# RFP and Contract Exercise Documents - Table of Contents

<table>
<thead>
<tr>
<th>Document</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFP A</td>
<td>1</td>
</tr>
<tr>
<td>RFP B</td>
<td>9</td>
</tr>
<tr>
<td>RFP C</td>
<td>15</td>
</tr>
<tr>
<td>RFP D</td>
<td>18</td>
</tr>
<tr>
<td>RFP E</td>
<td>20</td>
</tr>
<tr>
<td>Contract A</td>
<td>21</td>
</tr>
<tr>
<td>Contract B</td>
<td>25</td>
</tr>
<tr>
<td>Contract C</td>
<td>31</td>
</tr>
<tr>
<td>Contract D</td>
<td>36</td>
</tr>
<tr>
<td>Contract E</td>
<td>39</td>
</tr>
</tbody>
</table>
E. **FERPA** – means the Family and Educational Rights and Privacy Act (20 U.S.C. 1232g) and any applicable regulations promulgated thereunder, including but not limited to 34 C.F.R. Part 99.

F. **Handle** – means (in the context of Confidential Information) to create, view, modify, store, transmit or delete

G. **PII** – means personally identifiable information, as defined under FERPA.

H. **System** – means any information technology processing device, including routers, servers, Applications, workstations and mobile devices.

I. **Vendor** – means an entity awarded a contract by the DOE to provide a product, service or work for the DOE.

4. **Note on Security & Privacy**

DOE systems and Applications may contain sensitive data, including records of academic performance, medical, legal, criminal and family details and proprietary and confidential internal records concerning DOE students and employees, in addition to information that is confidential by law.

Failure to protect Confidential Information from unauthorized disclosure or abuse can have severe legal, financial and reputation consequences for the DOE, its students, families, employees and the Vendor.

5. **Relevant Laws, Regulation, Policies and Standards**

   A. **Family Education Rights and Privacy Act (FERPA)**

   FERPA is the primary federal legislation that governs the privacy of educational records. The Vendor must hold all PII obtained, learned or developed by the Vendor in confidence pursuant to applicable provisions of FERPA. The Vendor understands that the release of PII to persons or agencies not authorized to receive such information is a violation of US federal law. Vendor understands that under FERPA it must limit access to PII to those who need to know the Confidential Information for Vendor to perform its duties under its contract, and to destroy all copies of PII, or to return PII to the DOE, when no longer needed or at the expiration of any contract. Vendor understands that upon request, it must permit DOE access to PII that it holds, in order for DOE to meet other obligations under FERPA or pursuant to law.

   B. **New York Education Law § 3012-c(10)**

   New York Education Law § 3012-c(10) governs the confidentiality of certain Confidential Information concerning teacher and principal evaluation data. Vendor understands that to the extent that information protected under New York State Education Law §3012-c(10) is shared with Vendor, Vendor is responsible for complying with this law. Vendor further understands that New York State Education Law § 2-d imposes additional requirements concerning such Confidential Information.
C. **New York State Education Law § 2-d**

New York State Education Law §2-d is a state law that imposes a number of confidentiality and data security requirements in addition to those found in FERPA and New York Education Law §3012-c(10), including a number of requirements and obligations that apply directly to Vendor. Vendor understands that it is required to comply with the requirements of New York Education Law 2-d and any regulations promulgated thereunder. Vendor understands that among other requirements, New York Education Law §2-d requires Vendor to:

- Limit internal access to Confidential Information covered under Education Law §2-d (“Covered Confidential Information”) to those with legitimate educational interests;
- Not use Covered Confidential Information for any other purposes than those authorized in its contract;
- Not disclose Covered Confidential Information without parental consent, except to authorized representatives of the Vendor who are carrying out the contract;
- Maintain reasonable technical, administrative and physical safeguards to protect Covered Confidential Information;
- Not sell covered Confidential Information, nor use Covered Confidential Information for marketing purposes;
- Provide training on laws governing confidentiality to its officers, employees and assignees with access to Covered Confidential Information;
- Use encryption technology to protect Covered Confidential Information while in motion or in its custody from unauthorized disclosure, using a technology or methodology specified under HIPAA by the US Department of Health and Human Services; and
- Notify the DOE of any security breach resulting in an unauthorized release of Covered Confidential Information, and to promptly reimburse DOE for the full notification cost.

Vendor also agrees to cooperate with the DOE in complying with any regulations implementing New York Education Law § 2-d and any DOE or state policies promulgated pursuant to New York Education Law § 2-d, including but not limited to any requirements concerning (a) the inclusion of a data security and privacy plan in Vendor’s contract with the DOE, (b) its compliance with any future DOE data privacy/security policy, (c) its compliance with and signature of the Parent Bill of Rights required of the DOE, and (d) the inclusion of supplemental information concerning Vendor’s contract in the Parent Bill of Rights.

A. **DOITT Citywide Information Security Policies & and DOE RFP Information Security Requirements**

At all locations where Vendor stores any Confidential Information, the Vendor shall implement information security policies and procedures that, at a minimum, are at least rigorous as the DOITT Citywide Information Security Policies, accessible at: [http://www.nyc.gov/html/doitt/html/business/security.shtml](http://www.nyc.gov/html/doitt/html/business/security.shtml), and/or this document (Request for Proposals (“RFP”) Information Security Requirements).

B. **DOE Chancellor’s Regulation A-820**

The Vendor must comply with the DOE Chancellor’s Regulation A-820, accessible at [http://docs.nycenet.edu/docushare/dsweb/Get/Document-44/A-820.pdf](http://docs.nycenet.edu/docushare/dsweb/Get/Document-44/A-820.pdf), which governs access to and the disclosure of information contained in student records.

C. **NYSED Records Retention and Disposition Schedule ED-1**

Schedule ED-1 specifies which information must be preserved for long periods of time in order to ensure business continuity, resolve fiscal and administrative questions and provide evidence in the event of litigation.
D. **DIIT SAML Integration Guidelines**

This is a technical document that specifies authentication options for integration with DOE Systems. Vendor must support authentication for DOE users as specified in the such document, set forth below in Section 18.

E. **DOE Secure Coding Standard**

This document defines mandated secure coding practices for all Applications that Handle Confidential Information. Code for Applications that Handle Confidential Information must comply with with such standard. The DOE’s Secure Coding Standard is set forth below in Section 19 as an example. Vendors can use this as a reference.

6. **Information Security Policies**

   A. Vendors must have, and upon request by the DOE shall promptly provide the DOE with copies of its, information security policies that cover the following elements:

   1. Data classification and privacy
   2. Security training and awareness
   3. Systems administration, patching and configuration
   4. Application development and code review
   5. Incident response
   6. Workstation management, mobile devices and antivirus
   7. Backups, disaster recovery and business continuity
   8. Regular audits and testing
   9. Requirements for third-party business partners and contractors
   10. Compliance with information security or privacy laws, rules, regulations or standards
   11. Any other information security policies

   B. Policy Requirements: In addition to addressing the elements set forth above:

      1. Vendor must indicate in their policies the date of the most recent revision.
      2. Vendor must include a certification from its Chief Operating Officer, or individual with an equivalent title with authority to represent the Vendor, with Vendor’s proposal/response to the RFP that all of the above elements are addressed in Vendor’s security policies, and that such policies are at least as rigorous as the policies set forth in this document and the NYC DoITT Citywide Information Security Policies. If Vendor cannot make such certification for any reason (e.g Vendor’s policies do not address an element listed above), Vendor must notify the DOE of the deficiency in its proposal/response to the RFP.
      3. Vendor shall maintain compliance with such policies and, unless the Vendor receives the DOE’s prior written approval, Vendor shall not make any changes to such policies that would result in such policies (i) not addressing one or more elements set forth above or (ii) not being as rigorous as the policies set forth in this document or the NYC DoITT Citywide Information Security Policies.

7. **Privacy & Confidentiality**

   A. The Vendor must hold Confidential Information in strict confidence and not disclose it to any third parties nor make use of such Data for its own benefit or for the benefit of another, or for any use other than the purpose agreed upon.

   B. The Vendor shall use commercially reasonable efforts to secure and defend any System housing Confidential Information against third parties who may seek to breach the security thereof, including, but not limited to
breaches by unauthorized access or making unauthorized modifications to such System.

C. The Vendor shall protect and secure all Confidential Information in transit (collected, copied and moved) and at rest (stored on the physical servers), including during any electronic data transmission or electronic or physical media transfer.

D. The Vendor shall maintain all copies or reproductions of Confidential Information with the same security it maintains the originals. At the point in which the Confidential Information is no longer useful for its primary or retention purposes, as specified by DOE, Vendor must destroy such Data, making it unusable and unrecoverable.

E. For all Application screens, front pages of reports, and landing pages of web Applications that contain Confidential Information, Vendor must include prominent confidentiality notices in legible-sized font on each page (e.g. a prominent notice that the information on such screen or report is confidential on the bottom of a web screen or the footer of a report page).

