledges that if and when Customer delegates or relies on Naviant to perform certain tasks for obligations as they relate to the SaaS Security Attachment, Host Vendor will rely on Naviant in the same way it relies on Customer as described in the SaaS Security Attachment.

1.2 Service Class. Prior to or on the Effective Date, Naviant has delivered a then-current copy of the applicable Service Class Manual to Customer. After the Effective Date, Naviant will have the right to modify the applicable 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 Naviant provides written notice to Customer informing Customer of such modifications or revisions. Notwithstanding the foregoing, no modifications of any Service Class Manual relating to Customer's then-current Service Class will be effective until the next renewal of this CSA. The initial Service Class purchased by Customer is set forth in the initial Statement of Work. Customer may upgrade the Service Class at any time, but may downgrade such Service Class only after the expiration of the Initial Term. 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 CSA. To modify a Service Class selection, Customer must submit a purchase order indicating the new Service Class.

1.3 Return of Customer Data and Deletion. Upon termination or expiration of this CSA for any reason:

(a) Upon written request by Customer to Naviant sent to Naviant Customer Success Team at support@naviant.com, made within thirty (30) days after the effective date of any such termination or expiration, for Customer Data extraction services to be billed in accordance with Naviant's time and materials prices set forth in the Software Support Level agreement ("Notice of Return of Customer Data"), Naviant will either: (1) return Customer Data to Customer by providing: Customer Data on one (1) or more encrypted hard drives or other similar media and an export file containing the relevant keyword values and related file locations for the Customer Data or (2) make available to Customer the Customer Data for extraction by Customer. Naviant will work with Customer on determining the extraction method most suitable to meet Customer's requirements. Customer acknowledges and agrees that thirty (30) days after Naviant has sent or made available to Customer the Customer Data, Naviant 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 Host Vendor's datacenters, including all replicated copies.

(b) Upon written request by Customer to Naviant sent to Naviant Customer Success Team at support@naviant.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"), Naviant will have no obligation to maintain or provide any Customer Data and shall thereafter, unless legally prohibited, delete all Customer Data from all of Host Vendor's datacenters, including all replicated 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 CSA, Naviant will have no obligation to maintain or provide any Customer Data and shall thereafter, unless legally prohibited, delete all Customer Data from all of Host Vendor's datacenters, including all replicated copies.

1.4 Data Location. Hyland Cloud Services shall store Customer Data at data centers located in the Customer's home country. Naviant or Host Vendor may, at its expense, change the location of the Customer Data to other data centers; provided that such locations remain in that country.

1.5 Subcontract of Hyland Cloud Service. Customer acknowledges and agrees that Naviant shall subcontract to Host Vendor the provision of the Hyland Cloud Service and fulfillment of all other obligations under this Section.

1.6 Customers may license some Software as part of the Hyland Cloud Service, and other Software which is implemented only on the customer's premise (or a third party cloud other than the Hyland Cloud Platform), such as Hyland RPA ("On-Premise Software"). For clarity, if Customer licenses On-Premise Software from Naviant, this SaaS Schedule does not apply to such On-Premise Software.

2. GRANT OF RIGHTS.

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

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

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

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

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

2.5 Audit Rights. Naviant shall be permitted access to assess Customer's use of the Hyland Cloud Service in order to determine Customer's compliance with the grant of use and pricing terms of the CSA, including, where applicable, to measure Customer's volume usage. Customer shall reasonably cooperate with Naviant with respect to its performance of such assessment.

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

2.7 Ownership of Customer Data. As between Naviant and Customer, Customer owns Customer Data.

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

5. HYLAND CLOUD SERVICE SUPPORT.

5.1 HYLAND CLOUD SERVICE SUPPORT TERMS. Naviant will provide Hyland Cloud Service Support in accordance with this Section.

(a) Technical Support Services. Naviant will provide telephone or online technical support related to problems reported by Customer in connection with a defect in the Software.

(b) Error Correction Services. With respect to any issues or errors in the Hyland Cloud Service which are reported by Customer and which are confirmed by Naviant, Naviant will engage Host Vendor to use reasonable efforts to correct such issue or error, which may be affected by a reasonable workaround. Naviant shall commence to confirm any reported issues or errors after receipt of a proper report of such suspected issue or error from Customer. Host Vendor may elect to correct the issue or error by updating or upgrading the applicable component of the Hyland Cloud Service to a new build or version.

(c) Reporting Policies and Procedures Applicable to Technical Support Services and Error Correction Services.

(1) Customer Reporting Requirements. When requesting Hyland Cloud Service Support, Customer will submit such requests in accordance with Naviant's then-current reporting procedures Hyland Cloud Service Support generally will be available during the hours of 7:00 a.m. to 7:00 p.m., CST Time, Monday through Friday, excluding holidays, or as otherwise provided by Naviant to its customers, by on-line connectivity, telephonically or both. In the case of reporting a problem, issue, or error with the Hyland Cloud Service, Customer will provide Naviant with as much information and access to systems as reasonably possible to enable Naviant to investigate and attempt to identify and verify the problem, issue or error. Customer will work with Naviant support personnel during the problem isolation process, as reasonably needed. Customer will notify Naviant of any configuration changes it has made

to the Hyland Cloud Service, such as workflow configuration changes, network installation/expansion, integrations, upgrades, relocations, etc.

(2) Response Procedures. Naviant shall respond to all reports in accordance with Naviant's procedures and Naviant's obligations for a reported issue or error concludes upon delivery of a Resolution.

(d) Software Upgrades and Enhancements. Naviant will make available, in accordance with Host Vendor's then current policies, all Upgrades and Enhancements to the Software, if and when released during the term of this CSA. Professional services required to implement the Software Upgrades and Enhancements are excluded and will be charged separately.

Customer acknowledges and agrees that for regulatory compliance purposes, **Naviant** may be required to engage Host Vendor under a services agreement to implement Upgrades and Enhancements to a regulated product. If Host Vendor offers a self-service option for implementing Upgrades and Enhancements to a regulated product, and the Customer chooses this option, Customer agrees to comply with the training, reporting, and documentation requirements established by Host Vendor to ensure that the implementation is performed and documented as required by applicable regulations.

(e) Update, Upgrade, Change or Replacement of Components of the Hyland Cloud Service. Host Vendor may update or upgrade the build or version of the Software used in the Hyland Cloud Service from time to time at Host Vendor's expense. Host Vendor also may change, replace, update or upgrade the Hyland Cloud Platform from time to time. Customer agrees to collaborate with Host Vendor and assist Host Vendor in connection with the completion of installation and testing of any update or upgrade related to the Hyland Cloud Service.

