This Statement of Work ("**SOW**") is issued pursuant to Master Services Agreement number [NewTBD], by and between NCC Group Security Services, Inc. ("**NCC Group**") and IndexData ("**Client**") and is effective as of the date last signed below by both parties. Terms not otherwise defined in this SOW shall have the meanings as defined in the Agreement. In the event of any conflict between the terms of this SOW and the Agreement, the terms in this SOW shall govern.

1. **Description of NCC Group Project Deliverables:** At the completion of this effort, NCC Group will prepare and present one report to be discussed and reviewed in one project close call or meeting:

   - **Executive Summary –** discussing the findings at a high-level, in particular:
       - Summary of the project scope and methodology
       - Summary of NCC Group opinion and test findings
       - Analysis of security issues identified, including:
           o Recommended next steps, including recommendations as to which vulnerabilities should be addressed as a priority
           o Analysis of security needs, including conformance to best practices
   - **Detailed Findings –** discussing the vulnerabilities identified at a low technical level, in particular:
       - Listing of identified security vulnerabilities
       - Recommended solutions for gaps and vulnerabilities. Solution descriptions will include:
           o Specific technical recommendations for remediation
           o Specific process recommendations for maintaining a secure environment
   - **Appendices**
       - Reference materials used to support findings within the report
       - Additional detail or context for complex security issues or conditions

   - **Letter of Engagement**
     NCC Group will produce a letter of engagement ("LOE") indicating that NCC Group performed a test of Client's environment and application (limited by the engagement scope). If requested in writing by the Client, NCC Group will wait to produce this LOE until after NCC Group has performed a retest (such retest to be performed pursuant to a Change Order if not otherwise provided for in this SOW), provided that the retest is performed within 3 months of completion of the initial testing. This document is targeted towards potential customers that have security concerns or require third-party audits. Client shall (i) not modify the LOE prior to disclosing it to third parties, and (ii) always disclose the LOE in its entirety. The LOE will indicate the type of test performed, and when it was accomplished. No details of the findings or methodology used will be included. Client cannot share the LOE with any third party, including (without limitation) partners, clients, or vendors, without a Non-Disclosure Agreement ("NDA")

2. **Description of NCC Group Project Schedule:** NCC Group will devote 12 person-days to the project.

3. **Description of Targets**: Testing efforts will be contingent on the given timeframe and will focus on the following Client Targets:

   - Folio Server-Side Authorization Assessment Security asssessment of the core Folio authentication/authorization components - Okapi, mod-users, mod-permissions, mod-login, and mod-authtoken - as described in "Securing Okapi" (https://github.com/folio-org/okapi/blob/master/doc/securing.md)

   Details of the application(s), including virtual hostnames, credentials, API keys, and other materials that may be required by NCC Group to perform testing, will be provided by Client before or during the project kick-off meeting which will be scheduled between NCC Group and the Client prior to testing.

4. **Description of Services:** All testing and assessment efforts will be contingent on the given timeframe and will focus on the following:

- **Web Service Security Testing**: NCC Group will perform web services security testing on the in-scope targets, covering the following items. Unless otherwise noted, automated and manual techniques based on both public and internal knowledge will be leveraged to conduct tests. .
  - Application Abuse/Logic Testing: determine whether attackers can:
    - Obtain access to private data belonging to other users and/or other clients of the web service
    - Make unauthorized changes to the application or its data
    - Bypass business logic rules
    - Bypass authentication and authorization mechanisms
    - Elevate privileges to site administrator or other higher-privileged users
    - Hijack accounts of other users
  - Common Web Services Vulnerability Testing: evaluate the application for common web services security issues, including:
    - Code execution
    - Privilege escalation
    - Application denial of service
    - Injection attacks (including SQL, LDAP, XML)
    - XML complexity, serialization, and external reference attacks
    - Message replay attacks
    - WSDL/WS-Inspection information disclosure vulnerabilities
    - Incorrect use of WS-Security standards
    - Transport security weaknesses including:
      - Insufficient certification chain validation
      - Weak cipher suite configuration