F. All web Application screens that contain Confidential Information must be non-cacheable.

G. Confidential Information should not appear in URLs.

H. Vendor’s development, test and QA environments shall not use real Confidential Information.

8. Application Development

A. Vendors shall have a comprehensive secure development lifecycle System in place consistent with industry standard best practices, including policies, training, audits, testing, emergency updates, proactive management, and regular updates to the secure development lifecycle System itself.

B. Code for Applications that handle Confidential Information must comply with the DOE Secure Coding Standard. Any exceptions to this standard must be approved in writing by the DOE.

C. Vendor must review and test all application code for security weaknesses and backdoors prior to deployment with DOE. All high risk findings and exploitable vulnerabilities must be resolved before the Application is released. A development manager of Vendor must certify in writing to the DOE that a security review has been conducted and that all risks are acceptable before every release. For further information please refer to National Institute of Standards and Technology ("NIST") Special Publication 800-64 Revision 2.

D. Vendors that handle Confidential Information must respond to and resolve security-related bug reports, inquiries and incidents in a timely and professional manner. The Vendor must notify the DOE within 24 hours of when Vendor becomes aware of any such incident that poses a potential risk to DOE data. The Vendor shall send the notification to sppsecurity@schools.nyc.gov.
9. **Authentication & Identity Management**

A. If an application requires Single Sign-On (SSO) integration with the DOE, the Vendor must support authentication for DOE Users as specified in the DIIT SAML Integration Guidelines
   1. Vendors will not have the ability to make any changes to the DOE Identity Management Systems.
   2. If new DOE Users need to be enrolled or register in order to use a Vendor’s System, the plan for registration process and ownership of identity management must be agreed upon in writing by DIIT Office of Information Security.

B. If the Vendor maintains its own identity management system for its users, it must:
   1. Enforce a one user, one account policy in which shared/group accounts and duplicate accounts are not permitted
   2. Be free of testing, development and non-production accounts.
   3. Maintain accurate legal name, address, phone number information for all users who are permitted to access Confidential Information, and upon request from the DOE, produce lists of users who will have access to Confidential Information.
   4. Enforce a strong password policy of eight characters minimum, with mixed case and at least one number or special character.
   5. Store all passwords in non-reversible one-way cryptographic hash.
   6. Log all successful and failed authentication attempts, including date, time, IP address, and username.
   7. Offer a secure password reset feature, including verification of identity, email or text notification and a one-time-use password link that expires after 24 hours.
   8. Automatically de-provision accounts for terminated employees of Vendor and DOE.
   9. Temporarily lock accounts with repeated failed login attempts and provide support to affected users.
   10. Keep attributes and group structures that support authorization accurate.

10. **Confidential Information Authorization**

A. Applications that Handle Confidential Information must have explicitly defined authorization controls that prevent users from exceeding their intended privileges.

B. Applications must perform authorization checks before performing any action that creates, views, updates, transmits or deletes Confidential Information. Authorization logic must be highly configurable and alterable without code changes.

C. Authorization checks must verify the user has appropriate role to perform the requested action, and also the correct scope. Scope authorization checks should reference DOE location codes, student-teacher-class linkage, parent-student linkage and other data sources.

D. Whenever possible, authorization checks will use the DOE RBAC framework, DOE identity management system and other DOE Systems of record. Access to these Systems may be either via a web service or replicated database, at the DOE’s discretion. The Vendor Application will not be able to make any changes to the contents of these Systems.

E. Any non-DOE accounts that are managed locally by the Vendor must follow the principal of “Least Privileged Access” whereby those user accounts are provided the most restrictive access necessary to perform the required business function. “Super users” (i.e. application administrators) must be avoided unless absolutely necessary due to a legitimate administrative or educational need for such access in order to provide the Services.
11. Incident Response

A. Vendors must have a plan for compliance with all applicable breach notification laws, including New York State Education Law § 2-d and the New York State Data Breach Notification Act (General Business Law §899-aa and New York State Technology Law § 208, as appropriate).

B. The DOE must be notified in writing within 24 hours of the earliest indication or report of a potential breach or unintended disclosure of Confidential Information or a System that supports it.

C. Response actions to incidents that might affect Confidential Information or Systems must be conducted quickly and with ample resources. Vendor will hire a professional third-party incident response team if in-house resources do not have sufficient skill or availability.

D. DOE shall have the right to view all incident response evidence, reports, communications and related materials upon request.

E. If requested by the DOE, or if required by law, the Vendor shall notify in writing all persons affected by the incident, at its own cost and expense.

12. Audit & Inspection

A. The Vendor shall allow DOE, upon reasonable notice, to perform security assessments or audits of Systems that Handle or support Confidential Information. Such an assessment shall be conducted by an independent 3rd party agreed upon by the Vendor and the DOE, and at the DOE’s own expense, provided that the Vendor cooperate with any such assessment/audit and shall, at its own expense, provide all necessary support, personnel and information needed to ensure the successful completion of the assessments or audits.

B. The Vendor shall provide DOE, upon DOE’s request, with a SSAE 16 or similar report as agreed to by DOE for critical business processes relating to protection of Confidential Information and safeguards implemented in its organization.

C. Vendors must engage an independent third party annually to assess the practical security of Vendor’s Systems. These reviews must include penetration tests from the perspective of an external attacker and an internal user with common privileges. The penetration tests must include all Systems exposed to the internet and any Systems, internal or external, that Handle Confidential Information. Such annual assessment shall be at Vendor’s sole expense.

D. Audit logs must be implemented for all Systems that Handle Confidential Information. All attempted violations of System security must generate an audit log. Audit logs must be secured against unauthorized access or modification.

E. In the event of adverse findings through a DOE or Vendor audit, the Vendor shall cooperate with the DOE in remediating any risks to Confidential Information, including complying with request to temporarily taking the system offline or otherwise limiting access to the system, and any other follow up actions reasonably necessary to secure the Confidential Information.
13. Availability

A. Vendor Systems that Handle Confidential Information shall be available and fully functional 24x7x365 with 99.99% uptime, unless otherwise agreed upon in writing with the DOE. Vendor shall make plans for colocation, backups and any other Systems necessary to ensure continuity.

B. Vendor must notify and obtain agreement from the DOE for any planned interruptions in service, with the exception of emergency security updates. Vendor must notify the DOE immediately of any unintended service interruption.

14. Encryption

A. All Systems that Handle Confidential Information must encrypt the DOE data that include Confidential Information in transit using algorithms and key lengths consistent with the most recent NIST guidelines.

B. For HTTP and other protocols that use SSL/TLS, Vendor shall use the TLS 1.1 or later protocol with 128-bit or larger key size, and shall make previous protocols and smaller keys unavailable.

C. Vendor shall utilize a third party provider that is a recognized and trusted authority in the industry to generate any certificates that are used for authentication between two parties (e.g., Vendor and the DOE or Vendor and any other party).

D. Web Applications that contain Confidential Information must be available only over Transport Layer Security ("TLS"). Attempts to use the Application without encryption shall be rejected. Encrypted and non-encrypted content shall not be mixed.

E. Data at rest that is stored outside of hardened Application or database production Systems must be protected by encryption consistent with NIST recommendations.

F. The Vendor shall keep private keys confidential, implement key lifecycle management and protect all keys in storage or in transit.

G. The Vendor shall choose keys randomly from the entire key space and ensure that encryption keys allow for retrieval for administrative or forensic use.

H. Encryption of the DOE data in production databases is not required. Any database encryption system must be approved by the DOE, which approval shall not be unreasonably withheld. The DOE must be provided with a complete set of decryption keys. All DOE data must be recoverable.

I. In the event that Vendor will store DOE data outside of the United States, Vendor shall notify the DOE of the locations outside the U.S. by providing notice either in its proposal to the RFP if known by Vendor prior to award, or if known after award, to appsecurity@schools.nyc.gov; provided that the DOE reserves the right to require that the use, storage, or handling of DOE data occur within the contiguous United States or similar regional boundary as defined by the DOE, which, if applicable, shall be specified in the RFP.
15. Data retention
A. Vendors may be required to support retention of Confidential Information as per NYSED Education Data Retention Schedule ED-1.
B. Retention requirements for DOE data may be specified in the RFP. If applicable, the Vendor must acknowledge in its proposal to the RFP that it can meet the requirements and, upon request by the DOE, demonstrate that retention requirements are being implemented.
C. Record retention systems must comply with all security and privacy controls set forth in this document.

16. System Configuration & Maintenance
A. All operating Systems, servers, and network devices that support DOE Systems or Confidential Information must be kept hardened and patched.
B. All Vendor Systems that are used to host, transfer, or otherwise interact with Confidential Information must enforce strict separation from any non-DOE Systems. This can be achieved through physical and/or logical separation. The separation must be auditable and able to be proven at the request of the DOE.
C. Vendors must maintain technical best security practices configuration guidelines for all such Systems and update them at least twice per year.
D. All security-related patches must be installed on Systems within 24 hours of their release. Vendor will maintain a testing lab in order to support this.