5.2 EXCLUSIONS.

Generally. Naviant is not responsible for providing, or obligated to provide, Hyland Cloud Service Support: (1) 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 the Hyland Cloud Service or from any error or defect in any configuration of any component of the Hyland Cloud Service, which activities in any such case were undertaken by any party other than Naviant or Host Vendor; (2) in connection with any error or defect or problem in any other component of the Hyland Cloud Service if Host Vendor has previously made available corrections for such error or defect which Customer fails to implement; (3) 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 Hyland Cloud Service; (4) if any party other than Naviant or Host Vendor has provided any services in the nature of Hyland Cloud Service Support to Customer with respect to the Hyland Cloud Service; or (5) in connection with any questions related to the operation or use of the Software application programming interfaces (APIs).

6. SECURITY. During the term of this CSA, Host Vendor shall maintain a security program which shall conform to the SaaS Security Attachment, attached hereto.

7. CERTAIN RESPONSIBILITIES AND OBLIGATIONS OF CUSTOMER.

7.1 Customer Responsibilities. In connection with the relationship established between Customer and **Naviant** under this CSA:

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

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

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

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

(e) Customer shall prohibit unauthorized access to, or use of, the Hyland Cloud Service and shall notify **Naviant** promptly of any such unauthorized access or use;

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

(g) Customer designates the initial Customer Security Administrator as ____[CUSTOMER TO COMPLETE WITH INDIVIDUAL'S NAME AND EMAIL]. Customer acknowledges that Naviant may also designate one or more Customer Security Administrators to interact directly with Host Vendor regarding Customer's Hyland Cloud Service. "Customer Security Administrators" (also referred to as "CSA" or "CSAs") are individuals designated by Customer or Naviant who are authorized to submit Hyland Cloud Service configuration change requests, speak authoritatively on behalf of Customer's Hyland Cloud Services and shall receive and provide, as applicable, all notifications related to maintenance, security, service failures and the like. Customer further acknowledges that where Naviant acts on behalf of Customer as it relates to actions or obligations under the SaaS Security Schedule, Host Vendor will rely on Naviant as if Naviant were Customer in such instances.

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

7.2 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 Hyland Cloud Service. Naviant shall have no responsibility or liability under this CSA, including this SaaS Schedule, for any unavailability or failure of, or nonconformity or defect in, the Hyland Cloud Service that is caused by or related in any manner to any failure of Customer to obtain and maintain all such software, hardware, equipment and relationships.

8. LIMITED WARRANTIES.

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

8.2 Hyland Cloud Service Warranty Remedy. Naviant's sole and exclusive remedy for any non-conformities to the express limited warranties under Section 8.1 shall be as follows: provided that Customer notifies Naviant in writing of the non-conformity, Naviant will either (a) correct the non-conforming component of the Hyland Cloud Service, which may include the delivery of a reasonable workaround for the non-conformity; or (b) if Naviant determines that correcting the non-conformity is not practicable, then terminate this CSA with respect to the non-conforming component, in which event, upon compliance by Customer with its obligations under Section 1.3 of the General Terms Schedule, Naviant will provide a refund to Customer of the "unused portion of pre-paid SaaS Fees" (as defined below) paid by Customer and attributable to the non-conforming component. The "unused portion of the prepaid SaaS Fees" shall mean an amount equal to the total SaaS Fees paid by Customer for the non-conforming portion of the Hyland Cloud Service for the then current term (or applicable twelve-month period within the Initial Term) during which such removal occurs, multiplied by a fraction, the numerator of which shall be the number of full calendar months remaining during the term (or applicable twelve-month period within the Initial Term) during which such removal occurs, and the denominator of which shall be twelve (12).

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

9. COMPLIANCE WITH LAWS. Naviant agrees to comply in all material respects with all laws applicable to Naviant in its performance of services under this SaaS Schedule.

10. INFRINGEMENT INDEMNIFICATION.

10.1 Generally. Host Vendor 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 Hyland Cloud Service of any patent, registered copyright or registered trademark of a third party, provided that Host Vendor: (a) is notified promptly after Customer receives notice of such claim; (b) is solely in charge of the defense of and any settlement negotiations with respect to such claim, provided, that Host Vendor 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 the Customer 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 (in the opinion of Host Vendor) of the occurrence of a finding of infringement or misappropriation, either to procure for Customer the right to continue use of the Hyland Cloud Service, or to replace the relevant portions of the Hyland Cloud Service with other equivalent, non-infringing portions. If Host Vendor is unable to accomplish either of the options set forth in subsection (d) of the preceding sentence, Host Vendor shall terminate this Agreement or this SaaS Schedule (as the case may be) upon thirty (30) days advance written notice to Customer and refund to Customer the "unused portion of prepaid SaaS Fees" as defined below paid during the then current term (or applicable twelve-month period within the Initial Term). For these purposes, the "unused portion of prepaid SaaS Fees" shall mean an amount equal to the total SaaS Fees paid by Customer for the term (or applicable twelve-month period within the Initial Term) during which termination occurs, multiplied by a fraction, the numerator of which shall be the number of full calendar months remaining during the term (or applicable twelve-month period within the Initial Term) during which such termination occurs, and the denominator or which shall be twelve (12). Notwithstanding anything to the contrary, Host Vendor shall have no obligation to indemnify Customer against any claims made against Customer and otherwise described in this Section that arise from: (v) any Customer Data; (w) use of the Hyland Cloud Service other than as expressly permitted herein; (x) the combination of the Hyland Cloud Service or any component thereof with any product not furnished by Host Vendor; (y) the modification or addition of any component of the Hyland Cloud Service, other than by Host Vendor or any of its authorized channel partners specifically retained by Host Vendor to provide such modification or addition; or (z) the Customer's business methods or processes.

10.2 THIS SECTION STATES HOST VENDOR'S ENTIRE LIABILITY AND THE SOLE AND EXCLUSIVE REMEDY OF CUSTOMER WITH RESPECT TO ANY ALLEGED INFRINGEMENT OR MISAPPROPRIATION OF INTELLECTUAL PROPERTY OR PROPRIETARY PROPERTY BY THE HYLAND CLOUD SERVICE.