  - Code Review of Protection Mechanisms: NCC Group will review the source code to verify correct implementation of the following protection components as applicable:
    - Data validation mechanisms
    - Cryptography
    - Storage of application secrets
    - Authentication
    - Certificate validation
    - Output encoding mechanisms
    - Single Sign-On (SSO) and session management (session generation and session token randomness)
  - Code Review for Common Vulnerabilities: NCC Group will examine source code to find vulnerabilities in:
    - Database calls and queries (usage and implementation)
    - Memory management
    - Buffer/heap management (vulnerability to overflow)
    - Integer handling (vulnerability to overflow, underflow, and arithmetic errors)
    - Format strings

- **Project Management Services:** NCC Group will provide a dedicated project manager with experience managing security-related engagements. Dependent on prompt and accurate client responses, the NCC Group project manager will:
  - Provide oversight and coordination of entire project from start to finish. Serve as the single point of contact for project scheduling, logistics, and non-technical issues
  - Collate, communicate and track all project-related tasks and issues. Perform necessary follow-up to ensure tasks and issues are resolved in a timely manner
  - Ensure all required review materials are ready at the proper time. Notify the appropriate parties of missing or overdue materials impacting NCC Group's ability to deliver the work in scope

- Ensure any schedule or scope adjustments are accurate and made with the appropriate agreement of all parties
- Facilitate access to internal and/or privileged client systems and locations
- As needed, coordinate the acquisition, provisioning, shipping and/or tracking of any required hardware or devices
- Coordinate and schedule all project meetings per standard NCC Group process
- Quickly escalate and resolve project issues as they arise
- Ensure any agreed-to procedures or plans are followed, both by NCC Group and the client
- Resolve any third-party project dependencies
- As needed, build and implement custom project management trackers and tools, tailored to the needs of the project

5. **Description of Client Responsibilities**: NCC Group has used this information in establishing the project schedule and Fees for this project. In the event an item identified below does not occur in the manner or time frame shown, such circumstance shall constitute a change that may require an adjustment to the schedule and/or Fee. In connection with the services performed by NCC Group under this SOW, the Client will provide NCC Group with:

- **Web Services Security Testing Request List:**
    - A client application for the in-scope web service(s), and complete installation instructions, that can be used to perform all the requests within scope of the engagement. Note: failure to provide a client application can cause a significant change to this SOW as NCC Group consultants may be required to develop one during the course of the engagement.
    - Access to a dedicated test environment containing a functional instance(s) of the in-scope web services.
    - Test accounts and credentials for the web service. Multiple test accounts should be provided for each privilege level if multiple levels exist (for example, administrators and regular users).
    - Information regarding any potential difficulties with proxying traffic and testing such as if certificate pinning is in use, or if the test environment doesn't possess a valid certificate.
    - Information regarding any non-standard communication protocols in use by the application.
    - Access to developers and QA engineers for technical questions throughout the project as needed.
    - Any relevant design and architecture documentation, including:
        - Web service and API method definitions and documentation.
        - WSDL/WADL or relevant configuration files.
    - VPN credentials if remote access to protected environments is required (e.g. intranet test lab).
    - For NCC Group consultants performing on-site work, facilities access (e.g. cardkeys/badges), working space (e.g. dedicated room, desk, chairs), and technical accommodations (e.g. telephone, guest internet wireless access, access to electric outlets) necessary to facilitate performance of this SOW should be provisioned by Client prior to any scheduled work.
    - Access to buildable source code for the in-scope applications(s), of the most relevant version (which is typically the most recent, production-ready version released to customers).

- **Project Management Client Responsibilities**
    - Prompt and accurate responses to requests and tasks from the NCC Group project manager
    - A single point of contact with firm knowledge of client systems and ownership as well as overall client organization, policies, and vendor provisioning processes
    - A clear escalation path should the single point of contact become unavailable
    - Early internal communication with developers and engineers, informing them of scheduled NCC Group services. This communication should assess general readiness for the scheduled NCC Group services

- **General Responsibilities**
  - Immediate access to Client's business operations and technical resources required for the delivery of the services identified in this SOW, and not limited to: individual business unit managers, and IT security operations staff; and
  - A dedicated project manager, to ensure that the relevant IT operations staff and business unit managers are briefed and aware of NCC Group testing and interview tasks being undertaken; and
  - Immediate notification of any compliance or regulatory efforts that the results of NCC Group testing may be used to support and/or that will **require additional deliverables** (*i.e.*, PCI-DSS, OCC, *etc.*); and
  - Permission to perform testing from any third-party vendors that either own applications or infrastructure that is in the scope of the engagement.

