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 **SailPoint Technologies, Inc**., a Delaware corporation registered to do business in Colorado, whose address is 11120 Four Points Drive, Suite 100, Austin, Texas 78726 ("Contractor" or "SailPoint"), jointly "the parties."

RECITALS

IT IS HEREBY AGREED BETWEEN THE PARTIES AS FOLLOWS:

INCORPORATION OF RECITALS. The recitals set forth above are incorporated herein as set forth in their entirety.

1. DEFINITIONS

a. "Affiliate" is an entity that controls, is controlled by or shares common control with SailPoint or Customer, where such control arises from either (a) a direct or indirect ownership interest of more than 50% or (b) the power to direct or cause the direction of the management and policies, whether through the ownership of voting stock by contract, or otherwise, equal to that provided by a direct or indirect ownership of more than 50%.

b. "Documentation" means the written documentation relating to the Software delivered by SailPoint to Customer with the Software.

c. "Identity Cube" means a unique collection of identity data for an individual that will be managed by SailPoint IdentityIQ for the purposes of certifying user access, enforcing access policy, processing access requests, or modeling user risk. Identity data may be physically or logically maintained in a single repository or in separate physical or logical repositories. Although Identity Cubes for user accounts that have been deactivated may remain in the identity management system, those inactive Identity Cubes will not be included in the number of Identity Cube licenses in use by Customer.

d. "Order" means the document(s) by which Customer orders Software licenses and/or services pursuant to this Agreement. An Order may consist of either (a) a schedule, statement of work, or quotation, that has been signed by both Customer and SailPoint, and/or (b) if applicable, a purchase order issued by Customer pursuant to this Agreement that has been expressly accepted in writing by SailPoint. Orders shall be governed solely by the terms of this Agreement.

e. "Software" means the computer software programs specified in Quote Q-15277-1 hereto, in object code format, and their related materials, which include updates, modifications, new releases, and Documentation.

2. SOFTWARE LICENSE, SUPPORT, HARDWARE AND MAINTENANCE TO BE PROVIDED AND SERVICES TO BE PERFORMED:

A. Contractor, under the general direction of, and in coordination with, the City's Chief Information Officer or other designated supervisory personnel (the "Manager") agrees to provide the Software pursuant to an Order, and perform the technology related services described on an applicable Statement of Work ("SOW") and provide the software support and maintenance services described on attached **Exhibit A**

B. As the Manager directs, the Contractor shall diligently undertake, perform, and complete all of the services and produce all the deliverables set forth on an applicable SOW to the City's satisfaction in accordance with an applicable SOW.

C. The Contractor is ready, willing, and able to provide the services required by this Agreement.

D. The Contractor shall faithfully perform the 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 the Agreement and in accordance with the terms of the Agreement.

3. GRANT OF LICENSE; RESTRICTIONS:

A. Subject to the terms and conditions of this Agreement, SailPoint grants to Customer a non-exclusive, non-transferable license (except as otherwise set forth herein) to (a) install, execute, copy, display or otherwise use the Software in machine readable format solely for internal use and solely for the number of Identity Cubes specified on an Order and (b) use the Documentation solely for use with the Software. Customer may make a reasonable number of copies of the Software in machine-readable form solely for archive or backup purposes in accordance with Customer's standard archive or backup policies and procedures. Use of such Software greater than the number of Identity Cubes paid for is prohibited and any such use will be subject to additional license and Support and Maintenance fees. .

The Software may only be used by employees of Customer or contractor/agents of Customer who are acting on behalf of Customer by providing implementing, consulting or outsourcing services and are under a written agreement with Customer that will protect SailPoint's Software similar to the protections and restrictions stated under this Agreement.

B. Title to and ownership of the Software will remain with Contractor. City will not nor allow any third party to reverse engineer or reverse compile or attempt to discover any source code or underlying ideas or algorithms of any part of the Software without Contractor's prior written consent. Except as mutually agreed to in writing as an exception under this Agreement, Customer will not, nor allow any third party to modify, lease, lend, use for timesharing or service bureau purposes or otherwise use or allow others to use Software for the benefit of any third party. City will not remove, obscure or deface any proprietary notice or legend contained in the Software or documentation without Contractor's prior written consent.

C. Deployment Verification. Upon reasonable advance notice to Customer and on a non-interference basis with Customer's normal business operations, SailPoint has the right to verify the quantity of Software Customer has placed into use under this Agreement. Such verification shall not be conducted more frequently than once per year unless agreed otherwise in an Order.

D. Except as otherwise set out herein, Contractor at its expense will, within thirty (30) days after the signing of this Agreement and continuously thereafter, deposit the Software in source code form, including all enhancements, in escrow pursuant to a source code escrow agreement ("Escrow Agreement") acceptable to City. The following events automatically will give City the right to cause the release of the applicable source code from Contractor or the escrow agent, whether or not contained in the Escrow Agreement, upon notice to Contractor or presentation of this Agreement to the escrow agent: (i) the institution by or against Contractor of insolvency, receivership or bankruptcy proceedings; (ii) Contractor's making an assignment for the benefit of creditors; (iii) Contractor's dissolution or ceasing its ongoing business operations or sale, licensing, maintenance or other support of the Software; or (iv) Contractor failing to pay the applicable fees due under the Escrow Agreement.

4. DELIVERY AND ACCEPTANCE:

A. Contractor shall deliver the Software and Documentation via electronic download, subject to the receipt of all required documentation, including any required export and import permits. Customer's Order shall be considered delivered on the date that SailPoint emails instructions for downloading the Software and Documentation to Customer. Thereafter, Customer shall be responsible for and bear all expenses (including taxes) related to making the permitted number of copies and distributing such copies as permitted in this Agreement. Customer will be the importer of record for the Software. The Software, support and training are set out in the attached Quote #Q-15277-1.

B. SailPoint Professional Services. The following terms and conditions shall apply to professional services ("Professional Services") supplied by SailPoint to Customer. Customer may purchase Professional Services from SailPoint to be performed on a time and material basis.

1) Scope of Professional Services. Professional Services will be documented in a Statement of Work ("SOW"), attached as Exhibit B. The Software provided under this Agreement is not custom software but is standard commercial software and the scope of Professional Services provided hereunder shall consist solely of (i) program planning, (ii) Software deployment assistance, (iii) interface adapter efforts, and/or (iv) formal or non-formal software training. Professional Services provided to Customer by SailPoint shall not constitute works for hire.

2) Term of Professional Services. Professional Services will begin and terminate on the dates or times defined in a SOW which has been mutually agreed to by Customer and SailPoint in writing, unless earlier terminated in accordance with this Agreement.

3) Fees and Expenses. Fees for Professional Services are defined in a SOW or an Order. Invoices may be published on a monthly basis for Professional Services actually performed or in accordance to the payment schedule mutually agreed to and documented in the SOW or Order. Professional Services fees exclude reasonable expenses for travel, food and lodging, directly related to the performance of Professional Services. All actual and reasonable expenses for travel, food and lodging, directly related to the performance of Professional Services shall be paid by Customer.

4) Termination or delay of Professional Services. Professional Services may be terminated by Customer by giving ten (10) days prior written notice to SailPoint; termination shall be effective ten (10) days after SailPoint's receipt of such notice. If Customer delays the scheduled start of contracted Professional Services, Customer shall reimburse SailPoint for any actual non-refundable costs incurred due to such delay. If Customer terminates Professional Services before the end of the Term of Professional Services engagement, Customer shall pay SailPoint for Professional Services completed prior to the effective termination date and reasonable and actual subcontractor costs incurred by SailPoint as a result of such delay or termination.

5) SailPoint Proprietary Information. All SailPoint Proprietary Information and all right, title and interest, including without limitation, all patents, copyrights, and trade secret rights anywhere in the world, and all other intellectual property and rights in connection therewith shall be the sole property of and remain with SailPoint or its licensors, as applicable. SailPoint Proprietary Information includes, but is not limited to, Software and related documentation and any modifications thereto developed in whole or in part by Professional Services. Except for the license use rights otherwise expressly provided in this Agreement, no right, title or interest in SailPoint Software is granted hereunder.

6) Independent Contractors. SailPoint is an independent contractor and is solely responsible for all taxes, withholdings, and other similar statutory obligations including, but not limited to Worker's Compensation Insurance. Nothing herein shall form or be construed to form a joint venture or partnership.

7) Performance Standards. SailPoint's performance of Professional Services under this Agreement will be conducted with standards of practice common in the industry for such services. SailPoint will comply with all applicable laws and Customer privacy, customer information, network and safety rules, guidelines and policies, in the course of performing Professional Services.

8) Consent to Subcontract. Customer hereby consents for SailPoint to subcontract Professional Services to persons or companies qualified and certified by SailPoint to provide services on SailPoint's behalf.

C. If Contractor's performance of the services is not in accordance with an applicable SOW and/or Order, the City will so notify Contractor within thirty (30) days after Contractor's performance thereof. Contractor will, at its own expense, re-perform the service within fifteen (15) days after receipt of City's notice of deficiency. The foregoing procedure will be repeated until City accepts or finally rejects the service due to non-conformance with the applicable SOW and/or Order. In the event that City finally rejects any service, Contractor will refund to City all fees paid by City with respect to such services not yet performed or that SailPoint was unable to perform in accordance with an applicable SOW and/or Order.

4. **TERM:** The term of the Agreement is from date of last signature below ("Effective Date") through December 15, 2024, unless earlier terminated in accordance with section 7. below.

5. **COMPENSATION AND PAYMENT:**

A. Fee: Fees and expenses shall be paid pursuant to the City's Prompt Payment Ordinance.

B. Reimbursement Expenses: The fees for the Software and any Services shall be more specifically detailed in one or more Order(s) referencing this Agreement.

C. Invoicing: Contractor must submit an invoice which shall include the City contract number, clear identification of the deliverable that has been completed, 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.

D. Maximum Contract Liability:

(i) Notwithstanding any other provision of the Agreement, the City's maximum payment obligation will not exceed TWO MILLION TEN THOUSAND FIVE HUNDRED SEVENTY-TWO DOLLARS AND FOURTEEN CENTS ($2,010,572.14) (the "Maximum Contract Amount"). The City is not obligated to execute an Agreement or any amendments for any further services, including any services performed by Contractor beyond that specifically described in the attached exhibits**.** Any services performed beyond those in an applicable SOW are performed at Contractor's risk and without authorization under the Agreement.

(ii) 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 the Agreement. The City does not by the Agreement irrevocably pledge present cash reserves for payment or performance in future fiscal years. The Agreement does not and is not intended to create a multiple-fiscal year direct or indirect debt or financial obligation of the City.

(iii) LIABILITY LIMIT - MUTUAL. EXCEPT AS STATED BELOW, IN NO EVENT SHALL EITHER PARTY (INCLUDING SUCH PARTY'S SUBCONTRACTORS, AGENTS, SUPPLIERS, DIRECTORS OR EMPLOYEES) BE LIABLE FOR ANY SPECIAL, INCIDENTAL, PUNITIVE, EXEMPLARY, INDIRECT, RELIANCE OR CONSEQUENTIAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS, LOSS OF PROFITS, BUSINESS INTERRUPTION, LOSS OF DATA, LOST SAVINGS OR

OTHER SIMILAR PECUNIARY LOSS) WHETHER ARISING FROM CONTRACT, TORT, OR ANY OTHER THEORY OF LIABILITY EVEN IF SUCH PARTY KNEW OR SHOULD HAVE KNOWN OF THE POSSIBILITY OF SUCH DAMAGES.

(iv)NOTWITHSTANDING THE FOREGOING, THE LIMITATIONS OF LIABILITY SET FORTH IN THIS SECTION SHALL NOT APPLY TO (I) DAMAGES ARISING FROM A PARTY'S BREACH OF ITS CONFIDENTIALITY OBLIGATIONS PURSUANT TO THIS AGREEMENT, (II) DAMAGES ARISING FROM INFRINGEMENT OF THE OTHER PARTY'S INTELLECTUAL PROPERTY RIGHTS OR (III) CLAIMS FOR DEATH, BODILY INJURY OR DAMAGE TO TANGIBLE PROPERTY CAUSED BY THE NEGLIGENCE OF SUCH PARTY OR ITS EMPLOYEES, SUBCONTRACTORS OR AGENTS OR (IV) CLAIMS ARISING FROM AN INDEMNIFICATION OBLIGATION.

6. 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.

7. TERMINATION:

A. The City has the right to terminate the Agreement with cause upon written notice effective immediately, and without cause upon twenty (20) days prior written notice to the Contractor. However, nothing gives the Contractor the right to perform services under the Agreement beyond the time when its services become unsatisfactory to the Manager.