ACCEPTABLE USE POLICY ATTACHMENT

1. INTRODUCTION.

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

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

2. USER OBLIGATIONS.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

SAAS SECURITY ATTACHMENT

Introduction: Hyland maintains and manages a comprehensive written security program that covers the Hyland

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

1. Risk Management.
   a. Conducting an annual risk assessment designed to identify threats and vulnerabilities in the administrative, physical, legal, regulatory, and technical safeguards used to protect the Hyland Cloud Service.
   b. Maintaining a documented risk remediation process to assign ownership of identified risks, establish remediation plans and timeframes, and provide for periodic monitoring of progress.
2. Information Security Program.
   a. Maintaining a documented comprehensive Hyland Cloud Service information security program. This program will include policies and procedures based on industry standard practices, which may also include ISO 27001/27002, or other equivalent standards.
   b. Such information security program shall include, as applicable: (i) adequate physical and cyber security where Customer Data will be processed and/or stored; (ii) reasonable precautions taken with respect to Hyland personnel employment.
   c. These policies will be reviewed and updated by Hyland management annually.
3. Organization of Information Security. Assigning security responsibilities to appropriate Hyland individuals or groups to facilitate protection of the Hyland Cloud Service and associated assets.
4. Human Resources Security.
   a. Hyland employees undergo comprehensive screening during the hiring process. Background checks and reference validation will be performed to determine whether candidate qualifications are appropriate for the proposed position. Subject to any restrictions imposed by applicable law and based on jurisdiction, these background checks include criminal background checks, employment validation, and education verification as applicable.
   b. Ensuring all Hyland employees are subject to confidentiality and non-disclosure commitments before access is provisioned to the Hyland Cloud Service or Customer Data.
   c. Ensuring applicable Hyland employees receive security awareness training designed to provide such employees with information security knowledge to provide for the security, availability, and confidentiality of Customer Data.
   d. Upon Hyland employee separation or change in roles, Hyland shall ensure any Hyland employee access to the Hyland Cloud Service is revoked in a timely manner and all applicable Hyland assets, both information and physical, are returned.
5. 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 Hyland media handling procedures to ensure media containing Customer Data as part of the Hyland Cloud Service is encrypted and stored in a secure location subject to strict physical access controls.
   c. When a Hyland Cloud Service storage device has reached the end of its useful life, procedures include a decommissioning process that is designed to prevent Customer Data from being exposed to unauthorized individuals using the techniques recommended by NIST to destroy data as part of the decommissioning process.
   d. If a Hyland storage device is unable to be decommissioned using these procedures, the device will be virtually shredded, degaussed, purged/wiped, or physically destroyed in accordance with industry-standard practices.
6. Access Controls.
   a. Maintaining a logical access policy and corresponding procedures. The logical access procedures will define the request, approval and access provisioning process for Hyland personnel. The logical access process will restrict Hyland user (local and remote) access based on Hyland user job function (role/profile based, appropriate access) for applications and databases. Hyland user access recertification to determine access and privileges will be performed periodically. Procedures for onboarding and offboarding Hyland personnel users in a timely manner will be documented. Procedures for Hyland personnel user inactivity threshold leading to account

suspension and removal threshold will be documented.

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

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

7. System Boundaries.

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

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

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

8. Encryption.

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

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

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

9. Physical and Environment Security.

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

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

10. Operations Security.

a. Maintaining documented Hyland cloud operating procedures.

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

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

d. Utilizing virus and malware protection technologies, which are configured to meet common industry standards designed to protect the Customer Data and equipment located within the Hyland Cloud Platform 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 location.

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

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

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

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

11. Communications Security.

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

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

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

13. Security Incident.

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

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

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

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

e. Hyland will notify Customer of a Security Incident within 48 hours. A "Security Incident" means a determination by Hyland of an actual disclosure of unencrypted Customer Data to an unauthorized person or entity that compromises the security, confidentiality, or integrity of the Customer Data.

14. Information Security Aspects of Business Continuity Management.

a. Maintaining a business continuity and disaster recovery plan.

b. Reviewing and testing this plan annually.

15. Aggregated Data.

a. Hyland owns all aggregated, anonymized and statistical data derived from the operation of the Hyland Cloud Service, including without limitation, the number of records in the Hyland Cloud Service, the number and types of transactions, configurations, and reports processed as part of the Hyland Cloud Service and the performance results of the Hyland Cloud Service (the "Aggregated Data").

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

16. Audit and Security Testing.

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

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

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

d. Customer may conduct penetration testing against the public URL used to access the Hyland Cloud Service 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 Hyland Cloud Service. Customer is prohibited from distributing or publishing the results of such penetration testing to any third party without Hyland's prior written approval.

Exhibit C CERTIFICATE OF LIABILITY INSURANCE

DATE (MM/DD/YYYY)
7/29/2025

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
M3 Insurance Solutions, Inc.
828 John Nolen Drive
Madison, WI 53713

CONTACT NAME: JD Leisemann
PHONE (A/C, No, Ext): 800-272-2443 **FAX (A/C, No):**
E-MAIL ADDRESS: jd.leisemann@m3ins.com

INSURER(S) AFFORDING COVERAGE	NAIC #
INSURER A : Citizens Insurance Company of	31534
INSURER B : The Hanover Insurance Company	22292
INSURER C :	
INSURER D :	
INSURER E :	
INSURER F :	