17. Subcontractors
A. In addition to the subcontracting provisions in the agreement with the DOE (which require DOE approval of all subcontractors), in the event that a Vendor utilizes subcontractors to support a System that Handles Confidential Information (each a “subcontractor”), such subcontractors shall be subject to, and Vendor must require that each subcontractor comply with, the requirements set forth herein.
E. Data Security and Access

26. Describe data management practices to which the solution adheres, including those for patron and circulation transaction information. Include relevant information on standards compliance (such as ISO 27001) and any organizational information technology audits that have been completed.

27. Describe your plans for disaster recovery for LMS SaaS host facilities and operations and how would your LMS SaaS delivered in case of a major disaster?

28. Describe the solution’s use of and support for secure protocols to safeguard data in transit and at rest. (See Exhibit 8: Data Protection Policy with Contractors)

29. Describe the solution’s support for encryption in backups and in replica sets.

30. Describe how your solution handles data recovery or the ability to roll back in the event of human or system error. Is the recovery process a self-service mechanism or, must the vendor perform the recovery? Are there any costs associated with this service?

31. What protocols have been established for dealing with unauthorized access to or disclosure of confidential data?

32. Describe what data validation the solution performs on records as they are created or edited and indicate whether this is different for batch jobs as compared to single records.

33. Describe how the solution tracks changes to records. Is there an audit trail for edits? Is it possible to revert to previous versions of a record?

34. Describe the extent to which the solution has been designed to comply with laws and regulations governing the storage and use of “protected” user data (see Exhibit 8 section A35: Data Protection Policy with Contractors.). Examples of such laws and regulations include: Family Educational Rights Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standards (PCI-DSS), and Children's Internet Protection Act (CIPA).

35. Describe how your data storage practices and procedures adhere and or deviate to the policies outlined in Exhibit 8: Data Protection Policy with Contractors.
Exhibit 8 – Data Protection Policy with Contractors

DATA POLICY/DATA WITH CONTRACTOR

"Breach" means the acquisition, access, use, or disclosure of Protected Information that compromises the security or privacy of the Protected Information.

"Contractor" means an entity that receives or encounters Protected Information. Contractor includes, without limitation, entities that store Protected Information, or host applications that process Protected Information. The provisions of this Data Policy includes not only the entity that is a signatory to this Policy but all subcontractors, of whatever tier, of that entity; the signatory must inform and obtain the agreement of such subcontractors to the terms of this Data Policy.

"Protected Information" means all data provided by City to Contractor or encountered by Contractor in the performance of the services to the City, including, without limitation, all data sent to Contractor by City and/or stored by Contractor on its servers. Protected Information includes, but is not limited to, employment records, medical and health records, personal financial records (or other personally identifiable information), research data, and classified government information. To the extent there is any uncertainty as to whether any data constitutes Protected Information, the data in question shall be treated as Protected Information.

1. Information Security. Contractor agrees to the following:

1.1. General. Notwithstanding any other obligation of Contractor under this policy, Contractor agrees that it will not lose, alter, or delete, either intentionally or unintentionally, any Protected Information, and that it is responsible for the safekeeping of all such information, except to the extent that the City directs the Contractor in writing to do so.

1.2. Access to Data. In addition to the records to be stored / maintained by Contractor, all records that are possessed by Contractor in its service to the City of Chicago to perform a governmental function are public records of the City of Chicago pursuant to the Illinois Freedom of Information Act (FOIA), unless the records are exempt under the Act. FOIA requires that the City produce records in a very short period of time. If the Contractor receives a request from the City to produce records, the Contractor shall do so within 72 hours of the notice.

1.3. Minimum Standard for Data at Rest and Data in Motion. Contractor must, at a minimum, comply, in its treatment of Protected Information, with National Institute of Standards and Technology (NIST) Special Publication 800-53 Moderate Level Control. Notwithstanding this requirement, Contractor acknowledges that it must fully comply with each additional obligation contained in this policy. If data is
protected health information or electronic protected health information, as defined in the Health Insurance Portability and Accountability Act and Health Information Technology for Economic and Clinical Health Act (HIPAA/HITECH) and regulations implementing these Acts (see 45 CFR Parts 160 and 164), it must be secured in accordance with "Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals," available on the United States Department of Health and Human Services (HHS) website (http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html), or at Volume 74 of the Federal Register, beginning at page 42742. That guidance from the HHS states that valid encryption processes for protected health information data at rest (e.g., protected health information resting on a server), must be consistent with the NIST Special Publication 800-111, Guide for Storage Encryption Technologies for End User Devices. Valid encryption processes for protected health information data in motion (e.g., transmitted through a network) are those which comply with NIST Special Publications 800-52, Guidelines for the Selection and Use of Transport Layer Security Implementation; 800-77, Guide to IPsec VPNs; or 800-113, Guide to SSL VPNs, or others which are Federal Information Processing Standards (FIPS) 140-2 validated.

1.4. **Where Data is to be Stored.** All data must be stored only on computer systems located in the continental United States.

1.5. **Requirement to Maintain Security Program.** Contractor acknowledges that the City has implemented an information security program to protect the City's information assets, which Program is available on the City website at http://www.cityofchicago.org/city/en/depts/doit/supp_info/initiatives _informationsecurity.html ("City Program"). Contractor shall be responsible for establishing and maintaining an information security program that is designed to: (i) ensure the security and confidentiality of Protected Information; (ii) protect against any anticipated threats or hazards to the security or integrity of Protected Information; (iii) protect against unauthorized access to or use of Protected Information; (iv) ensure the proper disposal of Protected Information; and, (v) ensure that all subcontractors of Contractor, if any, comply with all of the foregoing.

1.6. **Undertaking by Contractor.** Without limiting Contractor's obligation of confidentiality as further described herein, in no case shall the safeguards of Contractor's information security program be less stringent than the information security safeguards used by the City Program.

1.7. **Right of Audit by the City of Chicago.** The City of Chicago shall have the right to review Contractor's information security program prior to the commencement of Services and from time to time during the term of this Agreement. During the performance of the Services, from time to time and without notice, the City of
Chicago, at its own expense, shall be entitled to perform, or to have performed, an on-site audit of Contractor's information security program. In lieu of an on-site audit, upon request by the City of Chicago, Contractor agrees to complete, within forty-five (45 days) of receipt, an audit questionnaire provided by the City of Chicago or the City of Chicago's designee regarding Contractor's information security program.

1.8. **Audit by Contractor.** No less than annually, Contractor shall conduct an independent third-party audit of its information security program and provide such audit findings to the City of Chicago, all at the Contractor's sole expense.

1.9. **Audit Findings.** Contractor shall implement at its sole expense any remedial actions as identified by the City as a result of the audit.

1.10. **Demonstrate Compliance - PCI.** No less than annually, as defined by the City of Chicago and where applicable, the Contractor agrees to demonstrate compliance with PCI DSS (Payment Card Industry Data Security Standard). Upon City's request, Contractor must be prepared to demonstrate compliance of any system or component used to process, store, or transmit cardholder data that is operated by the Contractor as part of its service. Similarly, upon City's request, Contractor must demonstrate the compliance of any third-party it has sub-contracted as part of the service offering. As evidence of compliance, the Contractor shall provide upon request a current attestation of compliance signed by a PCI QSA (Qualified Security Assessor).

1.11. **Demonstrate Compliance - HIPAA / HITECH.** If the Protected Information includes protected health information or electronic protected health information covered under HIPAA/HITECH, Contractor must execute, and be governed by, the provisions in its contract with the City regarding HIPAA/HITECH, the regulations implementing those Acts, and the Business Associate Agreement in its contract with the City. As specified in 1.3, protected health information must be secured in accordance with the "Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals."

1.12. **Data Confidentiality.** Contractor shall implement appropriate measures designed to ensure the confidentiality and security of Protected Information, protect against any anticipated hazards or threats to the integrity or security of such information, protect against unauthorized access or disclosure of information, and prevent any other action that could result in substantial harm to the City of Chicago or an individual identified with the data or information in Contractor's custody.

1.13. **Compliance with All Laws and Regulations.** Contractor agrees that it will comply with all laws and regulations.
1.14. **Limitation of Access.** Contractor will not knowingly permit any Contractor personnel to have access to any City of Chicago facility or any records or data of the City of Chicago if the person has been convicted of a crime in connection with (i) a dishonest act, breach of trust, or money laundering, or (ii) a felony. Contractor must, to the extent permitted by law, conduct a check of public records in all of the employee's states of residence and employment for at least the last five years in order to verify the above. Contractor shall assure that all contracts with subcontractors impose these obligations on the subcontractors and shall monitor the subcontractors' compliance with such obligations.