B. Notwithstanding the preceding paragraph, the City may terminate the 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, kick backs, collusive bidding, bid-rigging, antitrust, fraud, undue influence, theft, racketeering, extortion or any offense of a similar nature in connection with Contractor's business. Termination for the reasons stated in this paragraph is effective upon receipt of notice.

C. Upon termination of the 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 as described in the Agreement and shall refund to the City any prepaid cost or expenses.

D. This Agreement, or a license granted hereunder, may be terminated (i) by mutual agreement of SailPoint and Customer, or (ii) by either party if the other party commits a material breach of this Agreement and fails to cure such breach within thirty (30) days following receipt of breach notice.

E. Effect of Termination. Upon termination of this Agreement or expiration or termination of a license, all rights granted to Customer for the applicable license(s) shall cease and Customer shall immediately: (i) cease using the applicable Software and Documentation, (ii) return the applicable Software to SailPoint together with all Documentation and other materials associated with the Software and all copies of any of the foregoing, or destroy such items, (iii) cease using the Maintenance Services associated with the applicable License(s), (iv) give SailPoint a written certification that Customer has complied with all of the foregoing obligations, and (v) in case of termination due to an uncured Customer breach, Customer will pay SailPoint or the applicable Partner all amounts due and payable.

8. EXAMINATION OF RECORDS: 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 any pertinent books, documents, papers and records of the Contractor, involving transactions related to the Agreement until the latter of three (3) years after the final payment under the Agreement or expiration of the applicable statute of limitations.

9. 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 the Agreement shall be deemed or taken to be a waiver of any other breach.

10. INSURANCE:

A. General Conditions: 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. Contractor shall keep the required insurance coverage in force at all times during the term of the Agreement, or 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 contain a valid provision or endorsement requiring notification to the City in the event any of the required policies is 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, 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. If any policy is in excess of a deductible or self-insured retention, the City must be notified by the Contractor. 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.

B. **Proof of Insurance:** Upon request, Contractor shall provide a copy of this Agreement to its insurance agent or broker. Contractor may not commence services or work relating to the Agreement prior to placement of coverages required under this Agreement. Contractor certifies that the certificate of insurance, preferably an ACORD certificate, complies with all insurance requirements of this Agreement. The City requests that the City's contract number be referenced on the Certificate. 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 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.

C. **Additional Insureds:** For Commercial General Liability, Auto Liability and Excess Liability/Umbrella (if required), 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.

D. **Waiver of Subrogation:** For all coverages required under this Agreement, except those events that result solely from the City's acts, omissions, or gross negligence, Contractor's insurer shall waive subrogation rights against the City.

E. **Subcontractors and Subconsultants:** All subcontractors and subconsultants (including independent contractors, suppliers or other entities providing goods or services required by this Agreement) shall be subject to all of the requirements herein and shall procure and maintain the same coverages required of the Contractor. Contractor shall include all such subcontractors as additional insured under its policies (with the exception of Workers' Compensation) or shall ensure that all such subcontractors and subconsultants maintain the required coverages. Contractor agrees to provide proof of insurance for all such subcontractors and subconsultants upon request by the City.

F. **Workers' Compensation/Employer's Liability Insurance:** 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. Contractor expressly represents to the City, as a material representation upon which the City is relying in entering into this Agreement, that none of the Contractor's officers or employees who may be eligible under any statute or law to reject Workers' Compensation Insurance shall effect such rejection during any part of the term of this Agreement, and that any such rejections previously effected, have been revoked as of the date Contractor executes this Agreement.

G. **Commercial General Liability:** Contractor shall maintain a Commercial General Liability insurance policy with limits of $1,000,000 for each occurrence, $1,000,000 for each personal and advertising injury claim, $2,000,000 products and completed operations aggregate, and $2,000,000 policy aggregate.

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

I. **Technology Errors & Omissions with Cyber-Liability:** Contractor shall maintain Technology Errors and Omissions insurance including cyber liability, network security, privacy liability and product failure coverage with limits of $1,000,000 per occurrence and $1,000,000 policy aggregate.

J. **Additional Provisions:**

(a) For Commercial General Liability, the policy must provide the following:

(i) That this Agreement is an Insured Contract under the policy;
(ii) Defense costs are outside the limits of liability;
(iii) A severability of interests or separation of insureds provision (no insured vs. insured exclusion); and
(iv) A provision that coverage is primary and non-contributory with other coverage or self-insurance maintained by the City.

(b) For claims-made coverage:
(i) The retroactive date must be on or before the contract date or the first date when any goods or services were provided to the City, whichever is earlier.

(ii) Contractor shall advise the City in the event any general aggregate or other aggregate limits are reduced below the required per occurrence limits. At their own expense, and where such general aggregate or other aggregate limits have been reduced below the required per occurrence limit, the Contractor will procure such per occurrence limits and furnish a new certificate of insurance showing such coverage is in force.

11. **REPRESENTATION AND WARRANTY:** Contractor represents and warrants that:

A. The Software will materially conform to the accompanying Documentation for a period of one hundred eighty (180) days from the date of initial delivery. If during the warranty period the Software does not materially conform to the Documentation, then Customer's exclusive remedy under this provision will be to have SailPoint, at SailPoint's expense and option, either repair, replace, or refund the amount paid by Customer for the nonconforming Software. If refunded, Customer's license to use of the defective Software shall be terminated and the defective Software shall be returned to SailPoint. SailPoint does not warrant that the operation of the Software will be uninterrupted or error free, or that all software defects can be corrected. This warranty shall not apply if: (a) the Software is not used in accordance with SailPoint's instructions;

(b) the Software defect has been caused by any of Customer's malfunctioning equipment or Customer provided software; or (c) Customer has made modifications to the Software not expressly authorized in writing by SailPoint.

B. WARRANTY DISCLAIMER. THIS WARRANTY IS IN LIEU OF ALL OTHER WARRANTIES AND IS THE ONLY WARRANTY GRANTED BY SAILPOINT WITH RESPECT TO THE SOFTWARE, DOCUMENTATION OR THE SERVICES. THERE ARE NO OTHER EXPRESS OR IMPLIED WARRANTIES OR CONDITIONS, ORAL OR WRITTEN, INCLUDING THOSE OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, SATISFACTORY QUALITY, REGARDING THIS AGREEMENT OR ANY SOFTWARE LICENSED HEREUNDER. SAILPOINT DOES NOT WARRANTY UNINTERUPTED OR ERROR-FREE OPERATION OF THE PRODUCTS.

12. DEFENSE AND INDEMNIFICATION:

A. 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"), unless such Claims have been specifically determined by the trier of fact to be the sole negligence or willful misconduct of the City. This indemnity shall be interpreted in the broadest possible manner to indemnify City for any acts or omissions of Contractor or its subcontractors either passive or active, irrespective of fault, including City's concurrent negligence whether active or passive, except for the sole negligence or willful misconduct of City.

B. 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. 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.

C. Contractor will defend any and all Claims which may be brought or threatened 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.

D. 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.

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

F. Intellectual Property Indemnification. Contractor will, at Contractor's expense, indemnify, defend and hold harmless the City, its officers, agents and employees from and against any loss, cost, expense or liability (including but not limited to attorney's fees and awarded damages) arising out of a claim that the Software, services, or their use by the City, infringe, violate or misappropriate a patent, copyright, trademark, trade secret or other intellectual property or proprietary right of any third party. The City will promptly notify Contractor in writing of any claim and cooperate with Contractor and its legal counsel in the defense thereof. Contractor may in its discretion (i) contest, (ii) settle, (iii) procure for the City the right to continue using the Software, or (iv) modify or replace the infringing Software so that it no longer infringes (as long as the functionality and performance are not degraded as reasonably determined by the City). The City may participate in the defense of such action at its own expense. If Contractor concludes in its reasonable judgment that none of the foregoing options are commercially reasonable, then Contractor will refund a pro rata portion (based on a 5 year straight line depreciation running from City's final acceptance of the Software) of the Software license fee(s) paid by the City under this Agreement and reimburse the City for all reasonable expenses for removal and replacement of the Software.

G. The foregoing obligations do not apply with respect to Software or portions or components thereof (i) not supplied by SailPoint, (ii) made in whole or in part in accordance to Customer specifications, (iii) that are modified by Customer after delivery (iv) combined with other products, processes or materials where the alleged infringement relates to such combination which were unauthorized by SailPoint, (v) where Customer continues use of the infringing Software following SailPoint's supplying a modified, amended or replacement version of the Software, or (vi) where Customer's use of such Software is not strictly in accordance with this Agreement. Customer will reimburse SailPoint for any reasonable out of pocket expenses incurred by SailPoint if the cause of the infringement is attributable to Customer's actions as stated in this paragraph.

H. THE PROVISIONS OF SECTIONS 12.F. AND 12.G. ABOVE SET FORTH SAILPOINT'S SOLE AND EXCLUSIVE OBLIGATIONS, AND CUSTOMER'S SOLE AND EXCLUSIVE REMEDIES, WITH RESPECT TO INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS AND/OR PROPRIETARY RIGHTS OF ANY KIND.

13. <u>COLORADO GOVERNMENTAL IMMUNITY ACT</u>: 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. (2003).

14. <u>TAXES, CHARGES AND PENALTIES</u>: 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.

15. **ASSIGNMENT; SUBCONTRACTING**: Neither party shall voluntarily or involuntarily assign any of its rights or obligations, or subcontract performance obligations, under this Agreement without obtaining the other party's prior written consent. Any assignment or subcontracting without such consent will be ineffective and void, and shall be cause for termination of this Agreement by the City. Notwithstanding the foregoing, (a) either party may assign this Agreement to any party that acquires all or substantially all of its related business by merger, sale of stock or assets, or a similar transaction, and (b) SailPoint may subcontract its obligations hereunder to a third party, provided that SailPoint shall remain liable for any breach thereof.

16. **NO THIRD PARTY BENEFICIARY:** Enforcement of the terms of the Agreement and all rights of action relating to enforcement are strictly reserved to the parties. Nothing contained in the 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 the Agreement is an incidental beneficiary only.

17. **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.

18. **AGREEMENT AS COMPLETE INTEGRATION-AMENDMENTS:** The Agreement is the complete integration of all understandings between the parties as to the subject matter of the Agreement. No prior, contemporaneous or subsequent addition, deletion, or other modification has any force or effect, unless embodied in the Agreement in writing. No oral representation by any officer or employee of the City at variance with the terms of the Agreement or any written amendment to the Agreement will have any force or effect or bind the City.

19. **SEVERABILITY:** Except for the provisions of the Agreement requiring appropriation of funds and limiting the total amount payable by the City, if a court of competent jurisdiction finds any provision of the 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.

20. **CONFLICT OF INTEREST:**

A. No employee of the City shall have any personal or beneficial interest in the services or property described in the 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.

B. The Contractor shall not engage in any transaction, activity or conduct that would result in a conflict of interest under the 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 the Agreement in the event it determines a conflict exists, after it has given the Contractor written notice describing the conflict.

21. NOTICES: All notices required by the terms of the Agreement must be hand delivered, sent by overnight courier service, mailed by certified mail, return receipt requested, or mailed via United States mail, postage prepaid, if to Contractor at the address first above written, and if to the City at:

Chief Information Officer or Designee
201 West Colfax Avenue, Dept. 301
Denver, Colorado 80202

With a copy of any such notice to:

Denver City Attorney's Office
1437 Bannock St., Room 353
Denver, Colorado 80202

Notices hand delivered or sent by overnight courier are effective upon delivery. Notices sent by certified mail are effective upon receipt. Notices sent by mail are effective upon deposit with the U.S. Postal Service. The parties may designate 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.

22. DISPUTES: All disputes between the City and Contractor arising out of or regarding the 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 Manager as defined in this Agreement.

23. GOVERNING LAW; VENUE: The 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 the 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 the Agreement will be in the District Court of the State of Colorado, Second Judicial District.

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

25. **USE, POSSESSION OR SALE OF ALCOHOL OR DRUGS:** 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 Contractor from City facilities or participating in City operations.

26. **CONFIDENTIAL INFORMATION; OPEN RECORDS:**

A. **City Information:** "Proprietary Data" shall mean any materials or information which may be designated or marked "Proprietary" or "Confidential", or which would not be documents subject to disclosure pursuant to the Colorado Open Records Act or City ordinance, and provided or made available to Contractor by the City. Such Proprietary Data may be in hardcopy, printed, digital or electronic format. Contractor acknowledges and accepts that, in performance of all work under the terms of this Agreement, Contractor may have access to Proprietary data or Confidential Information that may be owned or controlled by the City, and that the disclosure of such Proprietary Data or Confidential Information may be damaging to the City or third parties. Contractor agrees that all Proprietary Data, Confidential Information or any other data or information provided or otherwise disclosed by the City to Contractor shall be held in confidence and used only in the performance of its obligations under this Agreement. Contractor shall exercise the same standard of care to protect such Proprietary Data and Confidential Information as a reasonably prudent contractor would to protect its own proprietary or confidential data.