INSURED NAVIINC-01
Naviant, LLC
201 Prairie Heights Drive
Verona, WI 53593

COVERAGES **CERTIFICATE NUMBER:** 1215929307 **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 GEN'L AGGREGATE LIMIT APPLIES PER: ☒ POLICY □ PRO-JECT □ LOC OTHER:	Y	Y	ZB1-H902365 03	1/27/2025	1/27/2026	EACH OCCURRENCE	$ 2,000,000
							DAMAGE TO RENTED PREMISES (Ea occurrence)	$ 300,000
							MED EXP (Any one person)	$ 10,000
							PERSONAL & ADV INJURY	$ 2,000,000
							GENERAL AGGREGATE	$ 4,000,000
							PRODUCTS - COMP/OP AGG	$ 4,000,000
								$
A	AUTOMOBILE LIABILITY □ ANY AUTO □ OWNED AUTOS ONLY □ SCHEDULED AUTOS ☒ HIRED AUTOS ONLY ☒ NON-OWNED AUTOS ONLY			ZB1H902365	1/27/2025	1/27/2026	COMBINED SINGLE LIMIT (Ea accident)	$ 1,000,000
							BODILY INJURY (Per person)	$
							BODILY INJURY (Per accident)	$
							PROPERTY DAMAGE (Per accident)	$
								$
B	☒ UMBRELLA LIAB ☒ OCCUR EXCESS LIAB □ CLAIMS-MADE DED ☒ RETENTION $ 0	Y	Y	UH1-H902366 03	1/27/2025	1/27/2026	EACH OCCURRENCE	$ 10,000,000
							AGGREGATE	$ 10,000,000
								$
A B	WORKERS COMPENSATION AND EMPLOYERS' LIABILITY Y / N ANYPROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? □ (Mandatory in NH) If yes, describe under DESCRIPTION OF OPERATIONS below	N / A	Y	WB1H868383 WH1H902426	1/27/2025 1/27/2025	1/27/2026 1/27/2026	☒ 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
B	Tech E&O/Cyber			LH1 H902721 02	1/27/2025	1/27/2026	Each Claim Aggregate Limit	10,000,000 10,000,000

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

Contract #: TECHS-202580661

As required by written contract, the City and County of Denver, its Elected and Appointed Officials, Employees and Volunteers are included as Additional Insured, with respect to the General Liability. As required by written contract, Waiver of Subrogation in favor of the City and County of Denver, its Elected and Appointed Officials, Employees and Volunteers applies, with respect to the General Liability and Workers' Compensation policies. Umbrella follows form. 30 Day Notice of Cancellation applies per policy provisions.

CERTIFICATE HOLDER

City and County of Denver
Department of Technology Services
201 W. Colfax Ave. Dept. 301
Denver, CO 80202

CANCELLATION

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

EXHIBIT D, INFORMATION TECHNOLOGY PROVISIONS

This Exhibit regarding Information Technology Provisions (this "Exhibit") is a material part of the Agreement between the Parties to which this Exhibit is attached. In addition to the requirements of the main body of this Agreement, the Contractor shall protect the City's information technology resources and City Data in accordance with this Exhibit. All provisions of this Exhibit that refer to the Contractor shall apply equally to any Subcontractor performing work in connection with this Agreement. Unless the context clearly requires a distinction between the Agreement and this Exhibit, all references to "Agreement" shall include this Exhibit.

1. TECHNOLOGY SERVICES SPECIFICATIONS

1.1. User ID Credentials: Internal corporate or customer (tenant) user account credentials shall be restricted, ensuring appropriate identity, entitlement, and access management and in accordance with established policies and procedures, as follows:

1.1.1. Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and Federation);

1.1.2. Account credential lifecycle management from instantiation through revocation;

1.1.3. Account credential and/or identity store minimization or re-use when feasible; and

1.1.4. Adherence to industry acceptable and/or regulatory compliant authentication, authorization, and accounting (AAA) rules (e.g., strong/multi-factor, expire able, non-shared authentication secrets).

1.2. Identity Management: The City's Identity and Access Management ("IdM") system is an integrated infrastructure solution that enables many of the City's services and online resources to operate more efficiently, effectively, and securely. All new and proposed applications must utilize the authentication and authorization functions and components of IdM. Strong authentication is required for privileged accounts or accounts with access to sensitive information. This technical requirement applies to all solutions regardless of where the application is hosted.

1.3. Supported Releases: The Contractor shall maintain the currency of all third-party software used in the development and execution or use of the Work with third-party vendor approved and supported releases, including, but not limited to, all code libraries, frameworks, components, and other products (e.g., Java JRE, code signing certificates, .NET, jQuery plugins, etc.), whether commercial, free, open-source, or closed-source. This includes any of the Contractor's controlled systems running on the City's network, including, but not limited to, any application, firewall, or other type of physical or virtual appliances.

1.4. Updates & Upgrades: During the Term of this Agreement, upon the request of the City, the Contractor shall provide the City with copies of all new versions, updates, and upgrades of the On-Premise Software (collectively, "Upgrades"), without additional charge outside of the maintenance fees of the Software Support Level Agreement agreed upon by the parties, promptly after commercial release. Upon delivery to the City, Upgrades will become part of the On-Premise Software and will be subject to the license and other terms of this Agreement applicable to such

On-Premise Software. In addition, the Contractor shall ensure that SaaS receives all updates and upgrades the Contractor provides to its customers generally.

1.5. **Compatibility with Third-Party Software**: The Contractor acknowledges and agrees that the Work relating to its product must integrate and operate compatibly with various third-party software products. The Contractor shall actively monitor and stay current on new version releases, updates, and changes made to any such third-party software that interfaces or integrates with the Contractor's Work. The Contractor shall ensure that its own products remain fully compatible with the most recent generally available versions of these third-party software components. Within ninety (90) days of the commercial release of a new generally available version of any interfacing third-party software, the Contractor shall complete all necessary testing, coding, and product updates to certify compatibility with the new version. The Contractor shall provide the updated and version-compatible products to the City at no additional cost outside of the maintenance fees of the Software Support Level Agreement agreed upon by the parties. If the Contractor's Work is not compatible with the most current generally available third-party software versions required for operation, the City reserves the right to temporarily cease using the incompatible Work until the compatibility issue is resolved, without penalty or payment for a period of noncompliance. Under no circumstances shall the Contractor require the City to run old, non-current versions of third-party software to remain compatible with the Contractor's Work. The responsibility and costs for ensuring third-party software version compatibility shall reside solely with the Contractor.

1.6. **Adjustment of Licenses**: The City may, at each anniversary date of this Agreement, increase or decrease the number of licenses it has purchased under this Agreement by giving written notice to the Contractor at least thirty (30) days prior to the anniversary date. The Contractor shall adjust the invoice for the next billing period based on the unit price per license specified in this Agreement. The City shall not reduce the number of licenses below the minimum quantity required under this Agreement. The City will be responsible for any additional costs that may be incurred due to the additional licenses. Any adjustment to the number of licenses may only occur at the execution of an annual renewal term.

1.7. **Timing of Fees and Subscriptions**: Notwithstanding any provision to the contrary: (i) no fees for maintenance of On-Premise Software or SaaS, including without limitation for Upgrades, will accrue before Go-Live (as defined below); and (ii) no period before Go-Live will be counted against the time covered by any maintenance period. In addition, no fees for use of SaaS will accrue before Go-Live, and no period before Go-Live will be counted against the time covered by any SaaS subscription fees. “Go-Live” refers to the earlier of Acceptance of the On-Premise Software or SaaS or the City’s first use of the On-Premise Software or SaaS in production, other than a beta use or trial.