1.15. **Data Re-Use.** Contractor agrees that any and all data exchanged shall be used expressly and solely for the purposes enumerated in the Agreement. Data shall not be distributed, repurposed or shared across other applications, environments, or business units of Contractor. As required by Federal law, Contractor further agrees that no City of Chicago data of any kind shall be revealed, transmitted, exchanged or otherwise passed to other Contractors or interested parties except on a case-by-case basis as specifically agreed to in writing by an officer of the City of Chicago with designated data, security, or signature authority.

1.16. **Safekeeping and Security.** Contractor will be responsible for safekeeping all keys, access codes, passwords, combinations, access cards, personal identification numbers and similar security codes and identifiers issued to Contractor's employees, agents or subcontractors. Contractor agrees to require its employees to promptly report a lost or stolen access device or information to their primary business contact and to the City of Chicago Information Security Office.

1.17. **Mandatory Disclosure of Protected Information.** If Contractor is compelled by law or regulation to disclose any Protected Information, the Contractor will provide to the City of Chicago with prompt written notice so that the City of Chicago may seek an appropriate protective order or other remedy. If a remedy acceptable to the City of Chicago is not obtained by the date that the Contractor must comply with the request, the Contractor will furnish only that portion of the Protected Information that it is legally required to furnish, and the Contractor shall require any recipient of the Protected Information to exercise commercially reasonable efforts to keep the Protected Information confidential.

1.18. **Data Breach.** Contractor agrees to comply with all laws and regulations relating to data breach, including without limitation, the Illinois Personal Information Protection Act and other applicable Illinois breach disclosure laws and regulations. Data breaches of protected health information and electronic protected health information shall be governed by the provisions regarding HIPAA/HITECH, and the regulations implementing those Acts, in the Contractor's contract with the City, specifically the Business Associate Agreement in such contract. Contractor will immediately notify the City if security of any Protected Information has been
breached, and will provide information as to that breach in such detail as requested by the City. Contractor will, if requested by the City, notify any affected individuals of such breach at the sole cost of the Contractor.

1.19. **Data Sanitization and Safe Disposal.** All physical and electronic records must be retained per federal, state and local laws and regulations, including the Local Records Act. Where disposal is approved, the Contractor agrees that prior to disposal or reuse of all magnetic media (e.g. hard disk, floppy disk, removable media, etc.) which may have contained City of Chicago data shall be submitted to a data sanitization process which meets or exceeds DoD 5220.28-M 3-pass specifications. Certification of the completion of data sanitization shall be provided to the City of Chicago within 10 days of completion. Acceptance of Certification of Data Sanitization by the Information Security Office of the City of Chicago is required prior to media reuse or disposal. All other materials which contain City of Chicago data shall be physically destroyed and shredded in accordance to NIST Special Publication 800-88, Guidelines for Media Sanitization, specifications.

1.20. **End of Agreement Data Handling.** The Contractor agrees that upon termination of this Agreement it shall return all data to the City of Chicago in a useable electronic form, and erase, destroy, and render unreadable all data in its entirety in accordance to the prior stated Data Sanitization and Safe Disposal provisions. Data must be rendered in a manner that prevents its physical reconstruction through the use of commonly available file restoration utilities. Certification in writing that these actions have been completed must be provided within 30 days of the termination of this Agreement or within 7 days of a request of an agent of the City of Chicago, whichever shall come first.
Section 5: Mandatory Technical and Data Requirements

The Bidder must fully document its ability to meet the following Technical and Data Requirements to be considered for this RFP.

5.1 Mandatory Technical Requirements

The selected vendor must have the ability to:

1) Utilize a Federated Security Model and support Transport Layer Security (TLS) v1.0 and higher.
2) Enable SUNY’s campus and System Administration users to access the solution through a seamless integration via sign-on access through the solution and/or SUNY’s portal based on standard Federated Security protocols.
3) Accept and process BulkLoad files (Excel, Pipe Delimited, XML, etc.) for initial seeding of required information.
4) Generate reports in various versions of the Microsoft Product suite.
5) Access any of the offeror’s applications via any of the major commercially available web browsers (e.g. Explorer, Safari, Firefox, Mozilla, Chrome, etc.) on any basic configuration PC or Mac computer, compatible with the latest browser versions as well as backward compatible.
6) Connect to multiple, independent, SUNY environments (i.e. Training, Test and Production) with the ability to copy production information into other environments for testing purposes.

5.2 Mandatory Data Requirements

The selected vendor must have the ability to properly meet and maintain the following SUNY Data Requirements.

5.2.1 Data Security

The selected vendor must have the ability at all times to maintain network security which at a minimum, includes: network firewall provisioning, intrusion detection, and regular (one or more annually) third party vulnerability assessments, and share assessment results with SUNY. Further, the
selected vendor will maintain network security that conforms to generally recognized “Industry Standards” and best practices that the Contractor applies to its own network.

Generally recognized industry standards include, but are not limited to, the current standards and benchmarks set forth and maintained by the Center for Internet Security (see http://www.cisecurity.org) or Payment Card Industry/Data Security Standards (PCI/DSS) - see http://www.pcisecuritystandards.org/.

5.2.2 Data Privacy

1) The selected vendor will use SUNY Data only for the purpose of fulfilling its duties under the resultant agreement and will not share such data with or disclose it to any third party without the prior written consent of SUNY, except as required by the resultant agreement or as otherwise required by law.

2) The selected vendor agrees SUNY Data will not be stored outside the United States.

3) The selected vendor will provide access to SUNY Data only to its employees and subcontractors who need to access the data to fulfill Contractor’s obligations under this Agreement.

4) The selected vendor will ensure that employees who perform work under this Agreement the resultant agreement will have read, understood, and received appropriate instruction as to how to comply with the data protection provisions of the agreement.

5) FERPA: If selected vendor will have access to the SUNY’s Education records as defined under the Family Educational Rights and Privacy Act (FERPA), the vendor acknowledges that for the purposes of the resultant agreement it will be designated as a “school official” with “legitimate educational interests” in the SUNY Education records, as those terms have been defined under FERPA and its implementing regulations, and the selected vendor agrees to abide by the limitations and requirements imposed on school officials. Selected vendor will use the Education records only for the purpose of fulfilling its duties under the resultant agreement for SUNY’s and its End User’s benefit, and will not share such data with or disclose it to any third party except as provided for in the agreement, required by law, or authorized in writing by the SUNY.

6) If the selected vendor will receive, maintain, process or otherwise will have access to confidential information on employees of the SUNY campuses, it shall pursuant to the Gramm-Leach-Bliley Act (P.L. 106-102) and the Federal Trade Commission’s Safeguards Rule (16 CFR Part 314), and to the extent the vendor is a covered entity or applicable service provider under these regulations with respect to student or customer data, the Vendor will implement and maintain a written Information Security Program (“Program”) in order to protect such confidential customer information. Customer information is defined as “any record containing nonpublic personal information as defined in 16 CFR §313(n)” (the FTC’s Privacy Rule) “about a customer of a financial institution, whether in paper, electronic, or other form” (16 CFR §314.2). Examples of nonpublic personal customer information include, but are not limited to, name, address, phone number, social security number, bank and credit card account numbers and student identification numbers.

5.2.3 New York Information Breach Notification Requirements

The selected vendor will use commercially reasonable efforts to maintain the security of private information (as defined in the New York State Information Security Breach and Notification Act, as amended “ISBNA” (General Business Law § 889-aa; State Technology Law § 208) that it creates, receives, maintains or transmits on behalf of SUNY and to prevent unauthorized use and/or disclosure of that private information; and implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of electronic private information that it creates, receives, maintains or transmits on behalf of SUNY (“SUNY Data”). The selected vendor will fully disclose to SUNY pursuant to the ISBNA, and any other applicable law any
breach of the security of a system where the vendor creates, receives, maintains or transmits private information on behalf of SUNY following discovery or notification of the breach in the system as to any resident of New York State whose private information was, or is, reasonably believed to have been acquired by a person without valid authorization (“Security Incidents”). The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system. The vendor shall be liable for the costs associated with such breach if caused by the Vendor’s negligent or willful acts or omissions, or the negligent or willful acts or omissions of the Vendor’s agents, officers, employees or subcontractors. In the event of a Security Incident involving SUNY Data pursuant to the ISBNA, SUNY has an obligation to notify every individual whose private information has been or may have been compromised. In such an instance, the Vendor agrees that SUNY will determine the manner in which such notification will be provided to the individuals involved pursuant to the ISBNA and agrees to indemnify SUNY against any cost of providing any such legally required notice. Upon termination or expiration of this Agreement, the Vendor will follow SUNY’s instructions relating to any SUNY Data remaining in the Vendor’s possession. Upon authorization from SUNY, the Vendor will use data and document disposal practices that are reasonable and appropriate to prevent unauthorized access to or use of SUNY Data and will render the information so that it cannot be read or reconstructed.

5.2.4 Disaster Recovery
The selected vendor shall maintain disaster recovery services at the dedicated facility that is able to handle SUNY data center and business continuity needs in the event disaster recovery is needed. Throughout the term of the resultant agreement, the vendor shall maintain contracts or arrangements that are substantially equivalent or an improvement to those currently in effect. The vendor shall test disaster recovery capabilities, at least once every calendar year and provide SUNY with a copy of its disaster recovery plan upon request.