B. **Use and Protection of Proprietary Data or Confidential Information:**

(a) Except as expressly provided by the terms of this Agreement, Contractor agrees that it shall not disseminate, transmit, license, sublicense, assign, lease, release, publish, post on the internet, transfer, sell, permit access to, distribute, allow interactive rights to, or otherwise make available any data, including Proprietary Data or Confidential Information or any part thereof to any other person, party or entity in any form of media for any purpose other than performing its obligations under this Agreement. Contractor further acknowledges that by providing data, Proprietary Data or Confidential Information, the City is not granting to Contractor any right or license to use such data except as provided in this Agreement. Contractor further agrees not to disclose or distribute to any other party, in whole or in part, the data, Proprietary Data or Confidential Information without written authorization from the Manager and will immediately notify the City if any information of the City is requested from the Contractor from a third party.

(b) Contractor agrees, with respect to the Proprietary Data and Confidential Information, that: (1) Contractor shall not copy, recreate, reverse engineer or decompile such data, in whole or in part, unless authorized in writing by the Manager; (2) Contractor shall retain no copies, recreations, compilations, or decompilations, in whole or in part, of such data; and (3) Contractor shall, upon the expiration or earlier termination of the Agreement, destroy (and, in writing, certify destruction) or return all such data or work products incorporating such data or information to the City.

(c) Contractor shall develop, implement, maintain and use appropriate administrative, technical and physical security measures to preserve the confidentiality, integrity and availability of all electronically maintained or transmitted data received from, or on behalf of City. It is the responsibility of the Contractor to ensure that all possible measures have been taken to secure the computers or any other storage devices used for City data. This includes industry accepted firewalls, up-to-date anti-virus software, controlled access to the physical location of the hardware itself.

C. Employees and Sub-Contractor: Contractor will inform its employees and officers of the obligations under this Agreement, and all requirements and obligations of Contractor under this Agreement shall survive the expiration or earlier termination of this Agreement. Contractor shall not disclose Proprietary Data or Confidential Information to subcontractors unless such subcontractors are bound by non-disclosure and confidentiality provisions at least as strict as those contained in this Agreement.

D. Disclaimer: Notwithstanding any other provision of this Agreement, the City is furnishing Proprietary Data and Confidential Information on an “as is” basis, without any support whatsoever, and without representation, warranty or guarantee, including but not in any manner limited to, fitness, merchantability or the accuracy and completeness of the Proprietary Data or Confidential Information. Contractor is hereby advised to verify its work. The City assumes no liability for any errors or omissions herein. Specifically, the City is not responsible for any costs including, but not limited to, those incurred as a result of lost revenues, loss of use of data, the costs of recovering such programs or data, the cost of any substitute program, claims by third parties, or for similar costs. If discrepancies are found, Contractor agrees to contact the City immediately.

E. Contractor’s Information: To the extent applicable in this Agreement, the City understands and agrees that the Contractor’s software and documentation including, but not limited to, source code, object code, the interface requirements document(s), acceptance test procedures, the Statement of Work, the software design, structure and organization, software screens, the user interface and the engineering know-how implemented in the software (collectively “Contractor Confidential Information”), and the terms of this Agreement and the fees identified in any Order may constitute the valuable properties and trade secrets of Contractor, embodying substantial creative efforts which are secret, confidential, and not generally known by the public, and which secure to Contractor a competitive advantage. The City agrees during the term of this Agreement and any license granted hereunder, and thereafter, to hold the Contractor Confidential Information including any copies thereof and any documentation related thereto, in strict confidence and to not permit any person or entity to obtain access to it except as required for the City’s exercise of the license rights granted hereunder, and except as required by the parties understand that all the material provided or produced under this Agreement may be subject to the Colorado Open Records Act., § 24-72-201, et seq., C.R.S. In the event of a request to the City for disclosure of such information, the City shall advise Contractor of such request in order to give Contractor the opportunity to object to the disclosure of any of its Contractor Confidential Information and take necessary legal recourse. In the event of the filing of a lawsuit to compel such disclosure, the City will tender all such material to the court for judicial determination of the issue of disclosure and Contractor agrees to intervene in such lawsuit to protect and assert its claims of privilege against disclosure of such material or waive the same. Contractor further agrees to defend, indemnify and save and hold harmless the City, its officers, agents and employees, from any claim, damages, expense, loss or costs arising out of Contractor's intervention to protect and assert its claim of privilege against disclosure under this Article including but not limited to, prompt reimbursement to the City of all reasonable attorney fees, costs and damages that the City may incur directly or may be ordered to pay by such court.

27. **<u>LEGAL AUTHORITY</u>:** 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 the Agreement. Each person signing and executing the Agreement on behalf of Contractor represents and warrants that he has been fully authorized by Contractor to execute the Agreement on behalf of Contractor and to validly and legally bind Contractor to all the terms, performances and provisions of the Agreement. The City shall have the right, in its sole discretion, to either temporarily suspend or permanently terminate the Agreement if there is a dispute as to the legal authority of either Contractor or the person signing the Agreement to enter into the Agreement.

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

29. **<u>ORDER OF PRECEDENCE</u>**: In the event of any conflicts between the language of the Agreement and the exhibits, the language of the Agreement controls.

30. **<u>SURVIVAL OF CERTAIN PROVISIONS</u>:** The terms of the Agreement and any exhibits and attachments that by reasonable implication contemplate continued performance, rights, or compliance beyond expiration or termination of the Agreement survive the Agreement and will continue to be enforceable. Without limiting the generality of this provision, the Contractor's obligations to provide insurance and to indemnify the City will survive for a period equal to any and all relevant statutes of limitation, plus the time necessary to fully resolve any claims, matters, or actions begun within that period.

31. **<u>INUREMENT</u>:** 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.

32. **<u>TIME IS OF THE ESSENCE</u>:** The parties agree that in the performance of the terms, conditions, and requirements of this Agreement, time is of the essence.

33. **<u>FORCE MAJEURE</u>**: 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 plant, 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 or its officers, directors, employees, agents, vendors or elected officials and/or other substantially similar occurrences beyond the party's reasonable control ("Excusable Delay") herein. In the event of any such Excusable Delay, time for performance shall be extended for a period of time as may be reasonably necessary to compensate for such delay.

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

35. 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.

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

37. ELECTRONIC SIGNATURES AND ELECTRONIC RECORDS: Contractor consents to the use of electronic signatures by the City. The 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 the 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 the 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.

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

Contract Control Number:	TECHS-201952801-00
Contractor Name:	SAILPOINT TECHNOLOGIES INC

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

SEAL	**CITY AND COUNTY OF DENVER:**
ATTEST:	By:
______________________________	______________________________
APPROVED AS TO FORM:	**REGISTERED AND COUNTERSIGNED:**
Attorney for the City and County of Denver	
By:	By:
______________________________	______________________________
	By:
	______________________________

Contract Control Number: TECHS-201952801-00
Contractor Name: SAILPOINT TECHNOLOGIES INC

By: DocuSigned by: Tom Beck
59B1BBB721C24F1...

Name: Tom Beck
(please print)

Title: VP of Operations
(please print)

ATTEST: [if required]

By: ____

Name: ____
(please print)

Title: ____
(please print)

EXHIBIT A

SUPPORT AND MAINTENANCE

1. Support and Maintenance Services

Customer shall be entitled to purchase Support and Maintenance Services at an annual rate as stated in Section 4 below. Support and Maintenance Services entitles Customer to the following:

(a) Telephone or electronic support in order to help Customer locate and correct problems with the Software.

(b) Bug fixes and code corrections to correct Software malfunctions in order to bring such Software into substantial conformity with the operating specifications.

(c) All extensions, enhancements and other changes that SailPoint, at its sole discretion, makes or adds to the Software and which SailPoint furnishes, without charge, to all other licensees of the Software who are enrolled in Software Support and Maintenance.

(d) Replacement of the Software at no charge if the media becomes destroyed or damaged so that the Software becomes unusable.

2. Response and Resolution Goals

- "business hours" coverage (Monday-Friday, 8am-6pm local time elected by Customer excluding local holidays)
- "Problem" means a defect in Software as defined in SailPoint's standard Software specification which significantly degrades such Software.
- "Fix" means the repair or replacement of Software component in the form of a patch or e-fix to remedy Problem.
- "Workaround" means a change in the procedures followed or data supplied by Customer to avoid a Problem without substantially impairing Customer's use of the Software.
- "Respond" means acknowledgement of Problem received containing assigned support engineer name, date and time assigned, and severity assignment.

Problem Severity	*Response Goals*	*Resolution Goals*
1. The production system or SailPoint application is down or seriously impacted and there is no reasonable workaround currently available.	SailPoint will Respond within 2 business hours for Standard Support or 1 clock hour for Premium Support.	Upon confirmation of receipt, SailPoint support personnel begins continuous work on the Problem, and a customer resource must be available at any time to assist with problem determination. SailPoint will provide commercially reasonable efforts for Workaround or Fix within 24 Business Hours, once the Problem is reproducible or once we have identified the Software defect. SailPoint may incorporate Fix in future release of software.
2. The system or SailPoint application is seriously affected. The issue is not critical and does not comply with the Severity 1 conditions. There is no workaround currently available or the workaround is cumbersome to use.	SailPoint will Respond within 4 business hours for Standard Support or 2 business hours for Premium Support.	SailPoint will provide commercially reasonable efforts for Workaround or Fix within 7 business days, once the Problem is reproducible or once we have identified the problem as a Software defect. SailPoint may incorporate fix in future release of software.
3. The system or SailPoint application is moderately affected. The issue is not critical and the system has not failed. The issue has been identified and does not hinder normal operation, or the situation may be temporarily circumvented using an available workaround.	SailPoint will Respond within 8 business hours.	SailPoint will provide commercially reasonable efforts for Workaround or Fix within 10 business days, once the Problem is reproducible or once we have identified the problem as a Software defect. SailPoint may incorporate Fix in future release of software.
4. Non-critical issues, functionality does not appear to match documented specifications.	SailPoint will Respond within 12 business hours.	Resolution of Problem may appear in future release of software.

3. Accessing Support

SailPoint offers several ways to resolve any technical difficulties. In addition to online help in the Software, which can be accessed by clicking the "Help" tab when logged into the Software, function-specific help information can also be accessed throughout the Software using the '?' option.

The Compass online community (https://community.sailpoint.com) is available 24x7 for self-service technical assistance including:

- Downloading software updates and patch
- Viewing updates to supported platforms and hardware
- Accessing our knowledgebase, product documentation, technical articles, and FAQs
- Viewing supported platforms and hardware

The Horizon online support portal (http://www.sailpoint.com/services/online-support) is used to manage your cases and includes:

- Logging tickets and viewing status of previously submitted tickets
- Submitting new product enhancements (Ideas)
- Support Policy documentation
- Reporting

The support email address is support@sailpoint.com. The support phone number is 512-346-2000 or 1-888-472-4578.

4. Annual Support and Maintenance Services

The initial term of Standard Support and Maintenance Services shall be twelve (12) months from the Order/purchasing schedule effective date at the operative rate of 20% for standard and 25% for premium. Support and Maintenance Services renewals are offered on an annual subscription basis and may increase in subsequent years by 5%.

5. Scope of Coverage. The same level of Support and Maintenance Services shall apply to all licensed Software at the installation site and Customer shall keep all licensed Software it has acquired at an installation site under current contracted Support and Maintenance Services in order to receive the maintenance update services.

6. Support Renewal. For each subsequent year after the first year Support and Maintenance Services term, the obligation to provide Support and Maintenance Services as described above will continue and Customer's obligation to pay the current Support and Maintenance Services charges then in effect shall be automatically renewed on the anniversary date of the Software delivery hereunder. Unless cancelled by Customer, Customer will be invoiced for annual Support and Maintenance Services for subsequent years sixty (60) days prior to the expiration of the annual Support and Maintenance Services period.

7. Cancellation. Customer may cancel its subscription for Support and Maintenance Services effective as of the next anniversary by written notice received by SailPoint sixty (60) days prior to the annual renewal date.

8. Reinstatement. Customer may reinstate Support and Maintenance Services at a later time by paying the annual Support and Maintenance Services fee current at the time of reinstatement plus a fee equal to the then current Support and Maintenance Services fees for the Software times the number of annual periods the Support and Maintenance Services subscription was interrupted.