1.8. **Performance Outside of the United States**: If applicable, the Contractor shall request written approval from the City to perform, or subcontract to perform, Services outside the United States. The City may approve or deny such request within the City’s sole discretion. Any notice or term in any Exhibit provided to the City by the Contractor regarding performance outside the United

States shall be deemed ineffective and void if the City has not granted prior written approval for such performance. This prohibition shall also apply to using, processing, transmitting, or maintaining City Data outside of the United States. Notwithstanding anything to the contrary contained in the Agreement, the City shall have no responsibility or obligation to comply with foreign data protection laws or polices, including, but not limited to, the General Data Protection Regulation of the European Union.

1.9. <u>Continuity of Critical Services</u>: The Contractor acknowledges that the Work to be performed under this Agreement is vital to the City and must be continued without interruption and that, upon this Agreement's expiration without renewal, a successor, either the City or another contractor, may continue them. The Contractor agrees to: (i) furnish phase-in training; and (ii) exercise its best efforts and cooperation to complete an orderly and efficient transition to a successor. The Contractor shall, upon the City's written notice: (i) furnish phase-in, phase-out services for up to sixty (60) days after this Agreement expires; and (ii) negotiate in good faith to determine the nature and extent of phase-in, phase-out services required. The Contractor shall provide sufficient experienced personnel during the phase-in, phase-out period to ensure that the Work called for by this Agreement are maintained at the required level of proficiency. The Contractor shall be reimbursed for all reasonable phase-in, phase-out costs (i.e., costs incurred within the agreed period after expiration that result from phase-in, phase-out operations) at the rates contained herein. The City shall have the authority extend this Agreement monthly if additional time is required beyond the termination of this Agreement, if necessary, to effectuate the transition, and the City shall pay a proration of the subscription fee and any additional support service costs required for the phase out after termination during any necessary extension.

1.10. <u>Software Escrow</u>: At the City's request, the Contractor shall maintain in escrow a copy of the source code and documentation for the licensed software purchased under this Agreement. With each new release of the software provided to the City, the Contractor shall maintain the updated source code and documentation in escrow. If the Contractor files for bankruptcy, becomes insolvent, or ceases operations for any reason, the City shall be provided the current source code and documentation in escrow. The City will only use the source code and documentation to support the licensed software. This Section shall survive the termination of this Agreement.

2. <u>SECURITY AUDITS</u>

2.1. <u>Performance of Security Audits</u>: As provided for in the Contractor's Work Fees, prior to the Effective Date of this Agreement, the Contractor, will at its expense conduct or have conducted or have received certifications of compliance from its third party software providers that they have conducted, the following, at least once per year, and immediately after any actual or reasonably suspected Security Breach: (i) a SSAE 18/SOC 2 Type 2 or other mutually agreed upon audit of the Contractor's security policies, procedures and controls; (ii) a quarterly external and internal vulnerability scan of the Contractor's systems and facilities, to include public facing websites, that are used in any way to deliver Services under this Agreement. The report must include the vulnerability, age, and remediation plan for all issues identified as critical or high; and (iii) a formal penetration test performed by qualified personnel of the Contractor's systems and facilities that are used in any way to deliver Work under this Agreement. The Contractor will provide the City the results of the above audits. The Contractor shall also protect data against deterioration or degradation of quality and authenticity by, at minimum, having a third party perform annual data integrity audits. In addition, the Contractor shall comply with the City's annual risk assessment and the results thereof.

2.2. **Security Audit Results**: If applicable, the Contractor will provide the City the reports or other documentation resulting from the above audits, certifications, scans, and tests within seven (7) business days of the Contractor's receipt of such results. The report must include the vulnerability, age, and remediation plan for all issues identified as critical or high. Based on the results and recommendations of the above audits, the Contractor will, within thirty (30) calendar days of receipt of such results, promptly modify its security measures to meet its obligations under this Agreement and provide the City with written evidence of remediation. The City may require, at the Contractor's expense, that the Contractor perform additional audits and tests, the results of which will be provided to the City within seven (7) business days of Contractor's receipt of such results. To the extent the Contractor controls or maintains information systems used in connection with this Agreement, the Contractor shall provide the City with the results of all security assessment activities when conducted on such information systems, including any code-level vulnerability scans, application-level risk assessments, and other security assessment activities as required by this Agreement or reasonably requested by the City. The Contractor will remediate any vulnerabilities to comply with its obligations hereunder. If additional funds are required to perform the tests required by the City that are not accounted for in this Agreement, the Parties agree to amend this Agreement as necessary.

3. DATA MANAGEMENT AND SECURITY

3.1. **Compliance with Data Protection Laws and Policies**: In addition to the compliance obligations imposed by this Agreement, the Contractor shall comply with all information security and privacy obligations imposed by any federal, state, or local statute or regulation, or by any specifically incorporated industry standards or guidelines, as applicable to the Contractor under this Agreement, including, without limitation, applicable industry standards or guidelines based on the data's classification relevant to the Contractor's performance hereunder. If the Contractor becomes aware that it cannot reasonably comply with the terms or conditions contained herein due to a conflicting law or policy, the Contractor shall promptly notify the City.

3.2. **Data Ownership**: Unless otherwise required by law, the City has exclusive ownership of all City Data under this Agreement, and the Contractor shall have no right, title, or interest in City Data. The Parties recognize and agree that the Contractor is a bailee for hire with respect to City Data. The Contractor's use and possession of City Data is solely on the City's behalf, and the Contractor shall only use City Data solely for the purpose of performing its obligations hereunder and shall not use City Data in the development of machine learning and artificial intelligence models for any purpose without the City's written consent. The City retains the right to access and retrieve City Data stored on the Contractor's infrastructure at any time during the Term. All City Data created and/or processed by the Work, if any, is and shall remain the property of the City and shall in no way become attached to the Work. This Agreement does not give a Party any rights, implied or otherwise, to the other's data, content, or intellectual property, except as expressly stated in this Agreement.