5.2.5 Data Portability
The selected vendor agrees to do whatever is reasonable and necessary to facilitate the orderly and professional transfer of the Services and SUNY Data upon the expiration or termination of the resultant agreement.

[deleted text not needed for the exercise]
E.4. Data Security and Data Access

E.4.1. Describe data management practices to which the solution adheres, including those for patron and circulation transaction information. Include relevant information on standards compliance (such as ISO 27001) and any organizational information technology audits that have been completed. Can data access be segmented -- for example, can institutions decide what patron information is viewable by staff at other institutions?

E.4.2. Describe the solution’s use of and support for secure protocols to safeguard data in transit.

E.4.3. Describe the solution’s support for encryption in backups and in replica sets.

E.4.4. Describe how the solution prevents loss of data, and how it provides data recovery or rollback to specific points in time in the event data loss does occur. Also describe the process through which data is recovered. For example, is the recovery process a self-service mechanism? Or, must the customer contact your organization to request data recovery? What is the typical turn-around time to have data recovered? How compartmentalized is the data with respect to data recovery? In other words, can a customer recover a subset of bibliographic records, a subset of patrons, or a particular range of transactions? Or, is system recovery or rollback only possible in its entirety?

E.4.5. What protocols have been established for dealing with unauthorized access to or disclosure of confidential data?
E.4.6. Describe what data validation the solution performs on records as they are created or edited, and indicate whether this is different for batch jobs as compared to single records.

E.4.7. Describe how the solution tracks changes to records. Is there an audit trail for edits? Is it possible to revert to previous versions of a record?

E.4.8. Describe the extent to which the solution has been designed to comply with laws and regulations governing the storage and use of “protected” user data. Examples of such laws and regulations include: Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA), and Payment Card Industry Data Security Standards (PCI-DSS).

E.5. Authentication, authorization and identity management

E.5.1. Many Alliance institutions have significantly invested in the development and management of existing identity-related data stores (e.g., Active Directory, LDAP). Describe how the solution can leverage these identity stores, both for staff and patron accounts. Describe also how such capabilities can co-exist alongside identities natively managed within the proposed solution.

E.5.2. Describe how administrative rights are assigned within the system. Can administrative rights be assigned to identities stored in external identity stores, such as Active Directory? Can administrative rights be assigned to groups, as well as users? Does the solution allow compartmentalizing of administrative rights on a per-institution basis? For example, can you limit the effect of administrative rights assignment to a single institution?

E.5.3. Because of the number of staff, the Alliance requires the ability to assign membership to groups, and then manage permissions and privileges based on group membership. Describe how your solution addresses group-based permissions. Also describe any differences in what permissions and privileges can be managed for a group vs. an individual account.

E.5.4. Describe the level of granularity of access controls for staff functions (principle of least privilege). E.g., can certain data elements be made read-only for some staff and read-write for others?

E.5.5. Some Alliance staff and patrons may have identities with multiple institutions. How would users with multiple affiliations be supported in the system, with respect to authentication, permissions assignment to their account, and permissions on their accounts?

E.5.6. Describe your support for single sign-on authentication and authorization solutions (e.g., CAS, Shibboleth, and Microsoft’s Identity and Access Management solution).
### Instructions

Vendor must complete this entire Questionnaire and include it in their Technical Proposal pursuant to Attachment 8 of the RFP.

#### Importance
Features and Functionality are categorized by Importance and include Mandatory, Highly Preferred, and Preferred and will be weighted accordingly.

#### Capability
Proposers should mark the appropriate Capability category (Off the Shelf, Configurable by Library, Configurable by Vendor, Not Provided) with an "X" for each Feature and Functionality. Any Mandatory line items indicated as "Not Provided" will result in disqualification. Questionnaires that fail to include a response for a line item will be assumed as "Not Provided."

### Capability

<table>
<thead>
<tr>
<th>Off the Shelf/Configurable by College</th>
<th>Configurable by Vendor</th>
<th>Available with Customization</th>
<th>Not Available</th>
<th>Comments/Clarifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mandatory</td>
<td>Preferred</td>
<td>Preferred</td>
<td>Preferred</td>
<td>Provided comments/clarification here if required.</td>
</tr>
<tr>
<td>Highly Preferred</td>
<td>Mandatory</td>
<td>Preferred</td>
<td>Preferred</td>
<td>Provided comments/clarification here if required.</td>
</tr>
<tr>
<td>Preferred</td>
<td>Available</td>
<td>Available</td>
<td>Available</td>
<td>Provided comments/clarification here if required.</td>
</tr>
</tbody>
</table>

#### Privacy, Security, & User Data

- Mandatory
- Highly Preferred
- Preferred

#### Interoperability

- Mandatory
- Highly Preferred
- Preferred

#### Usability & Reporting

- Mandatory
- Highly Preferred
- Preferred

#### Feature / Functionality

<table>
<thead>
<tr>
<th>#</th>
<th>Importance</th>
<th>Feature / Functionality</th>
<th>Off the Shelf/Configurable by College</th>
<th>Configurable by Vendor</th>
<th>Available with Customization</th>
<th>Not Available</th>
<th>Comments/Clarifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Mandatory</td>
<td>Seamless integration with Innovative Interfaces Sierra (library's current ILS) to access real time bibliographic records, item records, patron information, fines payment, etc.</td>
<td>Provide comments/clarification here if required.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Mandatory</td>
<td>Detailed and transparent privacy policy published on Vendor website.</td>
<td>Provide comments/clarification here if required.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Mandatory</td>
<td>Ability to assign Library Congress catalog numbers to events and blog posts so that patrons are alerted to them when they are presented to the customer.</td>
<td>Provide comments/clarification here if required.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Mandatory</td>
<td>Natural language searching (e.g. &quot;library channel movies&quot;) retrieves movies from the Library Channel, not books about movies for history.</td>
<td>Provide comments/clarification here if required.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Mandatory</td>
<td>User interface available in languages other than English, including but not limited to Spanish, Vietnamese, Chinese.</td>
<td>Provide comments/clarification here if required.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Highly Preferred</td>
<td>Tracks purchase suggestions submitted by users.</td>
<td>Provide comments/clarification here if required.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Highly Preferred</td>
<td>Allows users to save search strategies.</td>
<td>Provide comments/clarification here if required.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Highly Preferred</td>
<td>Provides option to sort by publishing date, date acquired by library, author, title, and patron rating.</td>
<td>Provide comments/clarification here if required.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Preferred</td>
<td>Includes &quot;forgot my PIN&quot; and &quot;forgot my username&quot; recovery features for users.</td>
<td>Provide comments/clarification here if required.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Preferred</td>
<td>Provides a customizable timeout setting that can vary for in-library versus home users, based on Library policy.</td>
<td>Provide comments/clarification here if required.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Preferred</td>
<td>Ability to highlight contributions by individual College staff members, giving customers the ability to maintain online relationships with specific staff members by &quot;following,&quot; messaging, etc.</td>
<td>Provide comments/clarification here if required.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>Highly Preferred</td>
<td>Provides a method for users to access, review, correct and delete their personal data.</td>
<td>Provide comments/clarification here if required.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Highly Preferred</td>
<td>Includes reading recommendations for similar titles.</td>
<td>Provide comments/clarification here if required.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>Highly Preferred</td>
<td>Ability for users to opt into providing personal information (versus opting out) and make customers aware of privacy implications when choosing to do so.</td>
<td>Provide comments/clarification here if required.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>Highly Preferred</td>
<td>Ability to manage library events that fail to include a response for a line item will be assumed as &quot;Not Provided.&quot;</td>
<td>Provide comments/clarification here if required.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>Highly Preferred</td>
<td>Includes &quot;forgot my PIN&quot; and &quot;forgot my username&quot; recovery features for users.</td>
<td>Provide comments/clarification here if required.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>Highly Preferred</td>
<td>Includes &quot;forgot my PIN&quot; and &quot;forgot my username&quot; recovery features for users.</td>
<td>Provide comments/clarification here if required.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>Highly Preferred</td>
<td>Provides a customizable timeout setting that can vary for in-library versus home users, based on Library policy.</td>
<td>Provide comments/clarification here if required.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>Highly Preferred</td>
<td>Provides a customizable timeout setting that can vary for in-library versus home users, based on Library policy.</td>
<td>Provide comments/clarification here if required.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>Highly Preferred</td>
<td>Allows users to set up customized new title alerts.</td>
<td>Provide comments/clarification here if required.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>Highly Preferred</td>
<td>Allows users to save search strategies.</td>
<td>Provide comments/clarification here if required.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>Highly Preferred</td>
<td>Offers auto-suggest when search terms are entered.</td>
<td>Provide comments/clarification here if required.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>23</td>
<td>Highly Preferred</td>
<td>Offers auto-suggest when search terms are entered.</td>
<td>Provide comments/clarification here if required.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>24</td>
<td>Highly Preferred</td>
<td>Provides option to sort by publishing date, date acquired by library, author, title, and patron rating.</td>
<td>Provide comments/clarification here if required.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>Highly Preferred</td>
<td>Provides a customizable timeout setting that can vary for in-library versus home users, based on Library policy.</td>
<td>Provide comments/clarification here if required.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>26</td>
<td>Highly Preferred</td>
<td>Provides a customizable timeout setting that can vary for in-library versus home users, based on Library policy.</td>
<td>Provide comments/clarification here if required.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>27</td>
<td>Highly Preferred</td>
<td>Provides a customizable timeout setting that can vary for in-library versus home users, based on Library policy.</td>
<td>Provide comments/clarification here if required.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>28</td>
<td>Highly Preferred</td>
<td>Provides a customizable timeout setting that can vary for in-library versus home users, based on Library policy.</td>
<td>Provide comments/clarification here if required.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>29</td>
<td>Highly Preferred</td>
<td>Provides a customizable timeout setting that can vary for in-library versus home users, based on Library policy.</td>
<td>Provide comments/clarification here if required.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>30</td>
<td>Highly Preferred</td>
<td>Provides option to sort by publishing date, date acquired by library, author, title, and patron rating.</td>
<td>Provide comments/clarification here if required.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>31</td>
<td>Highly Preferred</td>
<td>Provides option to sort by publishing date, date acquired by library, author, title, and patron rating.</td>
<td>Provide comments/clarification here if required.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
This KANOPY MASTER SUBSCRIPTION AGREEMENT is by and between Kanopy LLC, a Delaware limited liability company, with a notice address of Level 4, 781 Beach St, San Francisco, CA, 94109 (“Kanopy”) and the entity identified above (“Institution”). Kanopy and Institution hereby agree as follows:

Kanopy streams digital video content (and associated audio, graphics, text, images and other data) to universities, colleges, schools, libraries, corporations, and other institutions which use such content for viewing purposes only within their institution. Kanopy can also host and stream digital video content uploaded by such institutions where the institutions own the streaming rights for such content and this Agreement includes provisions to permit the use of this hosting service if purchased hereunder. This Agreement is intended to provide the basis for an ongoing relationship between Kanopy and Institution, establishing the terms of use for any films licensed from or hosted with Kanopy over the Term of the Agreement. The terms of any purchases that Institution may make over the course of the Term - including Products, Price, Subscription Terms, and Territorial and/or Authorized Use restrictions (if applicable) – are governed by the specific Orders made by Institution and Kanopy.

Kanopy’s online digital video content for which licenses are available for purchase are provided by Kanopy via the online platform at http://www.kanopystreaming.com/shop and/or other designated websites (“Website”). Institution may order and purchase access rights or a license to such content (such content for which access or a license has been purchased and their associated data and accompanying search and retrieval software (as updated from time to time) are the “Products”). When an order is received from the Institution (via mail, email, online purchase request, phone, fax, or otherwise) Kanopy will generate an invoice and/or order form and send it to Institution, and such invoice and/or order form is an “Order” hereunder. Institution may also order and purchase the right to upload the Institution’s digital video content to the Website for hosting by Kanopy for access and viewing by Institution and its Authorized Users (each such content defined in an Order is “Institution Content”) through Orders. Access will be given to the Products and Institution Content (as applicable) via the following URL: ecc.kanopystreaming.com (“URL”)

This Master Subscription Agreement is comprised of (in order of preference) (a) this signature page, (b) Exhibit A (General Terms and Conditions), (c) Orders, (d) the Terms of Use (available at www.kanopystreaming.com/terms, which govern Institution’s use of the Website and URL), (e) the Privacy Policy (located at www.kanopystreaming.com/privacy, which governs the registration data and other information Kanopy collects when Institution uses the Website and URL), and (f) any documents incorporated by reference into any of the foregoing; (collectively, the “Agreement”). Notwithstanding the foregoing, to the extent of any conflict or inconsistency between this Agreement and Kanopy’s Privacy Policy and Terms of Use for the Website and URL through which Institution accesses the Products and Institution Content, the terms of Kanopy’s Privacy Policy and Terms of Use shall prevail for the subject matter covered therein.

IN WITNESS WHEREOF, Kanopy and Institution have caused this Agreement to be executed by their respective, duly authorized officers or representatives, effective as of the Effective Date.

KANOPY LLC
By

Authorized Signature
Name (type or print)
Title

INSTITUTION
By

Authorized Signature
Name (type or print)
President
Title
Exhibit A General Terms and Conditions

1. Licenses; Services.
1.1 License to Institution. Subject to the terms and conditions of this Agreement, for the applicable Subscription Term, Kanopy grants to Institution a nonexclusive, nontransferable, limited license, without right of sublicense, to access and exhibit the Product(s) and Institution Content (as applicable) on a streaming-only basis via the URL and through Kanopy’s search and retrieval software (which forms part of the Product) only in the Territory to the Authorized Users for the Authorized Use and in compliance with all applicable laws in the Territory (“License”). “Authorized Users” means Institution’s currently enrolled students, employees, faculty, staff, affiliated researchers, distance learners, authorized attendees at educational classes hosted by the Institution, and visiting scholars authorized to view the Product(s) and Institution Content including by remote access through an authentication (proxy) server that guarantees access only by Authorized Users. Certain Products (e.g. Hollywood titles) may have Territory-restrictions on viewership, in which case these restrictions will be made known to the Institution at the time of purchase in the Order. “Authorized Use” means real-time viewing of a digital transmission or another Authorized Use as stated in an Order. “Subscription Term” means the term specified in the Order. “Territory” means the geographical area specified in the Order, if none is specified, the Territory is the United States.

1.2 Restrictions on Use. Kanopy reserves all rights not granted herein. Institution shall not, and shall not permit any third party to: (a) copy, store, upload or download, or otherwise reproduce the Product(s) or the software or systems supporting the Products (collectively, the “Kanopy IP”); (b) use the license to access products for which a subscription has not been purchased; or (c) decompile or reverse engineer, reverse compile, disassemble, or access the source code for, stream capture, archive, download, broadcast, transmit, retransmit, circumvent content protections of, scrape, use any data mining, data gathering or extraction method on, modify or create a derivative work of, remove, obscure, or modify copyright notices for, sell, rent, lease, loan, market, distribute, commercially exploit, transfer, assign, or sublicense, recreate, display (except as permitted), perform, post, use, replicate, frame, mirror, disclose, publish, or translate the Kanopy IP, or any component thereof.

1.3 Services. Kanopy shall use commercially reasonable efforts to stream the Products (and to host and stream the Institution Content where applicable), including scanning for viruses; to provide sufficient capacity and rate of connectivity to provide the Institution with a quality service; and to make the Products and Institution Content available with an average of 28 days of up-time per month and to perform scheduled downtime at low-usage times. Kanopy will offer reasonable levels of continuing support via email, phone or fax, during normal business hours in California, for feedback, problem-solving, or general questions. Any technical assistance that Kanopy may provide to the Institution is provided at the sole risk of the Institution.

1.4 Ownership. The Products and Kanopy IP and any other materials, processes, know-how and the like utilized by and created by Kanopy in the provision of the services are owned by or licensed to Kanopy and are subject to copyright and other intellectual property rights under United States and foreign laws and international conventions.

1.5 Indemnification. Institution shall indemnify and hold Kanopy harmless from any claims, damages, liabilities and losses (including reasonable attorney’s fees and expenses) arising out of any inaccuracy or incompleteness of information provided by Institution hereunder, breach of Institution’s representations, warranties or obligations under this agreement, or misuse or breach of any License by or via Institution.

2. Institution Content License. This Section 2 shall apply only if Institution is hosting Institution Content with Kanopy via the URL. Where Institution Orders hosting services for the Institution Content, Institution grants to Kanopy a nonexclusive, sublicensable, royalty-free, license in the Territory to upload, host, store, transmit, stream, reproduce, display and exhibit the Institution Content for Institution during the Subscription Term. Institution shall deliver the Institution Content to Kanopy in the format determined by Kanopy at Institution’s expense. Institution retains ownership rights to Institution Content. Institution represents and warrants that: (a) Institution owns or has the necessary rights and licenses (including intellectual property rights) to grant the license set forth in this Agreement; (b) Institution has procured all written consents, releases, and/or permissions to enable inclusion and use of the Institution Content in the manner contemplated herein, including the consent, release and/or permission of every identifiable individual person in the Institution Content to use the name or likeness of such identifiable individual person; (c) Institution Content shall not contain any malware, unlawful or tortious material, including material that violates privacy rights; and (d) Institution shall comply with Kanopy’s acceptable use policy (www.kanopystreaming.com/aup). Institution acknowledges that it is solely responsible for all Institution Content and its use and that Kanopy shall make no independent assessment or evaluation thereof. Institution shall indemnify and hold Kanopy harmless from any claims, damages, liabilities and losses (including reasonable attorney’s fees and expenses) relating to the Institution Content.