6. **Fees and Invoicing:** Client will pay to NCC Group the fees listed below and the actual travel and living expenses incurred, up to a maximum of the expense cap below (unless otherwise agreed by Client) ("Fees"). All fixed priced Services will be invoiced upon completion of each milestone as listed below.

Project Name: **Folio Test**

Information Security Services	$30,000.00
Project Management	$2,400.00
Expense Cap:	$ .00
PROJECT TOTAL (Purchase Order Amount):	**$32,400.00**

Payment Structure:

Milestone 1:	Signature of SOW	Payment:	$16,200.00
Milestone 2:	Project Completion	Payment:	$16,200.00 + Expenses

Payment Information:

Purchase Order Number:		Payment Terms:	Net 30

Unless otherwise provided for in this SOW, all Fees are for Services performed during the normal, daytime, business hours of the location at which they are performed (which shall be determined by NCC Group in its reasonable opinion) ("Normal Business Hours"). Any Services that Client requests to be performed outside of Normal Business Hours following mutual agreement of the SOW will result in an automatic increase in the Fees at a rate of 1.5 x daily rate stipulated in this SOW, or, if no daily rate is stipulated in this SOW, an additional daily fee of a minimum of $1,000 per day will be charged.

7. **Cancelation Policy:**

Upon mutual agreement of a start date for Services ("**Start Date**"), NCC Group will immediately start to allocate resources and facilities and commit to third party expenditure to fulfil its contractual commitments. Client may, on written notice, re-schedule or cancel the Services but if it does so, Client agrees to pay NCC Group a proportion of the Fees under the relevant SOW ("**Cancelation Fees**") as compensation (and not as a penalty) to reflect the losses which NCC Group will incur as a result of such cancelation or re-scheduling, as follows:

(i) cancelation request 8-21 days before the Start Date: 50% of the Fees for the relevant SOW will be payable;

(ii) re-schedule request 8-14 days before the Start Date: 50% of the Fees for the relevant SOW will be payable;

(iii) cancelation or rescheduling request within 7 days of the Start Date: 100% of the Fees for the relevant SOW will be payable.

Cancelation Fees will be paid within thirty (30) days of approval of the cancellation or rescheduling request.   The Parties have computed, estimated, and agreed upon the Cancelation Fees as an attempt to make a reasonable forecast of probable actual loss because of the difficulty of estimating with exactness the damages which will result.

Where NCC Group permits a rescheduling of the Services, Client will pay the full Fees for the Services as rescheduled in addition to any Cancelation Fees specified above (Cancelation Fees will not be credited against the full Fees). Client will also be responsible for all non-refundable expenses which have been incurred prior to cancellation or rescheduling.

8. **Export Control**

Client to confirm whether any material or information NCC Group consultants will come into contact with during this engagement will be subject to export control laws or regulations:

Yes ☐

No ☒

8. **Special Terms:**

9. **Address for Performance of the Services:**

Remote Testing	Testing will be performed remotely unless otherwise agreed.

Location for Performance of Onsite Services	
Street Address	
City, State Zip	

10. **Contact Information:**

CLIENT	
Primary Contact	Mike Gorrell
Address	
Phone	
Email	
Accounts Payable Contact	
Phone	
Email	

INVOICING ADDRESS	

NCC Group	
Name	Brett Arpaia

Address	123 Mission Street, Suite 900 San Francisco, CA 94105-5126
Phone	+1 646-362-9613
Fax	415-974-6339
Email	Brett.Arpaia@nccgroup.com

AGREED:

CLIENT: **NCC GROUP SECURITY SERVICES, INC.:**

Signature by: _____   Signature by: _____

Printed Name: _____   Printed Name: _____

Title: _____   Title: _____

Date: _____   Date: _____