3.3. **Data Access and Integrity**: The Contractor shall implement and maintain all appropriate administrative, physical, technical, and procedural safeguards necessary and appropriate to ensure compliance with the applicable law and regulation as they relate to the Contractor's performance hereunder to ensure the security and confidentiality of City Data. The Contractor shall protect against threats or hazards to the security or integrity of data; protect against unauthorized disclosure, access to, or use of data; restrict access to data as necessary; and ensure the proper and legal use of data. The Contractor shall provide the City with access, subject to the Contractor's reasonable security requirements, for purposes of inspecting and monitoring access and use of City Data and evaluating security control effectiveness. The Contractor shall not engage in "data mining" except as specifically and expressly required by law or authorized in writing by the City. Upon written request, the Contractor shall provide the City its policies and procedures to maintain the confidentiality of City Data.

3.4. **Response to Legal Orders for City Data**: If the Contractor is required by a court of competent jurisdiction or administrative body to disclose City Data, the Contractor shall first notify the City and, prior to any disclosure, cooperate with the City's reasonable requests in connection with the City's right to intervene, quash, or modify the legal order, demand, or request, and upon request, provide the City with a copy of its response. Upon notice, the City will promptly coordinate with the Contractor regarding the preservation and disposition of any City Data and records relevant to any current or anticipated litigation. If the City receives a subpoena, legal order, or other legal demand seeking data maintained by the Contractor, the City will promptly provide a copy to the Contractor. Upon notice and if required by law, the Contractor shall promptly provide the City with copies of its data required for the City to meet its necessary disclosure obligations.

3.5. **Mandatory Disclosures**: In addition to the requirements set forth herein, the Contractor shall provide the City with a copy of any disclosure the Contractor is required to file with any regulatory body as a result of a Security Breach or other incident that requires the Contractor to make such a disclosure, including but not limited to, required disclosures mandated by the Securities and Exchange Commission. If the contents of any such disclosure is protected by law, the Contractor shall instead provide the City with prompt notice that it was required to make such a disclosure along with the name of the regulatory body requiring the Contractor to make such a disclosure.

3.6. **Data Retention, Transfer, Holds, and Destruction**: Using appropriate and reliable storage media, the Contractor shall regularly backup data used in connection with this Agreement and retain such backup copies as necessary to meets its obligations hereunder. All City Data shall be encrypted in transmission, including by web interface, and in storage by an agreed upon National Institute of Standards and Technology ("NIST") approved strong encryption method and standard. Upon the expiration or termination of this Agreement, the Contractor shall, as directed by the City, promptly return all City Data provided by the City to the Contractor, and the copies thereof, to the City or destroy all such City Data and certify to the City that it has done so; however, this requirement shall not apply to the extent the Contractor is required by law to retain copies of certain City Data. The Contractor shall not interrupt or obstruct the City's ability to access and retrieve City Data stored by the Contractor. Unless otherwise required by law or regulation, when paper or electronic documents are no longer needed, the Contractor shall destroy or arrange for the destruction of such documents within its custody or control that contain City Data by shredding, erasing, or otherwise modifying the City Data in the paper or electronic documents to make it unreadable or indecipherable. The Contractor's obligations set forth in this Subsection, without limitation, apply likewise to the Contractor's successors, including without limitation any trustee in bankruptcy.

3.7. Software and Computing Systems: At its reasonable discretion, the City may prohibit the Contractor from the use of certain software programs, databases, and computing systems with known vulnerabilities to collect, use, process, or store, City Data received under this Agreement. The Contractor shall fully comply with all requirements and conditions, if any, associated with the use of software programs, databases, and computing systems as reasonably directed by the City. The Contractor shall not use funds paid by the City for the acquisition, operation, or maintenance of software in violation of any copyright laws or licensing restrictions. The Contractor shall maintain commercially reasonable network security that, at a minimum, includes network firewalls, intrusion detection/prevention, and enhancements or updates consistent with evolving industry standards The Contractor shall use industry-standard and up-to-date security tools, technologies and procedures including, but not limited to, anti-virus and anti-malware protections. The Contractor will require that any underlying or integrated software employed under this Agreement is updated on a regular basis and does not pose a security threat. Upon request, the Contractor shall provide a software bill of materials ("SBOM") annually or upon major changes to the solution(s) provided to the City under this Agreement. The Contractor shall provide a complete SBOM for the supported life of the solution(s). The Contractor shall monitor for security vulnerabilities in applicable software components and use a risk-based approach to mitigate any vulnerabilities.

3.8. Background Checks: The Contractor shall ensure that, prior to being granted access to City Data, the Contractor's agents, employees, Subcontractors, volunteers, or assigns who perform work under this Agreement have all undergone and passed all necessary criminal background screenings, have successfully completed annual instruction of a nature sufficient to enable them to effectively comply with all data protection provisions of this Agreement and applicable law, and possess all qualifications appropriate to the nature of the employees' duties and the sensitivity of the data. If the Contractor has access to federal tax information ("FTI") under this Agreement, the Contractor shall comply with the background check requirements of IRS Publication 1075.

3.9. Subcontractors: If the Contractor engages a Subcontractor under this Agreement, the Contractor shall ensure its Subcontractors are subject to data protection terms that provide at least the same level of data protection as in this Agreement and to the extent appropriate to the nature of the Work provided. The Contractor shall monitor the compliance with such obligations and remain responsible for its Subcontractor's compliance with the obligations of this Agreement and for any of its Subcontractors acts or omissions that cause the Contractor to breach any of its obligations under this Agreement. Unless the Contractor provides its own security protection for the information it discloses to a third party, the Contractor shall require the third party to implement and maintain reasonable security procedures and practices that are appropriate to the nature of the City Data disclosed and that are reasonably designed to protect it from unauthorized access, use, modification, disclosure, or destruction. Any term or condition within this Agreement relating to the protection and confidentially of any disclosed data shall apply equally to both the Contractor and any of its Subcontractors, agents, assigns, employees, or volunteers. Upon request, the Contractor shall provide the City copies of its record retention, data privacy, and information security policies. The Contractor shall ensure all Subcontractors sign, or have signed, agreements containing nondisclosure provisions at least as protective as those in this Agreement, and that the nondisclosure provisions are in force so long as the Subcontractor has access to any data disclosed under this Agreement. Upon request, the Contractor shall provide copies of those signed nondisclosure agreements to the City.