End of Page

SailPoint

EXHIBIT B

SailPoint IdentityIQ
Accelerator Pack Deployment

For

City and County of Denver

SailPoint Technologies, Inc.

Table of Contents

1 Introduction

This Statement of Work (SOW), s governed under the ("Agreement") between City and County of Denver ("CCD") and SailPoint Technologies, Inc. ("SailPoint"), and the Agreement is fully incorporated herein. All terms used in this SOW and not otherwise defined will have the same meaning set forth in the Agreement. To the extent of any conflict or inconsistency between this SOW and the terms of the Agreement, this Agreement shall prevail.

SailPoint is excited about the opportunity to utilize our IdentityIQ Accelerator Pack features to implement IdentityIQ with CCD. The objective of this SOW is to outline the implementation activity that will take place within CCD's environment. The purpose of this document is to detail the scope, timeline and fees for the implementation.

As a part of this engagement, SailPoint will implement IdentityIQ using IdentityIQ Accelerator Pack for the In Scope Data Sources listed in this SOW. SailPoint will leverage the following IdentityIQ modules, which CCD has licensed:

- IdentityIQ Governance Platform
- IdentityIQ Lifecycle Manager (LCM)
- IdentityIQ Compliance Manager (CM)

IdentityIQ Accelerator Pack was built to help our customers rapidly implement IdentityIQ using industry best practices. IdentityIQ Accelerator Pack contains many preconfigured use cases that will be implemented during this project. These preconfigured use cases accept parameters which will be specified as part of the project. SailPoint will work with CCD to identify how the IdentityIQ Accelerator Pack parameters should be set to deploy the desired use cases. Only these preconfigured use cases will be used during the implementation; no changes will be made to the IdentityIQ Accelerator Pack preconfigured use cases or modules during this project.

SailPoint will provide mentoring to CCD personnel on the operation and configuration of IdentityIQ Accelerator Pack and IdentityIQ in general. It is our goal to educate and enable CCD's staff to use IdentityIQ Accelerator Pack to continue to enhance their IdentityIQ implementation.

2 Executive Summary

The high level IdentityIQ functionality delivered, through IdentityIQ Accelerator Pack, in this SOW is listed below. Further details on the functionality listed in the Executive Summary is found in subsections of this SOW.

- Installation of IdentityIQ in a development environment and providing assistance to CCD to install IdentityIQ in Test and Production environments
    - Installation includes installing all licensed SailPoint products in scope for this project as well as IdentityIQ Accelerator Pack.
    - CCD is responsible for the procurement, installation and networking of all hardware.
    - CCD is responsible for the installation and configuration of all required supporting platforms (java, database, java application server).
- SailPoint will provide education on IdentityIQ Accelerator Pack, the deployment process of IdentityIQ Accelerator Pack and how it has been configured for CCD.
    - SailPoint provides standard documentation of the Accelerator Pack via the customer portal, Compass, for further detail and information on the workflows
- Requirements planning sessions, in the first week of the engagement, where SailPoint Professional Services will work with CCD to understand their business requirements and properly map them to the existing features of IdentityIQ Accelerator Pack.
- Working with CCD on delivery of the IdentityIQ Accelerator Pack Implementation Guide, which will serve as the As-Built document at the end of the engagement.
- Loading of data and building of identity cubes for the following 12 Applications. This includes connecting to one instance of each application type
    - Workday (Authoritative)
    - Active Directory
    - VertiQ – REST
    - SalesForce – Direct Connector
- Configuration of the IdentityIQ role model for use in CCD's initial deployment using IdentityIQ Accelerator Pack and for future implementations.
    - SailPoint will batch import 140 Roles that currently exist in OIM to IdentityIQ
    - Limited to building up to 20 Roles, CCD would be responsible for building any additional roles
    - SailPoint will provide 40hrs of consulting to CCD on Roles Based Access Control (RBAC). This will include review of the CCD RBAC model and recommendations on best practices going forward
- Configuration of the following use cases using IdentityIQ Accelerator Pack.
    - Data Aggregation and Data Categorization
    - Automated Provisioning
    - Access Request and Approval
    - Configure the Accelerator Pack Joiner, Mover, Leaver
- Compliance Manager – Building of three certification types (Manager, Data Owner and Role Owner)
    - SailPoint will build one certification of each type, CCD will be responsible for building any further certifications
- Configure ServiceNow Ticketing Integration
    - Configure ServiceNow to generate tickets for flat file provisioning/deprovisioning
- Configure Integration with Okta using the standard SailPoint connector
    - Okta will be configured outside of IdentityIQ to handle PW management
- Install and configure File Access Manager (formerly SecurityIQ)
    - Connect FAM up to 5 individual endpoints
        - SharePoint (FAM)

-
    -
        - OneDrive (FAM)
        - File Shares
- Configure core FAM functionality
    - Permissions collection and analysis
    - File activity monitoring
    - Data classification – sensitive data discovery
- Set up alerts and reports for continued monitoring of file activity
- Test & Validation
    - CCD will lead the overall testing process, including the building of a testing strategy, test environments, test data, test cases, and the execution of testing and defect reporting and tracking. SailPoint will fix defects that arise from the configuration of IdentityIQ Accelerator Pack and IdentityIQ, as reported by CCD during their testing efforts, to meet CCD's business requirements.
- Go-Live Support
    - SailPoint will provide support during the production go-live during standard SailPoint business days and hours in the time zone of the assigned resource(s).
    - SailPoint will provide a total of five (5) days of post-production support under this statement of work.
    - If extended go-live support is required for after business hours, weekends or holidays, an additional SOW will need to be executed.
- Education and mentoring for CCD on IdentityIQ and how it has been configured, using IdentityIQ Accelerator Pack, for CCD's business requirements.

3 Project Scope and Implementation Details

3.1 Scope: Project Implementation Stages

The table below details each stage of the project implementation and the tasks that will be completed during each stage of the project. Each Project Stage should be completed before moving into the next Project Stage, but SailPoint and CCD will mutually agree if a particular Project Stage should begin prior to the completion of the previous Project Stage.

Project Stage	Tasks
Pre-Project Kickoff	❖ IdentityIQ Accelerator Pack Overview Discussion ➢ CCD will learn about the IdentityIQ Accelerator Pack approach to deploying IdentityIQ and be educated on features that are included in this SOW. ➢ SailPoint will work to educate CCD on the terminology, which is used in IdentityIQ Accelerator Pack and in the IdentityIQ Accelerator Pack Implementation Guide and will be used in discussions during the implementation. ➢ SailPoint will work with CCD to review IdentityIQ Accelerator Pack Standard Operating Procedures documentation. ➢ SailPoint will work with CCD to review the IdentityIQ Secure Deployment Procedures found on Compass. ❖ SOW Review and Project Readiness ➢ SailPoint will review this SOW with CCD to ensure they understand the scope, assumptions and responsibilities of the project. ➢ CCD will review the steps they need to take internally to be ready for the implementation. ➢ CCD will inform SailPoint that they have internally signed-off and completed this task ❖ Application Owner Introduction ➢ SailPoint will provide the IdentityIQ Accelerator Pack Application Owner Overview document for the owners of the applications listed in In Scope Data Sources. ➢ Each application owner will review the IdentityIQ Accelerator Pack Application Owner Overview. ❖ IdentityIQ System Readiness Review ➢ SailPoint will work with CCD to review and verify that the recommended hardware was been procured in the development environment. ▪ This task may also be performed at this point for other IdentityIQ environments or can be done later in the project. ▪ CCD will inform SailPoint that they have internally signed-off and completed this task ➢ SailPoint will work with CCD to review and verify that the required Platform Software has been configured in the process. ▪ This task may also be performed at this point for Test, QA and Prod IdentityIQ environments or can be done later in the project.

	➢ SailPoint will work with CCD to review the access for SailPoint resources needed to commence the project ▪ CCD will commit to a plan to ensure that the proper access is available for SailPoint resources to commence the project. ▪ CCD will inform SailPoint that they have internally signed-off and completed this task ❖ Testing Readiness Review ➢ Test Planning and Execution Readiness ▪ SailPoint will review testing responsibilities and best practices with CCD. ▪ CCD will commit to being ready to execute a proper test cycle. ▪ CCD will inform SailPoint that they have internally signed-off and completed this task ➢ Test System and Test Data readiness review ▪ SailPoint will review the necessary test systems required for the implementation and the test data standards required for the implementation. ▪ CCD will commit to a plan to ensure that test systems and test data are ready for the project
Project Initiation & Planning	❖ Project Kickoff Meeting ➢ SailPoint will travel onsite to officially begin the project. ▪ Offsite kickoff is also acceptable if preferred by CCD. ➢ High-Level SOW Review with project team and review of project roles and responsibilities. ➢ Test Planning, Test Systems and Test Data review with project team. ➢ Project Plan will be reviewed with CCD. ▪ This will include identifying estimated dates when representatives from CCD will be expected to perform various tasks. ▪ This will include identifying estimated dates when SailPoint will return for onsite visits. ▪ This will include identifying estimated dates when functionality will be deployed into the production environment. More details on this is outlined in Project Phasing. ➢ Access to CCD's network will be reviewed with SailPoint and SailPoint will test it works as expected. ❖ Product Installation ➢ SailPoint will install IdentityIQ in the development, test, and QA environment. ▪ CCD's standard environments are Dev, Test, QA and Prod. ▪ CCD will be responsible for any work related to the Production Environment ▪ ➢ SailPoint will configure using CCD's Gitsource control and the Services Standard Build.

	❖ Application Owner Technical Deep Dive ➢ SailPoint will work with the Application Owners for each application listed in the In Scope Data Sources. The following will be covered: ▪ Application Owners will provide the system accounts for their applications in each environment. ▪ Application Owners will provide the connection information for their production and pre-production environments. ▪ Application Owners will describe the data schema for accounts in their applications. ▪ Application Owners will describe how accounts need to be created, modified and deleted in their applications. ❖ Requirements Vetting ➢ SailPoint will walk CCD through the IdentityIQ Accelerator Pack Requirements Definition document to confirm the requirements of the project. ➢ SailPoint will finalize the IdentityIQ Accelerator Pack Requirements Definition and it will be signed off by both parties. ❖ Project Phase Planning ➢ The Project Phasing section of this SOW provides a high-level recommendation on how the IdentityIQ Accelerator Pack configuration should be phased and implemented into production. During the Project Initiation and Planning phase of the project, this will be finalized. ➢ The project milestones and tasks will be managed out of CCDs Azure Devops system. All resources will be required to update tasks daily. All milestones will consist of Epic, Feature, Product Backlog and task hierarchy.
IdentityIQ Accelerator Pack Implementation Guide Planning	❖ SailPoint will plan multiple sessions with technical representatives from CCD to educate them on IdentityIQ Accelerator Pack and the features that will be implemented in this project. ❖ SailPoint and CCD technical representatives will complete the IdentityIQ Accelerator Pack Implementation Guide. This will serve as the build of the solution and when complete as the As Built documentation.
IdentityIQ Accelerator Pack Testing Planning	❖ SailPoint will plan multiple sessions with test representatives from CCD to educate them on IdentityIQ Accelerator Pack and the features that will be implemented in this project. ❖ SailPoint will meet with test representatives from CCD to review planned test approach, test strategy and test coverage for in scope IdentityIQ Accelerator Pack capabilities. SailPoint will provide feedback and recommendations to CCD. ❖ SailPoint will hold up to four (4) one (1) hour working sessions with test representatives to review templates, sample test cases and related materials which can be leveraged by CCD test team in configuring a Requirements Traceability Matrix, authoring test cases and managing test execution.

Basic Application Configuration	❖ SailPoint will configure the Applications in scope as defined in the In Scope Data Sources of this document. Basic Configuration includes: ➢ Test Connection ▪ Service Account with proper username and password to be supplied in advance by CCD. ➢ Discovering and modifying the Account and Account Group Schemas. ❖ Basic Account and Account Group Aggregation. ➢ Aggregations will be run to ensure that all accounts and account groups are aggregated, that no errors occur and to get a baseline for the amount of time the processes will take. ➢ Further refinement of the aggregation process will take place during the Data Aggregation configuration.
Role Configuration	❖ SailPoint will work with CCD to configure the IdentityIQ role model for use in their initial deployment using IdentityIQ Accelerator Pack. ➢ SailPoint will configure up to twenty (20) roles. ➢ SailPoint will batch import 140 existing roles from OIM as provided by CCD ➢ SailPoint will educate CCD on how to configure roles. ➢ CCD will be responsible for configuration of roles outside of the twenty (20) initially configured by SailPoint.
Workflow Trigger Configuration	❖ SailPoint will configure LifeCycle Event Triggers for the following Business Processes: ▪ Joiner ▪ Leaver ▪ Attribute Synchronization ➢ These triggers will be used to launch the appropriate IdentityIQ Accelerator Pack Workflow based on a change detected in the Authoritative Source.
IdentityIQ Accelerator Pack Self Service Onboarding	❖ SailPoint will configure the following IdentityIQ Accelerator Pack Use Cases based upon the specifications found in the IdentityIQ Accelerator Pack Implementation Guide for each application listed in the In Scope Data Sources section. ➢ Application Aggregation Configuration. ➢ Joiner Workflow Configuration ➢ Leaver Workflow Configuration ➢ Attribute Synchronization Configuration ➢ Access Request Approval Process Configuration
Certification Configuration	❖ SailPoint will work with CCD to configure Access Reviews using the IdentityIQ Accelerator Pack configuration and Out of the Box Compliance Manager functionality. Details on the Certification use cases in scope are found in the Access Review Feature.
Testing	❖ CCD will lead the overall testing process, including the building of a testing strategy, test environments, test data, test cases, and the execution of testing and defect reporting and tracking.