3. Price and Term.
3.1 Price. Institution shall pay the fees as specified on the applicable Order for the license to the Products or hosting/streaming of the Institution Content during each
Subscription Term ("Price"). The Price is quoted and payable in the currency as stated based on Products purchased, and payment obligations are non-cancelable and fees paid are not refundable. Fees and charges may change periodically and Products may cease to be available for renewal in subsequent Subscription Terms. Kanopy will use all reasonable endeavors to keep the Website up to date with changes to the content and cost of the Licenses for the Products. The Price is exclusive of all taxes, which are Institution’s responsibility. Institution is responsible for all internet/wireless access charges.

3.2 Term of Agreement. This Agreement will commence on the Effective Date and remain in effect until terminated by Kanopy or Institution in accordance with Section 3.3. Subscriptions are for the applicable Subscription Term as specified in the Orders, unless earlier terminated as set forth herein.

3.3 Termination. If either party breaches any of the terms or conditions of this Agreement and fails to cure such breach within 14 days after written notice thereof, the other party shall have the right to terminate this Agreement (including all Orders) with written notice. If all Orders are terminated or not renewed, this Agreement shall terminate. Kanopy may suspend access for late payment, or if Kanopy, in its reasonable discretion, believes the Kanopy IP is at risk. On termination of this Agreement, all amounts past due shall be due, all licenses shall end, Institution shall cease use of the Products, Kanopy shall return to Institution, or destroy, the Confidential Information, and the following terms shall survive: 1.2, 1.4, 1.5, 2 (last sentence only), 3.1, 3.3, 5, 6 and 7.

4. Warranty and Disclaimer. Kanopy warrants that it has the right to grant the License to the Products. THIS WARRANTY IS IN LIEU OF ANY AND ALL OTHER WARRANTIES HEREUNDER, WRITTEN OR ORAL, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, NONINFRINGEMENT, SATISFACTORY QUALITY, SECURITY, VIRUSES, DELAYS, AND ACCURACY, ALL OF WHICH KANOPY AND ITS LICENSORS DISCLAIM.

5. LIMITATION OF LIABILITY. In no event shall Kanopy or its licensors be liable under or as a result of this Agreement to Institution, Authorized Users or any other third party for any indirect, special, incidental, punitive, consequential or exemplary damages (including, without limitation, damages for loss of goodwill, work stoppage, computer failure or malfunction, lost or corrupted data, lost profits, loss of use, lost business or lost opportunity), or any other similar damages even if Kanopy has been informed of the possibility thereof. In no event shall Kanopy’s total, cumulative liability under or as a result of this Agreement exceed the amount of fees actually paid by Institution to Kanopy during the twelve (12) months prior to the first event giving rise to such loss, cost, claim, legal action or damages. The limitations of liability set forth in this Section 5 and exclusion of certain damages shall apply regardless of the theory of liability (contract, tort, strict liability or otherwise) or success or effectiveness of any of the exclusive remedies provided for under this Agreement.

6. Confidentiality. This Agreement and all other nonpublic information furnished hereunder by either party are the proprietary and confidential information of the disclosing party. Each party as a recipient shall hold such proprietary information in confidence (using at least a reasonable standard of care), shall not use such proprietary information except for the fulfillment of this Agreement, and may only disclose such proprietary information to those of its employees and subcontractors (and for Institution, only its Authorized Users) who have a need to know and who are bound by obligations of confidentiality similar to the terms set forth in this Section 6.

7. Miscellaneous. Kanopy will not be responsible for any delay or failure to perform resulting from any cause beyond Kanopy’s control, including any force majeure event, or any termination of a third party supplier agreement. The parties agree to use their best endeavors to resolve any disputes under this Agreement promptly. The laws of the New York govern this Agreement and, to the extent permitted by law the parties irrevocably submit to the exclusive jurisdiction of the courts of the New York. The UN Convention on Contracts for the International Sale of Goods does not apply to this Agreement. Kanopy may freely subcontract. Neither party may assign any of its rights or obligations hereunder without the prior written consent of the other party (not to be unreasonably withheld), except to its affiliate or in connection with a merger, acquisition, corporate reorganization, or sale of all or substantially all of its assets. This Agreement shall inure to the benefit of the parties, their respective successors and permitted assigns. This Agreement constitutes the entire agreement of the parties and supersedes all prior communications, understandings, and agreements whether written or oral relating to the subject matter of this Agreement. No amendment or waiver of any provision of this Agreement shall be valid or binding unless agreed to in writing by the parties. If a term or condition of this Agreement is invalid or unenforceable, the remaining terms and conditions shall remain in full force and effect and shall be enforceable to the maximum extent permitted by law. If an electronic version of this Agreement has or is agreed to by Institution’s user(s) separately, then this Agreement shall supersede such electronic version(s). In this Agreement headings are for convenience only and do not effect interpretation. Kanopy and Institution are independent contractors. Neither party will represent that it has any authority to assume or create any obligation, expressed or implied, on behalf of the other party. All notices shall be in writing and shall be delivered personally or by fax or mailed by registered or certified mail, first class, postage prepaid, to the parties hereto at their addresses specified herein, subject to the right of either party to change its address by written notice. Any communication required or permitted hereunder shall be deemed delivered upon personal delivery, and faxing (with fax confirmation sheet), or 48 hours after deposit in any official post box. In the event of any legal action or proceeding arising out of or resulting from this Agreement, the prevailing party shall be entitled to recover its reasonable attorneys’ fees, costs and expenses incurred in such action. Each party acknowledges that any breach of the license rights and restrictions herein cannot reasonably or adequately be compensated by damages in an action at law and that a breach or threatened breach of such provisions shall cause the licensor irreparable injury and damage. In addition to any other remedies a licensor may have under this Agreement or otherwise, the recipient agrees
that the licensor shall have the remedies of preliminary and permanent injunctive and other equitable relief to prevent or curtail any actual or threatened breach of the license rights and restrictions. This Agreement shall supersede any nondisclosure agreement between the parties.
1. Definitions
   a. Service: Licensor is the provider of the Docuseek2 digital service (the "Service") that permits Licensee to license and view digital content under this agreement.
   b. Educational Use: Use in markets including, but not limited to, high schools, colleges, universities, libraries, museums and non-profit organizations, and students' use for study through high schools, colleges, universities and Distance Learning Programs.
   c. Classroom Use: A performance of a program in classrooms or other related venues, for audiences of more than one person, conducted without charging admission. In this context, programs may be shown by any means which do not require digitization, transfer, alteration, duplication or reproduction.
   d. Unified Campus: The setting(s) at which any of Licensee's programs are taught, including any branch campuses, to Authorized Users.
   e. Authorized Users: Individuals affiliated with the Licensee through employment or enrollment in a degree-granting program.
   f. Distance Learning: Coursework by Authorized Users conducted via internet connection.
   g. Server Fee: An annual fee for the digital delivery ("streaming") of content licensed by the Licensee.
   h. Content: The film or video programs listed in Schedule A below and made a part hereof and any other programs added to Schedule A by the mutual consent of the parties. Docuseek2 will make a digital file of each program (the "Master") available to the Licensee.
   i. Subscription: A license to use the Content for a specific period of time defined in the invoice for the Subscription.
   j. Life of File: A license to use a file of the Content for the life of the MPEG-4 (H.264) codec.

2. Grant of License
   a. Docuseek2 grants to the Licensee a limited, non-exclusive, revocable license for the Term to use the Content for Educational Use. Any other use of this content must be licensed through special arrangement with the Licensor.
   
   b. Life of File licenses permit the right to transcode the content into the streaming format of the Licensee's choice and to load the digital files onto the Licensee’s digital network for streaming to Authorized Users. Life of File licensed Content may be duplicated for the purpose of a backup copy.
   
   c. Not permitted under this license is the right to rent, loan, sublease or sub-license content to others. Subscription Content may not be digitized, transferred, converted to another medium or format, or altered by any means without prior, written authorization of Licensor. Life of File Content may not be digitized, transferred, converted to another medium or format, or al-
tered by any means except as noted in section 2.b. above. Content may not be downloaded and stored to any workstation or other device.

d. For Life of File licenses, in the event the Licensee decides to switch the codec of its Master, then this agreement must be renegotiated before the Content is re-encoded or new transcodes made and streaming of the Content resumed.

e. Films licensed for institutional use may only be shared within the Unified Campus; with Distance Learning classes; with Authorized Users; or with non-affiliated library patrons ("walk-ins") legitimately accessing the content from the Licensee's network.

f. Institutional streaming licenses permit classroom use. Institutional streaming permits screening on the Unified Campus to a group only when no admission is charged and there is no advertising outside the learning community.

g. Sharing of streamed Docuseek2 content with other institutions, or with individuals, classes or groups who are not Authorized Users, except as noted above, is not permitted without the express authorization of Docuseek2.

h. This license is granted only upon payment of fees specified by or through Docuseek2.

i. At the commencement of this license, the Licensor will provide access to the Content.

j. For Subscription licenses, Licensor will provide streaming access to the content for the term of the subscription. For Life of File licenses, Licensor will provide streaming services for the Content to the Licensee, renewable on an annual basis, for a Server Fee as specified in Schedule B below.