3.10. **<u>Request for Additional Protections and Survival</u>**: In addition to the terms contained herein, the City may reasonably request that the Contractor protect the confidentiality of certain City Data to ensure compliance with applicable law and any changes thereto. Unless a request for additional protections is mandated by a change in law, the Contractor may reasonably decline the City's request to provide additional protections. If such a request requires the Contractor to take steps beyond those contained herein, the Contractor shall notify the City with the anticipated cost of compliance, and the City may thereafter, in its sole discretion, direct the Contractor to comply with the request at the City's expense; provided, however, that any increase in costs that would increase the Maximum Contract Amount must first be memorialized in a written amendment complying with City procedures. Obligations contained in this Agreement relating to the protection and confidentially of any disclosed data shall survive termination of this Agreement, and the Contractor shall continue to safeguard all data for so long as the data remains confidential or protected and in the Contractor's possession or control.

4. <u>DISASTER RECOVERY AND CONTINUITY</u>

4.1. The Contractor shall maintain a continuous and uninterrupted business continuity and disaster recovery program with respect to the Work provided under this Agreement. The program shall be designed, in the event of a significant business disruption affecting the Contractor, to provide the necessary and sufficient capabilities, processes, and procedures to enable the Contractor to resume and continue to perform its duties and obligations under this Agreement without undue delay or disruption. In the event of equipment failures, the Contractor shall, at no additional expense to the City, take reasonable steps to minimize service interruptions, including using any back-up facilities where appropriate. Upon request, the Contractor shall provide the City with a copy of its disaster recovery plan and procedures.

4.2. Prior to the Effective Date of this Agreement, the Contractor shall, at its own expense, conduct or have conducted the following, and thereafter, the Contractor will, at its own expense, conduct or have conducted the following at least once per year:

4.2.1. A test of the operability, sufficiency, and completeness of business continuity and disaster recovery program's capabilities, processes, and procedures that are necessary to resume and continue to perform its duties and obligations under this Agreement.

4.2.2. Based upon the results and subsequent recommendations of the testing above, the Contractor will, within thirty (30) calendar days of receipt of such results and recommendations, promptly modify its capabilities, processes, and procedures to meet its obligations under this Agreement and provide City with written evidence of remediation.

4.2.3. Upon request, the Contractor shall provide the City with report summaries or other documentation resulting from above testing of any business continuity and disaster recovery procedures regarding the Services provided under this Agreement.

4.3. The Contractor represents that it is capable, willing, and able to provide the necessary and sufficient business continuity and disaster recovery capabilities and functions that are appropriate for it to provide services under this Agreement.

5. DELIVERY AND ACCEPTANCE

5.1. Acceptance & Rejection: Contractor's Software Support Level Agreement shall apply to the acceptance or rejection of any Service or Deliverables. Deliverables will be considered accepted ("Acceptance") only when the City provides the Contractor affirmative written notice of acceptance that such Deliverable has been accepted by the City. Such communication shall be provided within a reasonable time from the delivery of the Deliverable and shall not be unreasonably delayed or withheld. Acceptance by the City shall be final, except in cases of Contractor's failure to conduct proper quality assurance, latent defects that could not reasonably have been detected upon delivery, or the Contractor's gross negligence or willful misconduct. If any Deliverable does not perform to the City's satisfaction, the City reserves the right to repudiate acceptance pursuant to the terms of the Software Support Level Agreement. If the City ultimately rejects a Deliverable, or repudiates acceptance of it, the Contractor will refund to the City all fees paid, if any, by the City with respect to any rejected Deliverable. Acceptance shall not relieve the Contractor from its responsibility under any representation or warranty contained in this Agreement, and payment of an invoice prior to Acceptance does not grant a waiver of any representation or warranty made by the Contractor.

5.2. Quality Assurance: The Contractor shall provide and maintain a quality assurance system acceptable to the City for Deliverables under this Agreement and shall provide to the City only such Deliverables that have been inspected and found to conform to the specifications identified in this Agreement and any applicable solicitation, bid, offer, or proposal from which this Agreement results. The Contractor's delivery of any Deliverables to the City shall constitute certification that any Deliverables have been determined to conform to the applicable specifications, and the Contractor shall make records of such quality assurance available to the City upon request.

6. WARRANTIES AND REPRESENTATIONS

6.1. Any Work delivered to the City as a remedy under this Section shall be subject to the same quality assurance, acceptance, and warranty requirements as the original Work. The duration of the warranty for any replacement or corrected Work shall run from the date of the corrected or replacement Work.

6.2. **<u>Customization Services</u>**: The Contractor warrants that it will perform all customization services, if any, in a professional and workmanlike manner. In case of breach of the warranty of the preceding sentence, the Contractor, at its own expense, shall promptly re-perform the customization services in question or provide a full refund for all nonconforming customization services.

6.3. **<u>Third-Party Warranties and Indemnities</u>**: The Contractor will assign to the City all third-party warranties and indemnities that the Contractor receives in connection with any Work or Deliverables provided to the City. To the extent that the Contractor is not permitted to assign any warranties or indemnities through to the City, the Contractor agrees to specifically identify and enforce those warranties and indemnities on behalf of the City to the extent the Contractor is permitted to do so under the terms of the applicable third-party agreements.

6.4. **<u>Intellectual Property Rights in the Software</u>**: The Contractor warrants that it is either the owner of the Deliverables, or the recipient of a valid license thereto, and that it has and will maintain the full power and authority to grant the intellectual property rights to the Deliverables in this Agreement without the further consent of any third party and without conditions or requirements not set forth in this Agreement. In the event of a breach of the warranty in this Section, the Contractor, at its own expense, shall promptly take the following actions: (i) secure for the City the right to continue using the Deliverable as intended; (ii) replace or modify the Deliverable to make it non-infringing, provided such modification or replacement will not materially degrade any functionality as stated in this Agreement; or (iii) refund 100% of the fee paid for the Deliverable for every month remaining in the Term, in which case the Contractor may terminate any or all of the City's licenses to the infringing Deliverable granted in this Agreement and require return or destruction of copies thereof. The Contractor also warrants that there are no pending or threatened lawsuits, claims, disputes, or actions: (i) alleging that any of the Work or Deliverables infringes, violates, or misappropriates any third-party rights; or (ii) adversely affecting any Deliverables or Services, or the Contractor's ability to perform its obligations hereunder.