	SailPoint will fix defects that arise from the configuration of IdentityIQ Accelerator Pack and IdentityIQ, as reported by CCD during their testing efforts, to meet CCD's business requirements. ➢ Defects will be tracked and assigned to SailPoint for remediation. ➢ CCD will sign off on testing for a given piece of functionality. Upon sign off, the functionality may be promoted to the production environment (See Go-Live/Production Rollout below. ➢ During testing, if any limitations are found in the IdentityIQ Accelerator Pack feature set, they will not be treated as defects. SailPoint will be able to decide if the functionality could be included in future versions of IdentityIQ Accelerator Pack. ➢ Any defects that are discovered during testing but are found to not be part of the IdentityIQ Accelerator Pack configuration or IdentityIQ Accelerator Pack feature set, but are an issue with the core IdentityIQ product will be resolved via the standard SailPoint Support Process. These defects will be referred to CCD to open a support case with SailPoint. If Support cannot provide a viable work around then CCD can request to their Customer Success Manager for an efix be provided. ❖ Testing should begin early and should be exhaustive. ❖ Testing of functionality should be broken into logical pieces so that features can be tested and moved into production quickly and effectively, without waiting to finalize all configuration prior to testing beginning. ➢ SailPoint recommends that CCD perform an efficient regression test of existing production functionality prior to any rollout.
Go-Live/Production Rollout	❖ SailPoint recommends a phased go-live process for the IdentityIQ Accelerator Pack implementation. ➢ Functionality should be rolled out in phases after completing successful testing of the solution. ➢ See Project Phasing for recommended Testing/Go-Live Breakout. ❖ SailPoint will provide 5 days of post-production support with this SOW, which includes fixing defects discovered in production that SailPoint and CCD mutually agree should be fixed.
Project Conclusion and Next Steps	❖ SailPoint will conduct a two (2) hour planning session with CCD that will educate CCD on features of IdentityIQ Accelerator Pack that have not been implemented and could be considered for future phases. ❖ SailPoint will make necessary updates to the IdentityIQ Accelerator Pack Implementation Guide, which will service as the As Is Built documentation for the solution.

SailPoint and/or CCD can deploy additional releases to expand the solution. Future releases may extend the project functionality to additional data sources as well as deploy additional functionality using data sources already implemented.

3.2 In Scope Data Sources

One of the goals of IdentityIQ Accelerator Pack is to enable CCD to quickly deploy IdentityIQ with a subset of applications and allow CCD to augment their deployment with more applications after the conclusion of the work defined in this SOW. The table below lists the applications that are in scope for the Phase 1 deployment of IdentityIQ using IdentityIQ Accelerator Pack. These data sources should contain the authoritative source and entitlements for the use cases implemented during this statement of work. The following list is an estimate and will be finalized before project kick-off with mutual agreement between CCD and SailPoint. Changes to the list may result in a Change Order to be executed to properly fund the implementation.

Application Name	IdentityIQ Connector Type	In Scope User Cases	Provisioning Mechanism
Workday	Workday Direct	Authoritative Source	None
Active Directory	Active Directory Direct	Data Aggregation and Categorization Automated Provisioning Access Request Access Review	Direct Provisioning
ServiceNow	ServiceNow Connector	Automated Provisioning Access Request Access Review	Direct Provisioning
VertiQ	REST Web Services Connector	Data Aggregation and Categorization Automated Provisioning Access Request	Direct Provisioning
Okta	Okta Connector	Data Aggregation and Categorization Automated Provisioning Access Request	Direct Provisioning

3.3 In Scope Use Cases

3.3.1 Data Aggregation and Categorization

SailPoint will configure IdentityIQ with IdentityIQ Accelerator Pack to easily aggregate data into IdentityIQ and ensure that data is marked with the correct Metadata for use in IdentityIQ Accelerator Pack Workflows. The following aggregation features are in scope for this project and will be configured on a per application basis. CCD must provide deterministic logic for each bullet below.

- Determine if account is a Privileged Account for given Application.
- Determine if account is a Service Account for given Application.
- Determine if account is Disabled for given Application.
- Determine if account is Locked for given Application.
- Determine if an entitlement on an account is Privileged for given Application.
- Determine if an entitlement on an account is tied to Birthright Access for given Application.

Modifications to the out of the box feature are not in scope of this Statement of Work.

3.3.2 Automated Provisioning Use Cases: Joiner

SailPoint will configure IdentityIQ with IdentityIQ Accelerator Pack to process newly hired identities via a Joiner workflow. The following options are available for configuration for the Joiner, on a per application basis:

- Is Account Provisioned on this application for Joiner?
- What population of users should be provisioned access to the application?
- Assign selected birthright roles when the workflow is processed.
- Rehiring a previously terminated/separated account.
- Identities that have been put into a leave of absence state are reinstated.
- Identities that have been put into a long-term disability state are reinstated.
- Reverting an identity that was erroneously terminated back to its prior state.
- Send emails for providing welcome instructions for new hires and rehires and sending an initial password for new hires and rehires.

Modifications to the out of the box feature are not in scope of this Statement of Work.

3.3.2.1.1 Trigger

The triggering event for starting the joiner workflow process will be:

- A new identity being added into one of the authoritative sources listed In Scope Data Sources

3.3.3 Automated Provisioning Use Cases: Mover

SailPoint will configure IdentityIQ with IdentityIQ Accelerator Pack to process changes in an employee’s title, manager or other attribute that would require a revision of their access. The Mover Event Trigger will initiate a Manager Certification on the employee to review their current access. This may also trigger a Joiner event if there is an applicable birthright role that should be added to the employee based on the attribute changes.

3.3.4 Automated Provisioning Use Cases: Leaver

SailPoint will configure IdentityIQ with IdentityIQ Accelerator Pack to process terminated identities via a Leaver workflow. 3 main types of Leavers will be configured: terminations, leave of absence, long term disability. The following options are available for configuration for the Leaver, on a per application basis:

- Moving an account to a different Organizational Unit (OU) on termination (Active Directory and LDAP only).
- The following actions can be taken on an account when terminated, placed on leave of absence, or when placed on long term disability:
    - Disablement of account
    - Remove account of entitlements
    - Scramble password on account
- Defer termination process by a configurable number of days.
- Provide the ability to list exceptions of attributes that would be removed during a termination.

Modifications to the out of the box feature are not in scope of this Statement of Work.

3.3.4.1.1 Trigger

The triggering event for starting the leaver workflow process will be:

- A new Identity being marked as terminated, on leave of absence or on long term disability in one of the authoritative sources listed In Scope Data Sources.

3.3.5 Automated Provisioning Use Cases: Attribute Synchronization

SailPoint will configure IdentityIQ with IdentityIQ Accelerator Pack to process changes to identity attributes coming from the authoritative source with the attribute synchronization workflow. The following options are available for configuration for the attribute synchronization, on a per application basis:

- Synchronize primary account or all accounts.
- Rename LDAP based accounts.
- Provide a mechanism for mapping authoritative source attributes to target attributes.

Modifications to the out of the box feature are not in scope of this Statement of Work.

3.3.5.1.1 Trigger

The triggering event for starting the attribute synchronization workflow process will be:

- A mutually agreed upon set of attributes will change in one of the authoritative sources listed In Scope Data Sources.

3.3.6 Access and Account Request and Access Approvals

SailPoint will configure access and account request and approvals for the request of business roles and entitlements. The out of the box access request process of IdentityIQ will be utilized. Two levels of approvals will be available for all requestable items. The following options are available, on a per application or business role basis, for configuration for access request and access approvals.

- Account and Entitlement request approval flow
  - Manager approval.
  - Specify 1st level business approver.
  - Specify 2nd level business approver.
- Role request approval flow
  - Manager approval.
  - 1st level business approver.

Access requests will be available for all users in an organization to make requests for other identities. CCD will provide the names of the approvers for all requestable items that require approvals.

Modifications to the out of the box feature are not in scope of this Statement of Work.

3.3.7 Access Review Feature

SailPoint will configure the Compliance Manager module of IdentityIQ to make use of the features of IdentityIQ Accelerator Pack. The following certification types:

Use Case	Description
Manager	Access is presented to the manager on record for the user. Birthright access and privileged access will be filtered out of the certification. Manager will be able to approve or reject the access.
Privileged Access Review	Access is presented to the owner of the privileged access. Owner will be able to approve or reject the privileged access.

Generic configuration of IdentityIQ and Compliance Manager functionality including:

- Email template configuration with wording dictated by CCD
- Reminders and escalations for users who have not completed their access review campaigns.
- Basic UI Configuration
- Configuration and education on out of the box reporting.
- IdentityIQ will not provide a facility to make changes to access, only to approve/reject

3.3.8 Okta Connector

While Okta will be responsible for Password Management, SailPoint will configure IdentityIQ to connect to Okta as an application. This will allow IdentityIQ to manage Okta for Account Management and Group Management.

3.3.9 ServiceNow Service Integration Module

ServiceNow is a software platform that supports IT service management and automates common business processes for requesting and fulfilling service requests across a business enterprise. SailPoint will configure IdentityIQ's Service Desk Integration Module, or SDIM integration with ServiceNow, so that it converts IdentityIQ provisioning actions into tickets in ServiceNow for any source that is not directly connected. In addition to the ticket generation, this integration will also check the status of the service tickets within the system for all provisioning-based tasks to close the loop on provisioning requests.

Note The scope of the work for resources indicated in this SOW is limited to configuration within IdentityIQ and its ancillary components. Any configurations in additional systems, outside of IdentityIQ, are the responsibility of the customer, and should be factored externally to this scope.

3.3.10 Other Functionality Details

This SOW includes estimates to configure IdentityIQ for the following functionality:

- SailPoint will configure the IdentityIQ role model for use in the IdentityIQ Accelerator Pack use cases outlined in this SOW, but also for future implementation of additional IdentityIQ Accelerator Pack features.
  - SailPoint will spend one (1) day educating CCD on the use of the IdentityIQ role model and how it is used in IdentityIQ Accelerator Pack, along with future uses of roles.
  - SailPoint will configure twenty (20) roles as defined by CCD
  - SailPoint will batch upload 140 pre-existing roles from OIM into IdentityIQ
  - CCD will be responsible for configuring the remainder of the roles required
- SailPoint will provide guidance to CCD on implementing RBAC within IdentityIQ. This will include a review of CCD RBAC model, guidance on creating new roles going forward and best practices for implementing RBAC. This effort is limited to 40hrs of support.
- SailPoint will configure IdentityIQ to use existing Active Directory credentials for authentication purposes to IdentityIQ or enable SSO for IdentityIQ if the initiating SSO tool is on SailPoint’s supported SSO list.
- SailPoint will perform minimal branding of IdentityIQ with CCD logo and colors. This effort is limited to one (1) staff-day.
- SailPoint will configure out of the box auditing and reporting.

Custom Work Product will not be developed or created hereunder. The Services to be provided under this SOW shall consist solely of (i) Software deployment assistance, (ii) program planning, (iii) interface adapter efforts, and/or (iv) formal or non-formal Software training. SailPoint will not perform any development work or provide custom software, works for hire or Custom Work Product under this SOW.

CCD is expected to provide technical specialists with knowledge of CCD systems and an overall Project Manager with project control and oversight. CCD project manager will be responsible for coordinating internal resources and other contractors needed to help deliver on the implementation. This includes tracking their responsibilities and deliverables in relation to the overall project. Note that the percentage responsibility of the project for CCD's personnel can be modified to provide greater involvement and training during configuration and deployment.