6.5. **<u>Disabling Code</u>**: In the event a disabling code, virus, worm, trap door, back door, timer, clock, counter or other limiting routine, instruction or design, or other malicious, illicit or similar unrequested code, including surveillance software or routines which may, or is designed to, permit access by any person, or on its own, to erase, or otherwise harm or modify any City system, resources, or data (a "Disabling Code") that is intended to damage, destroy, or destructively alter software, hardware, systems, or data, that was not caused by the City's own conduct or the conduct of its authorized agents, representatives or contractors is identified, the Contractor shall take all steps necessary, at no additional cost to the City, to: (i) restore and/or reconstruct all data lost by the City as a result of a Disabling Code; (ii) furnish to City a corrected version of the Work or Deliverables without the presence of a Disabling Code; and, (iii) as needed, re-implement the Work or Deliverable at no additional cost to the City. This warranty shall remain in full force and effect during the Term.

7. LICENSE OR USE AUDIT RIGHTS

7.1. To the extent that the Contractor, through this Agreement or otherwise as related to the subject matter of this Agreement, has granted to the City any license or otherwise limited permission to use any of the Contractor's intellectual property, the terms of this Section shall apply.

7.2. The Contractor shall have the right, at any time during and throughout the Term, but not more than once per year, to request via written notice in accordance with the notice provisions of this Agreement that the City audit its use of and certify as to its compliance with any applicable license or use restrictions and limitations contained in this Agreement (an "Audit Request"). The Audit Request shall specify the period to be covered by the audit, which shall not include any time covered by a previous audit. The City shall complete the audit and provide certification of its compliance to the Contractor ("Audit Certification") within a reasonable amount of time following the City's receipt of the Audit Request.

7.3. If upon receipt of the City's Audit Certification, the Parties reasonably determine that: (i) the City's use of licenses, use of software, use of programs, or any other use during the audit period exceeded the use restrictions and limitations contained in this Agreement ("Overuse"), and (ii) the City would have been or is then required to purchase additional maintenance and/or services ("Maintenance"), the Contractor shall provide written notice to the City in accordance with the notice provisions of this Agreement identifying any Overuse or required Maintenance and request that the City bring its use into compliance with such use restrictions and limitations.

REMAINDER OF PAGE INTENTIONALLY LEFT BLANK

EXHIBIT E, FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM

The goal of this document is to augment the CJIS Security Policy to ensure adequate security is provided for criminal justice systems while (1) under the control or management of a private entity or (2) connectivity to FBI CJIS Systems has been provided to a private entity (contractor). Adequate security is defined in Office of Management and Budget Circular A-130 as "security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information."

The intent of this Security Addendum is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

This Security Addendum identifies the duties and responsibilities with respect to the installation and maintenance of adequate internal controls within the contractual relationship so that the security and integrity of the FBI's information resources are not compromised. The security program shall include consideration of personnel security, site security, system security, and data security, and technical security.

The provisions of this Security Addendum apply to all personnel, systems, networks and support facilities supporting and/or acting on behalf of the government agency.

1.00 Definitions

1.01 Contracting Government Agency (CGA) – the government agency, whether a Criminal Justice Agency or a Noncriminal Justice Agency, which enters into an agreement with a private contractor subject to this Security Addendum.

1.02 Contractor – a private business, organization or individual which has entered into an agreement for the administration of criminal justice with a Criminal Justice Agency or a Noncriminal Justice Agency.

2.00 Responsibilities of the Contracting Government Agency.

2.01 The CGA will ensure that each Contractor employee receives a copy of the Security Addendum and the CJIS Security Policy and executes an acknowledgment of such receipt and the contents of the Security Addendum. The signed acknowledgments shall remain in the possession of the CGA and available for audit purposes. The acknowledgement may be signed by hand or via digital signature (see glossary for definition of digital signature).

3.00 Responsibilities of the Contractor.

3.01 The Contractor will maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed and all subsequent versions), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

4.00 Security Violations.

4.01 The CGA must report security violations to the CJIS Systems Officer (CSO) and the Director, FBI, along with indications of actions taken by the CGA and Contractor.

4.02 Security violations can justify termination of the appended agreement.

4.03 Upon notification, the FBI reserves the right to:

a. Investigate or decline to investigate any report of unauthorized use;

b. Suspend or terminate access and services, including telecommunications links. The FBI will provide the CSO with timely written notice of the suspension. Access and services will be reinstated only after satisfactory assurances have been provided to the FBI by the CGA and Contractor. Upon termination, the Contractor's records containing CHRI must be deleted or returned to the CGA.

5.00 Audit

5.01 The FBI is authorized to perform a final audit of the Contractor's systems after termination of the Security Addendum.

6.00 Scope and Authority

6.01 This Security Addendum does not confer, grant, or authorize any rights, privileges, or obligations on any persons other than the Contractor, CGA, CJA (where applicable), CSA, and FBI.

6.02 The following documents are incorporated by reference and made part of this agreement: (1) the Security Addendum; (2) the NCIC 2000 Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20. The parties are also subject to applicable federal and state laws and regulations.

6.03 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they augment the provisions of the CJIS Security Policy to provide a minimum basis for the security of the system and contained information and it is understood that there may be terms and conditions of the appended Agreement which impose more stringent requirements upon the Contractor.

6.04 This Security Addendum may only be modified by the FBI, and may not be modified by the parties to the appended Agreement without the consent of the FBI.

6.05 All notices and correspondence shall be forwarded by First Class mail to:

Information Security Officer
Criminal Justice Information Services Division, FBI
1000 Custer Hollow Road
Clarksburg, West Virginia 26306

FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM

CERTIFICATION

I hereby certify that I am familiar with the contents of (1) the Security Addendum, including its legal authority and purpose; (2) the NCIC Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20, and agree to be bound by their provisions.

I recognize that criminal history record information and related data, by its very nature, is sensitive and has potential for great harm if misused. I acknowledge that access to criminal history record information and related data is therefore limited to the purpose(s) for which a government agency has entered into the contract incorporating this Security Addendum. I understand that misuse of the system by, among other things: accessing it without authorization; accessing it by exceeding authorization; accessing it for an improper purpose; using, disseminating or re-disseminating information received as a result of this contract for a purpose other than that envisioned by the contract, may subject me to administrative and criminal penalties. I understand that accessing the system for an appropriate purpose and then using, disseminating or re-disseminating the information received for another purpose other than execution of the contract also constitutes misuse. I further understand that the occurrence of misuse does not depend upon whether or not I receive additional compensation for such authorized activity. Such exposure for misuse includes, but is not limited to, suspension or loss of employment and prosecution for state and federal crimes.

______________________________________ ______________

Printed Name/Signature of Contractor Employee Date

______________________________________ ______________

Printed Name/Signature of Contractor Representative Date

____

Organization and Title of Contractor Representative