Project Constraints

Once a project start date is agreed upon and named resources are assigned to a project, any Delay requires that CCD either a) hold assigned resources for the project or b) put the project on hold and resources will be reassigned. Delays include but are not limited to onboarding, access to equipment, security tokens, networks, accounts, email, applications, pause in project, etc. as required to complete assigned work.

If resources are held, CCD agrees to pay for the greater of actual hours worked or eight (8) hours per day for each held resource until project startup commences, or the project is put on hold. If a project is put on hold, the project will remain on hold until a revised start date can be agreed, and resources are available.

4 FAM Services

This section details the specific activities to be undertaken in this project in support of the endpoints and capabilities in scope as listed above.

4.1 FAM Endpoints and Capabilities in Scope

As part of this Base Deployment, SailPoint will integrate specific sources of unstructured data (referred to as "endpoints") and identity source(s) into File Access Manager. These endpoints should contain entitlements for high priority sources of unstructured data with respect to data access governance and important to File Access Manager implementation for the organization. Most customers pick Active Directory, Exchange, SharePoint, and/or some file servers.

An instance of an endpoint is defined as the following for each endpoint type:

Endpoint Type	Endpoint Counting Metric
Active Directory	1 domain
Exchange	1 organization
Exchange Online	1 organization
Windows File Server	1 server
SharePoint	1 site collection
NetApp	1 filer/vfiler
EMC Ceterra or Isilon	1 CIFS server
Box	1 subscription
DropBox	1 subscription

NOTE: Office 365 includes Exchange Online, SharePoint Online, and OneDrive. Each of these technologies uses a different API, requiring a different connector for File Access Manager, and therefore counts as a separate endpoint.

This Base Deployment SOW includes **one (1) Identity Source** and up to **five (5) endpoints** (which typically includes the Identity Source itself when that Identity Source is Active Directory). It also includes the File Access Manager capabilities that SailPoint and CCD will configure for those endpoints. This list will be finalized before project kick-off with mutual agreement between CCD and SailPoint.

Table 1: Identity Source, Endpoints and Capabilities in Scope

Identity Source	
1	Active Directory

Table 2: Example Selection of Endpoints

Count	Endpoint	Activity Monitoring	Permissions Analysis	Data Classification (OOTB types only in Phase 1)
1	Active Directory (1 domain)	X	X	N/A
2	Exchange (1 organization)	X	X	N/A
3	SharePoint	X	X	X

	(1 site collection)			
4	NetApp (1 filer/vfiler)	X	X	X
5	Windows File Server (1 server)	X	X	X

4.2 Pre-Kickoff

The Pre-Kickoff phase is focused on all project startup activities, hardware planning and setup, and preparing for the project kickoff.

- **Introduction Meeting** – the SailPoint Project Manager or Professional Services Manager will conduct an intro call with the CCD team to discuss project priorities and timelines.
- **Gathering information** – SailPoint will solicit information about the CCD environment, endpoints, and use cases.
- **Hardware and pre-requisite** – SailPoint will provide a plan for hardware setup, along with a list of technical prerequisites.
- **Hardware Setup**- CCD will be responsible for procuring the virtual or physical machines according to SailPoint's requirements.
- **Training –** it is highly recommended that the CCD-assigned technical resource(s) attend SailPoint product/configuration training prior to the start of the engagement.
- **Project Readiness Call**- SailPoint will conduct a pre-requisite verification call to ensure everything is ready for installation and project kickoff.

4.3 Visibility

The visibility phase is focused on the formal project kickoff, initial installation of File Access Manager, analyzing results, and finalizing requirements.

4.3.1 Project Kickoff

A project kickoff meeting will be held with CCD to review the functionality, timeline, roles, and responsibilities for the project.

- **Onsite kickoff meeting** – the SailPoint project manager and technical team will conduct the onsite kickoff meeting once the project is ready to begin.
- **Product installation** – immediately after the kickoff meeting, the SailPoint technical team will work with the CCD team to complete the initial installation and configuration of the software.

4.3.2 Application Setup

The basic product configuration will immediately after the project kick-off. The installation will include the following steps:

- **Core File Access Manager Services** – this includes installing the Database instance and core File Access Manager services within 1 client environment. Note that administrators for each server will need to be available to provide access to the servers and SQL Server application.
- **General product configuration**- configuration of File Access Manager will include configuration of the following items:
  - Pass through authentication to a supported authentication source such as Active Directory
  - General tasks definitions
  - DB basic tuning
  - One Identity Collector (Active Directory or CSV file)

- **System setup validation –** The SailPoint team will work with CCD to conduct unit testing on the product installation to verify that the product is installed and functioning correctly.
- **File Access Manager administrative setup --** SailPoint will work with CCD to configure up to 5 users with Administrative Client Access and define up to 3 File Access Manager Admin Roles.

4.3.3 Application Configuration

Each endpoint, such as Active Directory, SharePoint, Exchange, Windows File Share, etc., will be configured to communicate with File Access Manager. This configuration will include the following steps per endpoint (aka "application" in File Access Manager).

SailPoint will work with CCD to configure the applications and features in scope. An on-the-job training model will be used, where SailPoint resources will configure the first of each type of server with CCD resources watching, then CCD resources will configure the next with SailPoint resources watching, then CCD configures the rest with SailPoint available for questions if needed.

- **Configure application**
    - Connection configuration – establishing a connection between the application and File Access Manager
    - Permissions configuration – configuring the appropriate prerequisite permissions
    - Crawling scheduling – building a schedule for File Access Manager to index the resources managed by the application
    - Permissions scan scheduling – building a schedule for File Access Manager to pull the permissions associated with the managed resources
- **Install application components**
    - Install monitor – the application monitor allows File Access Manager to watch activity on the managed resources
    - Install entitlement collector – the entitlement collector is responsible for analyzing the permissions on the application
    - Install Data Classification – the data classification component builds a rules structure to simplify rules and provide extended functionality
- **Managed application setup testing and verification -** The SailPoint team will work with CCD to conduct unit testing on each configured managed application to verify that it is functioning correctly.

4.3.4 Requirements Workshop

SailPoint will conduct a workshop (either onsite or remote) with the CCD team to analyze results and finalize requirements.

- **Data analysis –** SailPoint will analyze the results returned from permissions scan, activity monitoring, and initial data classification scan.
- **Requirements review –** SailPoint will conduct a detailed requirements/use case workshop to understand the business needs around ongoing control of unstructured data.
- **Recommendations** – based on requirements, scan results, any additional information gathered, and SailPoint's experience with similar customers, SailPoint will provide best practices recommendations on how to configure File Access Manager to achieve the stated goals.
- **Requirements document** – both teams will finalize the requirements document and plan for the Control phase.

4.4 Control

Once File Access Manager is installed and each endpoint is set up, all advanced configuration can occur. This includes reporting, polices and alerts that are tailored to meet the specific business needs of CCD.

4.4.1 Reporting

File Access Manager provides a rich set of reports that will allow CCD to identify areas of critical importance to the business. SailPoint's team will work with CCD to generate and analyze up to 10 reports. Report examples include:

- **Permissions reports**
    - Over exposed resources – identifying resources that can be accessed by too many users
    - Direct users' permissions – determining a full picture of what resources specific users have access to
    - Local administrators -- determining a full picture of what local administrators have access to
- **Activities reports**
    - Privileged users' activities – determining what activities are being conducted by users with increased privileges.
- **Customer-specific reports**
    - File Access Manager's reporting engine is configured to afford CCD flexibility in configuring reports based on collected data in by File Access Manager. The SailPoint team can help configure these reports within the File Access Manager GUI. SailPoint will configure up to 3 customer-specific reports.

4.4.2 Alerts, Tasks and Controls

File Access Manager has several different options for the configuration of on-going alerts and controls. For this engagement, SailPoint will configure up to 10 alerts/controls/policies within the CCD environment. Below are several examples of policies/alerts/rules that may be configured.

- **Policies and Rules**
    - Configuring crawls to scan only *relevant* data
    - Deleting activities older than 2 years
    - Activating PII or PCI policies for classification.
    - Configuring Discard Polices to filter out noisy, uninteresting activities
- **Alerts**
    - Configuring alerts on GPO modifications in AD
    - Configuring alerts on folder deletes
    - Configuring alerts on changes to sensitive AD groups
    - Configuring alerts on permissions changes
    - Sending alerts to other systems via scripts or SysLog
- **Scheduled Task Configuration --** SailPoint will work with CCD to define an automation schedule for tasks for data collection, reporting and access review processes.
- **Additional Configuration and Troubleshooting –** perform any additional tuning and troubleshooting of the configuration.

4.4.3 Phase-end Wrap Up

SailPoint will conclude the Control phase

- **Technical Review** – SailPoint review all deliverables and provide the necessary knowledge transfer to CCD team

4.5 Transition

For the final phase, SailPoint and will work to wrap up the project, provide any remaining documentation, and transition the project to the next phase.

- **Maintenance Procedures** – SailPoint will provide detailed documentation around the on-going maintenance of File Access Manager
- **Final Knowledge Transfer** – SailPoint will conduct a session with the CCD team to review all work done and answer any remaining questions
- **Documentation** – SailPoint will provide a Run Book and any necessary product documentation to the CCD team
- **Project Close-out Meeting –** SailPoint will conduct a final meeting with the CCD team to review the engagement, answer questions, and plan next steps.
- **Project Transition –** based on the hours remaining and the desired next steps, the project will be transitioned to the next phase
    - **Option #1 –** if project work is complete but hours remain, the project will be transitioned to SailPoint's Expert Services team.
    - **Option #2 –** If all project work is complete, the project will be formally wrapped up and transitioned to SailPoint's Customer Support team.
    - **Option #3 –** if additional phases are desired, a Statement of Work or Change Order will be executed, and the teams will transition into the new project.

4.6 Knowledge Transfer

It is SailPoint's goal to educate and enable CCD staff to be functional with the File Access Manager feature set as implemented in CCD's business environment.

Throughout the duration of the implementation, SailPoint will provide as-needed sessions to review the work that has been done. The purpose of these session will be to educate CCD on the work accomplished on the product, focusing on the configurations and project-related work.

5 Resourcing, Fees and Timeline

The estimated total calendar time to completion for this SOW is approximately **18 weeks**. This timeline presumes that both parties shall be equally engaged in the effort. This SOW includes 211 **staff-days** to perform the tasks included in this SOW.

This SOW will be completed on a Time & Materials basis. The work on this SOW may be performed jointly between SailPoint and one of our implementation practice partners. Daily rates are based on an 8-hour day. Actual time over or under the 8-hours will be charged. SailPoint resources work Monday through Friday from 9am to 5pm in their local time zone, excluding holidays.

SailPoint will issue invoices on a monthly basis for services rendered or travel and expenses incurred in the previous month. Reasonable travel related expenses will be billed in addition to the rate quoted below. Time spent travelling will be billed. All overseas travel will be booked in business class.

Additional days of Services or training (Training) may be purchased at the rates set forth below for a period of one (1) year from Effective Date of this SOW. Such Services or Training rates will expire after one (1) year from Effective Date of this SOW. The parties will enter into a mutually agreeable change order (Change Order) if CCD wishes to purchase additional days of Services or Training. Additional Services or Training will not be provided by SailPoint until such Change Order is fully executed by the parties.

Phase 1 IdentityIQ Accelerator Pack Implementation

Resource Role	Duration in Weeks	Staff Days	Daily Rate	Cost
Project Lead	18	35	$2,000	$70,000
Solution Architect	18	88	$2,000	$176,000
Implementation Engineer	18	88	$1,840	$161,920
TOTAL	18	211		**$407,920**

Weekend Go-Live Support

Offering	Calendar Duration	Cost
Weekend Go-Live Support	1 weekend	$7,500.00
TOTAL	**1 weekend**	**$7,500.00**

- The Weekend Go-Live Support offering will be completed on a pre-paid fixed fee basis.
- The Weekend Go-Live Support offering covers the period from Friday 6PM to Monday 8AM (US Central Time) on the designated go-live weekend.
- Prerequisite: CCD must have an existing Expert Services or Professional Services contract with SailPoint with at least 20 hours available to cover time used by the on call Professional Services resource if that resource is called upon.

Phase 1 Travel Expenses

Required number of trips for the project will be mutually agreed upon between CCD and SailPoint. The table below gives an idea of estimated trips and cost based on prior experience with similar projects and to assist you for budget planning purposes and inclusion of such expenses on purchase orders issued to SailPoint.

Travel	Resources Traveling	Approximate Cost Per Person (USD)	Approximate Total Cost per Trip (USD)
Project Kickoff	Project Lead, Solution Architect, Implementation Engineer	$2,000	$6,000
End of Build/Pre-Testing	Solution Architect, Implementation Engineer	$2,000	$4,000
Start of Test	Solution Architect, Implementation Engineer	$2,000	$4,000
End of Test/Pre-Go Live	Project Lead, Solution Architect, Implementation Engineer	$2,000	$6,000
Total			**$20,000**

(Optional) Additional Training Credits

Training Description	Price per Credit
Training Credits	$100

All training credits must be used within one-year of the Effective Date of this SOW.

Training credits can be used towards any SailPoint training offered on Identity University. Please email training@sailpoint.com with any questions.

(Optional) Additional à la carte assistance

Resource Role	Calendar Duration	Staff Days	Daily Rate
Project Lead	1 day	1	$2,400
Solution Architect	1 day	1	$2,200
Implementation Engineer	1 day	1	$2,000

5.1 Invoicing

To ensure that your invoices are delivered to the correct location, we normally process your invoices after receipt of a purchase order. If your purchase order is not currently available we ask you to complete the following to provide us with the information we need to process your order correctly:

My company does not issue purchase orders

I have not received the final purchase order from my companies' purchasing department

The purchase order number for this SOW is

In the event your company issues purchase order, the purchase should be issued to SailPoint at orders@sailpoint.com.

IN WITNESS WHEREOF, the parties hereto have executed this SOW as of the date last below written:

City and County of Denver	**SailPoint Technologies, Inc.**
By:	By:
Name:	Name:
Title:	Title:
Date:	Date:

6 Appendix A: Assumptions

This offering and the services and deliverables contained in this SOW are based on the following key assumptions:

6.1 Build Process

- This SOW assumes that SailPoint will use the Services Standard Build (SSB) process to build the deployable solution for test and production.
- CCD will provide a version control system (e.g., SVN) for management of the configuration artifacts built for the project. If CCD does not provide a version control system, SailPoint will use its environment for Source Control.

6.2 Logistics

- CCD will provide SailPoint with access to their personnel and facilities sufficient for SailPoint to fulfill its obligations under this SOW.
- CCD will allow SailPoint staff remote access to connect their laptops to the CCD LAN via VPN or similar method.
- CCD will provide network connectivity and install necessary hardware and necessary non-SailPoint software such as the Operating Systems, Web Application Servers, Databases, database client layer (if required), Database replication to DR site, any FTP/SFTP server for the CSV files, and other infrastructure necessary for the SailPoint Staff to perform their assigned tasks under this SOW. Note: SailPoint Staff will assist with providing the list of port and protocol for CCD to consider versus any necessary hardening CCD may wish to apply on the servers.
- If a laptop is to be provided by CCD for development purposes, SailPoint requests that it meets the following minimum performance standards: 16 GB RAM, a Core i7 or higher processor and at least 100GB free disk space, preferably using SSD.
- CCD will provide necessary service accounts and credentials to the infrastructure supporting the solution, as well as to the source/target systems that the solution will be connecting to, before configuration starts, so that SailPoint team can set up the SailPoint product software without delay.
- The development environment will be ready at the start of the project (prior to the Kickoff Meeting).
- SailPoint staff working at the CCD site will have access to the Internet through CCD's LAN for the purpose of research and communicating with other SailPoint staff.
- The SailPoint resources on this project will have the ability to work remotely from the CCD site and will have remote access to the CCD development and staging environments.
- The project milestones and tasks will be managed out of CCDs Azure Devops backlog system. All resources will be required to update backlog items daily. Project backlog will consist of a Epic, Feature, Product Backlog and Task hierarchy for all project scope.

6.3 Client Resource Commitments

- The scope and timelines for this project are based on the assumption that certain business and IT-related information as described in this document is available or can be gained through interview activities with CCD's organization.
- CCD stakeholders will be available to meet with SailPoint representatives and participate in workshops as required.
- CCD will dedicate the necessary time and effort to discover, analyze, and present data to support the implementation process.

- Designated CCD stakeholders will review and sign off on deliverables within agreed upon timeframes.
- CCD will designate a project manager who will manage the overall project and with whom all project communications will be addressed, and who has the authority to act on CCD's behalf for all aspects of the project.
- Organizational rollout within the client organization(s) is the responsibility of CCD. SailPoint resources will provide input to the rollout plan and conduct no more than two (2) stakeholder demos during the implementation project.
- CCD will provide all business user testing resources and scripts, test cases, use cases and test data as required.
- CCD will be responsible for managing/conducting testing of the solution, including preparation of the UAT test cases and test data, coordination of the tester feedback, and tracking of the resolutions together with SailPoint team. SailPoint will provide support as indicated in this document.

6.4 Technical: Data Loading

- The format of any file extracts will not change during the implementation and all application file extracts will be in the correct format prior to beginning of scheduled data aggregation and correlation (Build stage).
- Only pre-existing SailPoint Connectors are to be used (including the Delimited File Connector for flat file extracts). No customer-specific connectors or customer-specific file parsers are included in this SOW, nor will any pre-existing SailPoint Connectors be modified for this engagement, unless explicitly stated in this SOW.
- This SOW does not include automation of file extracts for delivery to IdentityIQ. CCD, if required, will carry out these services.
- CCD is responsible for managing business friendly roles and entitlement descriptions.

6.5 Technical: Governance Features

- The limited time allocated for discovery and definition of roles, policies, certifications, classification or risk scoring throughout IdentityIQ is not expected to cover analysis, definition, and modeling of all roles, policies, certifications, classifications or risk scoring in the organization but rather to serve as a demonstration and mentoring so that the organization can take responsibility for managing and adjusting its governance model in the future.

6.6 Technical: Provisioning Implementation

- For All Data source/target system in scope:
    - This SOW includes the number of target system instances in production as specified in the Data Sources section, including connecting to the same number of respective test instances accessible from development/test environment(s). In other words, in production the system will only be aggregating from and provisioning to production systems unless otherwise stated in the Data Sources section.
    - CCD will provide accessibility to a representative instance of the target system from development/test environment during Configuration and UAT respectively. Note: Rework due to significant discrepancy of target systems between development/test and production will go through Change Management.
- For commercial source/target systems, this SOW assumes that the version (if applicable) is supported by its original vendor.
- CCD will provide, at the request of SailPoint team, the full documentation for any CRUDS (Create, Read, Update, Delete, and Search) operations necessary to address the scope before

implementation starts, such as specific SQL Queries, REST/Web Services and methods, Java API classes and methods, and so on.

- This SOW assumes that Special Accounts (service accounts, privileged accounts and so on) are computable for each system through logic already documented and available.
- For any source based on file, the format of the file documented in the Solution Configuration will not change during the implementation unless otherwise documented in the Solution Configuration.
- Microsoft applications and systems (if any), such as Exchange, ADFS, Office 365, SharePoint, and so on, are assumed resources of the same Active Directory Forest(s) listed in the system to onboard as part of this Scope of Work
- This SOW assumes that multiple instances/domains of the same type of server platform, database system, and/or directory (e.g., LDAP, Active Directory) to be provisioned will use the same provisioning policy. Variations to the provisioning policy within type are not included unless otherwise stated.
- This SOW assumes that forms will be deployed without customer-specific changes, unless explicitly stated.
- For any home-grown system or process that the solution is required to interact with, CCD must provide the necessary documentation or information necessary to implement the integration, migration, synchronization in scope (if any). Note: reverse-engineering of home-grown system, subsystem, processes or data format, is not included in this SOW.

6.7 Technical: Lifecycle Manager

- This SOW assumes the use of Lifecycle Manager workflows as delivered by SailPoint via Accelerator Pack.

6.8 Technical: Password Management

- Password reset, and top down password synchronization capabilities will be implemented only for systems provisioned by the SailPoint Provisioning connectors included in this SOW.
- Password reset will be implemented through challenge & response questions unless otherwise stated.
- Desktop password reset will include manual installation of the GINA plugin on up to 5 development workstations. CCD will be responsible for any additional installations required.

6.9 Weekend Go-Live Support Package

- A Weekend Go-Live Services engagement consists of 2 parts:
  - CCD will have the ability to contact SailPoint Support for assistance on the go-live production weekend.
  - SailPoint will identify a SailPoint Professional Services resource as requested by CCD. This resource will be on call in case implementation assistance is needed that cannot be provided by the SailPoint Support team. If called, this resource will bill time against CCD's Expert Services hours.
- **Prerequisite:** CCD must have an existing Expert Services contract with SailPoint with at least twenty (20) hours available to cover time used by the on call Professional Services resource if that resource is called upon.
- Weekend deployment services is limited to one (1) go-live production weekend.
- CCD must submit the request for deployment services to SailPoint four (4) weeks prior to the go-live production weekend.
- CCD may have up to four named contacts that contact SailPoint either by phone or by email.
- The deployment services must be paid for in advance upon execution of this SOW and expire within twelve (12) months of Effective Date.

- There are no refunds for unused weekend support. Unused Expert Services hours can be used under the applicable Expert Services SOW as usual.
- SailPoint will endeavor to provide a consistent resource, though a different resource may be engaged based on weekend availability.
- SailPoint team is expected to provide remote assistance only and will not be onsite with CCD for the go-live production weekend.
- CCD is expected to provide the primary project delivery staff, with SailPoint providing assistance to those resources.

6.10 Scope

- No modifications to IdentityIQ Accelerator Pack forms, workflows or configuration options will be included in this Statement of Work.
- Any items outside of scope must go through Change Management, which will involve an assessment that may lead to a change order with additional time and cost requirements. This includes any additional or modified configuration specifications that result from business user testing.
- Mutually agreed upon success criteria will be documented during week 1 of the deployment. This will need to be criteria that may be checked off prior to formal Business User Testing unless CCD extends SailPoint for assistance during the Business User Testing process.
- Tasks with explicit staff-days specified will not exceed the number of days outlined in the SOW.
- Professional Services includes the support of a Project Manager to allocate the correct resources, escalate issues, and provide regular accounting of the hours used in support of the requests submitted by the customer. The Project Manager’s time will be billed as part of the Project Lead hours.
- Standard SailPoint supplied documentation; SailPoint’s online community forum and FAQ repository; SailPoint’s standard deployment overview; and the provided training materials will meet CCD’s documentation requirements. If additional documentation is requested, then CCD may contract SailPoint to write additional documentation per the services rates specified above.
- Project delays caused as a result of CCD actions may result in additional charges based on the resource daily rates quoted above.
- The certification processes will leverage the IdentityIQ out of the box processes.
- The IdentityIQ objects either initialized or extended throughout this engagement, such as applications, identities, accounts, entitlements, roles, policies and so on, will reference only data already loaded into the product by implementing data collection or enrichment from sources or target defined in this SOW.
- This SOW assumes only out-of-the-box reports supplied with IdentityIQ, IdentityIQ Accelerator Pack and the data export samples as specified, unless otherwise stated.

6.10 Change Management Process

If any changes in scope are identified throughout the course of the project, SailPoint will activate the Change Management process that consists (at a high level) of the following steps:

- Change Definition: confirm the understanding and nature of the change with CCD in order to obtain a written functional and technical description of the current and desired situation
- Change Qualification: Research the options available to address the change. Each option should be evaluated in terms of:
  - Impact analysis against each of the Use Cases listed in the signed-off Solution Configuration documentation
  - pros/cons considerations to measure each option

  - And time/dollar cost if applicable.
- The Options to address a change may be:
  - Non-technical: change may be addressed by educating selected users, e.g. sharing a pointer to SailPoint documentation, practical white papers, existing project documentation, or improve the communication plan to the end-user.
  - External: although surfacing in IdentityIQ, the change may be addressed by configuring something outside of the SailPoint product
  - OOTB: change may be addressed by configuring an OOTB feature
  - Workaround: the change can be addressed through another way than originally thought, maybe not exactly but close enough to the requirement to be acceptable.
  - Mitigation: change may be avoided by neutralizing the situation causing the need for change.
  - Actual change, with less or more implementation effort, time and cost.
- Explanation to client leading to written decision
- Change Order (if required)
- Assimilation in the Project plan / re-planning once confirmed.

General notes about changes:

- Even an out of the box feature that addresses a change may still infer a cost for document updates and/or re-testing work that can exceed the time needed to reconfigure or implement the feature.
- Request for changes are more likely to result in higher cost and delay if they are raised later rather than sooner in the project. It is a best practice in the Identity and Access Management industry to mitigate this aspect by phasing IDM projects.

6.11 Other

- Travel and expenses (T&E) are in addition to the project costs included in this SOW.
- This SOW is based on time and materials (i.e. it is not a fixed bid).

If any of these assumptions prove to be incorrect, this will adversely affect the deliverables outlined in this SOW and timelines assumed hereunder and may increase the hours required and necessitate a change order.

7 Appendix B: Project Governance

Project Governance is performed on every SailPoint deployment and is intended to provide checkpoints throughout the engagement to ensure SailPoint recommended practices are being applied. These reviews will be conducted at each major milestone for each new piece of functionality to be added. These checkpoints are described in the subsequent sections below.

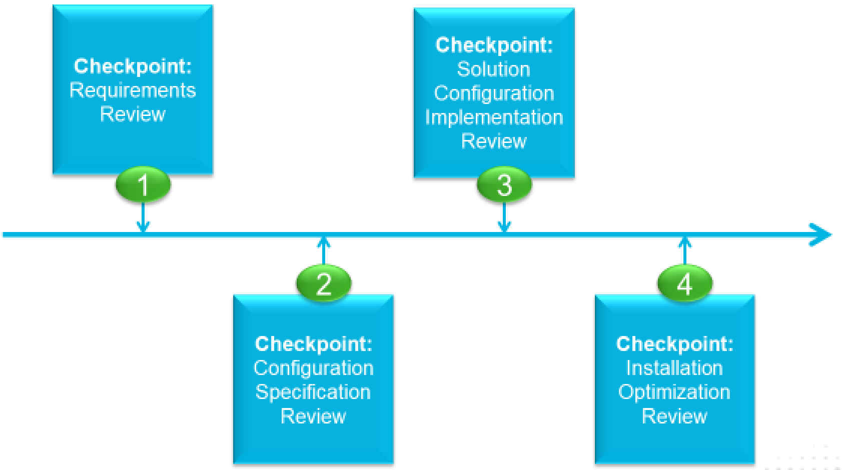
Checkpoint: Requirements Review
1
Checkpoint: Solution Configuration Implementation Review
3
2
Checkpoint: Configuration Specification Review
4
Checkpoint: Installation Optimization Review

Figure 5: Summary of Project Governance Checkpoints

7.1 Checkpoint 1: Requirements Review

This checkpoint will:

- Validate that the appropriate infrastructure (e.g., development/test/production instances, source control system, build process) is in place or planned for the project to be successful
- Validate that there is a written definition of the requirements for the functionality to be delivered
- Validate that the requirements are appropriate for an IdentityIQ-based solution

7.2 Checkpoint 2: Configuration Specification Review

This checkpoint will:

- Confirm that all parties have a clear understanding and written definition of how the functionality described in the requirements will be delivered
- Provide external validation of configuration decisions
- Review the connected systems and provide applicable lessons learned from similar projects
- Review the deployment and testing configuration strategies and processes

7.3 Checkpoint 3: Solution Configuration Review

This checkpoint will:

- Confirm that all configuration for a customer implementation follows SailPoint best practices
- Identify any potential performance concerns with the solution

7.4 Checkpoint 4: Installation Optimization Review

This checkpoint will:

- confirm that database and application server architecture for the production environment is sized, secured, and monitored appropriately for the customer's current and short-term future needs, usually accommodating 2-3 years of growth

- highlight any topological related issues, such as placement of infrastructure on different vlans, firewalling between the application servers and database servers, and other similar considerations
- highlight any concurrency configurations for system optimization

8 Appendix C: Training

This SOW includes resourcing for the End-User and Administrator training sessions described below. SailPoint provides a free self-paced IdentityIQ Introduction Training course to all customers and partners. The IdentityIQ Implementation: Essentials Training is available for an additional fee.

SailPoint will assist with the training of administrators and end-users as described below:

8.1 IdentityIQ Introduction Training

SailPoint provides a free self-paced IdentityIQ Introduction course to all customers and partners. This course covers the following topics:

- Creating identities and accounts
- Creating Roles
- Defining policies
- Modeling risk
- Certifying employees using access reviews
- Working with Lifecycle Manager
- Creating reports

8.2 Weekly Training Sessions

Throughout the duration of the implementation, SailPoint will provide a weekly session to review the work that has been done. The purpose of this session is to educate the client on the work accomplished on the product, focusing on the configurations and project related work. These sessions will help validate that the work being accomplished matches the configuration specification.

For more extensive training on IdentityIQ's full capabilities, it is recommended that the client's employees attend the IdentityIQ Implementation: Essentials Training as described below.

8.3 Product and Project Orientation

During the Project Kick-off as described earlier the client has the option for SailPoint to conduct a basic orientation session so that the project team can be familiarized with the IdentityIQ product architecture and functionality, terminology and project approach.

8.4 IdentityIQ Implementation: Essentials Training

This is an optional course, available by purchasing training credits.

Target audience: Staff Implementers or System Administrators responsible for application or complex role configuration and implementation

Duration: 4 days

Location: Austin, TX; London, England; Amsterdam, Netherlands; others upon request

Overview: This course covers the following general topics:

- IdentityIQ Installation and Architecture
- Services Delivery Overview and Best Practices
- Access Management
- Application Account/Group Aggregation (Delimited File, JDBC, LDAP, Multiplexed and Logical Applications)
- Roles (Business, IT)
- Policies
- Risk Modeling

- Tasks
- Rules (BeanShell) and the SailPoint API
- Lifecycle Manager
- Business Processes (Workflow Engine)
- Performance Tuning and Capacity Planning
- Debugging, Troubleshooting, Logging
- Customer Specific Reports/Data Export
- Provisioning

Prerequisites: It is highly recommended that attendees take the web-based IdentityIQ Introduction Training prior to attending the IdentityIQ Implementation: Essentials Training.

This course is the same Implementer training offered to our partners. It is intended for clients wishing to ultimately take responsibility for delivering their SailPoint solution. The course utilizes a combination of classroom instruction and hands-on lab exercises to guide the participant through the process of installing and configuring an instance of IdentityIQ. This course also assumes follow on knowledge transfer with the trained staff via a weekly 1-hour technical project recap by the SailPoint deployment team.

Quotation

Quote #:	Q-15277-1
Date:	9/30/2019 11:26 AM
Expires On:	2/29/2020

SailPoint Technologies

11120 Four Points Drive, Suite 100
Austin, TX 78726
US

Phone: (512) 346-2000

Ship To
Nate Kresse
City and County of Denver
1437 Bannock St
Denver, Colorado 80202
United States
7209134944
nate.kresse@denvergov.org

Bill To
City and County of Denver
1437 Bannock St
Denver, Colorado 80202
United States

SALESPERSON	Phone	EMAIL	PAYMENT METHOD
Richard Rossman		richard.rossman@sailpoint.com	Net 30

PART #	QTY	DESCRIPTION	NET UNIT PRICE	EXTENDED
IIQ-GOV-G3	1	IdentityIQ Core Governance Platform - Tier 3 (10K - 25K Identities)	$47,300.00	$47,300.00
BUNDLE-IGS LIC-IU	17,000	IdentityIQ Governance Suite - Internal Identity cube	$33.00	$561,000.00
IIQ-FS-O365-IU	17,000	IdentityIQ for O365 File Storage - Price per Internal Identity cube	$3.74	$63,580.00
IIQ-IAM-OKTA-IU	17,000	IdentityIQ for Okta - Price per Internal Identity cube	$1.32	$22,440.00
IIQ-SCIM-ServiceNow Catalog	1	ServiceNow Service Catalog SCIM	$12,100.00	$12,100.00
IIQ-SCIM-SVM-IU	17,000	IdentityIQ for ServiceNow Catalog - Price per Internal Identity cube	$0.88	$14,960.00
IIQ-SDIM-SVM	1	IdentityIQ Service Desk Integration Module - ServiceNow	$6,600.00	$6,600.00
IIQ-SDIM-SVM-IU	17,000	IdentityIQ for ServiceNow Service Desk - Price per Internal Identity cube	$0.88	$14,960.00

PART #	QTY	DESCRIPTION	NET UNIT PRICE	EXTENDED
PS-TRNG-CREDIT	100	Training Credit	$90.00	$9,000.00
			Total Price:	$751,940.00

PART #	Support	SUPPORT AMOUNT
SPT-STD	Standard Support (Business Hours Coverage). - Support hours – Monday through Friday, 8am-6pm - Support for a single production instance - Support SLA based on one geographic time zone specified by customer	$0.00

License Type

Customer shall receive a perpetual license to use the above listed Software to support up to the number of Identity Cubes stated above.

Payment

Upon execution of the Quote, SailPoint will issue an invoice for the Total Price and Customer agrees to pay in accordance with the payment terms outlined in the Agreement.

Support and Maintenance Services

Standard Support and Maintenance Services will be provided during the initial twelve (12) months from the Effective Date for no additional fee. If Support and Maintenance has been elevated to premium for the initial twelve (12) months, then a premium uplift fee will be identified in the Pricing Table above. Year 2 Support and Maintenance may be renewed at the same level of support for:

Year 2 - USD 148,588.00
Year 3 and beyond – Support and Maintenance Services renewals are offered on an annual subscription basis and may increase in subsequent years by 5%.

Implementation Services if Stated in Pricing Table Above

SailPoint will provide the number of days/hours for Implementation Service hours as stated in the Pricing Table above on a pre-paid basis. The Implementation Services will be outlined in a Statement of Work and mutually agreed to by the parties. Reasonable, necessary and documented travels and living expenses ("T&E") are not included. SailPoint will invoice Customer separately for such actual T&E monthly as the services are performed. All Implementation Services purchased must be used within one year of the Schedule effective date.

Additional Implementation Services will be available on a time and material basis as mutually agreed to in a follow-on schedule. SailPoint will invoice for such services and T&E monthly as such services are performed.

Training Services if Stated in Pricing Table Above

SailPoint will provide the number of training credits as stated in the above pricing table. Training Services may be conducted at either a SailPoint facility, a Customer/third party facility, or electronically via a SailPoint provided website. The training credits purchased above may be applied for the attendance of any then currently available classes as offered at SailPoint's Identity University plus sales tax, if applicable. The actual training services selected by Customer will be identified in either a mutually executed statement of work or upon enrollment at the Identity University. For courses taught at a SailPoint facility, Customer's travels and living expenses are not included and will be Customer's responsibility. For courses taught at a Customer provided facility, any SailPoint reasonable, necessary and documented travel and living expenses ("T&E") to teach at the Customer's facility are not included and will be the responsibility of Customer. All training service credits must be used within one year of the Schedule effective date.

Definition(s)

Identity Cube Usage:

The actual type of Identity Cube(s) applicable to this quote are identifies in the pricing table above under the Part # and Description columns.

- **Internal Identity Cubes** means an entity or person that is an employee, contractor or outsourcer to whom a customer provides access to its internal and external systems as part of the Customer's normal business operations.
- **Business Partner Cubes** means an entity or person, other than employees, contractors or consumers to whom Customer provides access to its internal or external systems (up to 5 Sources) as part of the Customer's normal business operations (e.g. providing access to a quoting system for independent insurance brokers).
- **Lite User Identity Cubes** means any entity or person who rarely interacts with the Software and to whom a Customer provides limited access to its internal or external systems (up to 5 Sources) as part of the Customer's normal business operations (e.g., retail location employees, manufacturing line workers, students etc.).
- **Inactive Identity Cubes** means a unique collection of Identity data for an individual human or non-human bot that no longer is associated with the Customer. Inactive Identity Cubes cannot manage passwords, certify access, or be provisioned. Accounts contained in these cubes are disabled so they cannot access customer IT resources. Customer is entitled to store Inactive Identities Cubes, up to thirty percent (30%) of the combined total identities across all types of Identity Cubes (i.e. Internal, Business Partner...).
- **Non-Human user or bot** is a preconfigured software instance that uses business processes and/or artificial intelligence to complete the autonomous execution of one or more processes, activities, transactions, and/or tasks in one or more systems to deliver work output. This includes IOT devices that can be used to automate processes, monitor and control operations, or optimize supply chains. In each case, the RPA, Bot, or IoT device has access to one or more systems or applications and that access needs to be governed like any other identity.

General

All pricing is in USD and is strictly Customer/SailPoint confidential. Notwithstanding the foregoing, Customer may disclose pricing or any other information as required by applicable law.

Software License Agreement or EULA

Customer, by its execution of this Quote, or incorporation of this Quote by reference into a Customer purchase order, hereby orders and purchases for delivery the software and services identified herein pursuant to the terms and conditions of the fully executed software license agreement executed between the parties ("Agreement").

Any terms contained in a Customer generated purchase order shall not apply to this Quote even if SailPoint has signed such document as a form of receipt and acceptance thereof.

Delivery of the Software will be provided via electronic download in accordance with the terms of the Agreement.

Notes

Customer	**SailPoint Technologies, Inc.**
By: ___________________________	By: ______________________________
Print Name: ____________________	Print Name: ______________________
Title: __________________________	Title: _____________________________
Date: _________________________	Date: ____________________________

The Effective Date of this Quote is the date of last signature above.