3. Copyright

a. All materials licensed from Licensor including, but not limited to, the Content, and other video, audio, graphics, text, images, and interactive media are the property of the Licensor or have been licensed to the Licensor and are protected by international copyright and trademark laws. Licensee has no ownership of the Content.

b. In addition, the contents of docuseek2.com, including but not limited to design, "look and feel," software code, text, images, audio, and Content, are copyrighted, with all rights reserved by Docuseek, LLC ©2016.

4. Term

The term of this License Agreement shall be for the period defined in the Subscription invoice, or, in the case of Life of File licenses, for the Life of File as defined above. Upon expiration, non-renewal, or any termination of the license, all Licensee's rights to use the Content shall cease.

5. User Account and Security

a. Account and Password. As a registered user of the Service, Licensee may receive or establish an administration account ("Account"). Licensee is solely responsible for maintaining the confidentiality and security of the Account. Licensee should not reveal Account information to anyone else or use anyone else's Account. Licensee is entirely responsible for all activities that occur on or through the Account, and Licensee agrees to immediately notify Docuseek2 of any unauthorized use of the Account or any other breach of security.
Docuseek2 shall not be responsible for any losses arising out of the unauthorized use of Licensee's Account.

b. Security. Licensee understands that the Service, and products purchased through the Service, include a security framework using technology that protects digital information and limits Licensee's usage of the Content to certain usage rules established by Docuseek2 and its licensors. Licensee agrees not to violate or attempt to violate any security components. Licensee agrees not to attempt to, or assist another person to, circumvent, reverse-engineer, decompile, disassemble, or otherwise tamper with any of the security components for any reason whatsoever. Licensee shall not access or attempt to access an Account that Licensee is not authorized to access. Licensee will not attempt to, or encourage or assist any other person to make use of Licensee's user name and password to stream a film Licensee has licensed. Violations of system or network security may result in civil or criminal liability.

6. Objectionable Material
Licensee understands that by using the Service, it may encounter content that may be deemed offensive, indecent, or objectionable, which content may or may not be identified as having explicit language. Nevertheless, Licensee agrees to use the Service at its sole risk and that Docuseek2 shall have no liability to Licensee for content that may be found to be offensive, indecent, or objectionable. Content types and descriptions are provided for convenience, and Licensee acknowledges and agrees that Docuseek2 does not guarantee their accuracy.

7. Representations and Warranties of the Licensor
All information, products and other content (including third party information, products and content) included in or accessible from Docuseek2 Content are provided "as is" and without warranties of any kind (express, implied and statutory, including but not limited to the warranties of title and noninfringement and the implied warranties of merchantability and fitness for a particular purpose), all of which Docuseek2 disclaims to the fullest extent permitted by law. Licensee's use of the Content is at licensee's sole risk.

8. Representations and Warranties of the Licensee
Licensee warrants that all information provided is true and accurate. Docuseek2 may terminate Licensee's rights to any or all service if any information Licensee provides is false or inaccurate.

9. Docuseek2's Privacy Policy
Except as otherwise expressly provided for in this Agreement, our Service is subject to Docuseek2's Privacy Policy, which is expressly made a part of this Agreement as Appendix A.

10. Governing Law
These Terms of Use are governed by the laws of the United States and, where no other state law is applicable, the State of Pennsylvania, without giving effect to any principles of conflicts of laws. However, with respect to a State or Public institution Licensee that is restricted by laws governing contracts solely to those of its applicable state, Licensor will agree that these Terms of Use be governed by the laws of such states.
11. Trademarks

Docuseek2 and its logo belong to Docuseek2 and other marks belong to third party trademark owners. Except as permitted by applicable laws, Licensee is prohibited from using any of the marks appearing on this site without express written consent from their respective trademark owners.

12. Miscellaneous

a. Licensor reserves the right to refuse service and terminate accounts at its sole discretion, with or without cause, including, but not limited to, if Licensor believes Licensee's conduct violates applicable law or is harmful to Licensor. Notification will precede any suspension of access, and a reasonable amount of cure time will be granted to Licensee to resolve any perceived breach, prior to termination.

b. Licensor's rights, including but not limited to all rights of remedy for Licensee's breaches under this Agreement, shall continue in perpetuity.

c. Licensor reserves the right to change, modify, add, or remove portions of the Service at any time. Licensor may add, delete, or modify features, titles, as well as the scope of service and support provided. Pricing, product features and specifications, and product title library are all subject to change without notice. Any variations to this License are only valid if they are recorded in writing and signed by both parties.

d. No delay or failure of Licensor to take action under these Terms and Conditions will constitute a waiver by Licensor, unless expressly waived in writing by Licensor.

e. These Terms of Use constitute the complete agreement of the parties and contain the entire understanding of the parties hereto relating to the Content, supersede any prior written or oral agreement or understandings between the parties with respect to the Content, and cannot be changed or terminated orally. Only a writing specifically referencing these Terms of Use and signed by the parties hereto may amend them.

Docuseek2's TERMS OF SALE

LICENSE PERIOD

User license period commences at the time the license is purchased.

SALES TO END USERS ONLY

Docuseek2 does not provide products for resale.

REFUND POLICY

All sales are final.

PAYMENT METHODS

Docuseek2 accepts credit cards as forms of payment. Docuseek2 accepts Visa and MasterCard for orders under $1000. For institutional licenses, we accept Purchase Orders, but at our discretion. Licenses may not be activated until payment is made. PLEASE NOTE: If a purchase has been declined online due to credit card issues, please ensure all data is correct and resubmit. If the transaction is not accepted online, Licensee will be unable to use that card for Licensee's purchase and should use another credit card.

BILLING

Each individual transaction authorizes and bills as a single purchase.

UPGRADES
Docuseek2 reserves the right to enhance Products purchased from Docuseek2, including Products purchased but not yet accessed. If an enhancement inadvertently alters the length of a purchased license, the purchaser may contact us for a reinstatement of that license to its original length, or for an acceptable substitute.

FOR ASSISTANCE WITH ORDERS - DOCUSEEK2 CUSTOMER SERVICE

For assistance with billing questions or other order inquiries, please refer to our online Contact Us page. We will respond as soon as possible, usually within one business day.

CONTENT USAGE RULES

Licensee's purchase or use of any Products from Docuseek2 signifies Licensee's complete agreement to these Terms of Use.

OTHER TERMS AND CONDITIONS

Docuseek2 is not responsible for misunderstandings resulting from typographic errors.

I have read, and on behalf of my institution, I accept the above Terms of Use.

_________________________________ _________________________________
Name (print) Name (print)

_________________________________ _________________________________
Signature Signature

_________________________________ _________________________________
Date Date
Appendix A - Privacy Policy

We take privacy very seriously. While we do log information on visits, queries and other site activity, this information is for evaluating the effectiveness and usefulness Docuseek2 only. All specific visit information is treated confidentially and anonymously, and is never shared with any other party, including the participating distributors. Aggregated data is shared with distributors. We do use cookies to record login state and other state information. The cookies serve no other purpose than this. If you have any questions concerning your privacy and your activity on Docuseek2, please contact us.

Institution admins and users

Docuseek2 supports two kinds of registered users. Administrators can see who else at their university has registered with Docuseek2. Administrators also have the ability to control the access of users from the institution to certain features on Docuseek2 related to licensing and viewing content. See the User Administration page for details on what rights institution administrators can grant or revoke. Administrators cannot see what a registered user has previewed, or what searches that user has done. Administrators may receive copies of emails when content is licensed by a registered user, or when a registered user asks that a title be made for streaming. These features exist to assist institutional media librarians in managing the institution's collections and helping their colleagues find and use media. The admin versus user access rights is a feature of the institutional licensing site only.

Shopping privacy and security

You can shop at Docuseek2 with confidence. We have partnered with Stripe, a leading payment processor, to accept credit card payments safely and securely. Stripe is certified as a PCI Level 1 Service Provider, the most stringent level of certification available.
This Agreement establishes the general terms and conditions for the provision of Products and Services. Additional Product or Service-specific terms and conditions are set forth in one or more schedules ("Schedules"), and are made a part of this MSA. In case of a conflict in terms between the MSA and any applicable Schedule, the terms and conditions of the Schedule shall prevail. If Institution orders additional Products or Services after its initial order and such order includes a master services agreement with the Schedule, this initial, executed MSA controls in lieu of such attached master services agreement.

Section 2  Scope & Construction

Section 3  Definitions

3.1 Bibliographic Data means all the bibliographic data (including subject data, such as local key words and subject headings), descriptive metadata, relationship metadata and other metadata of the type stored in WorldCat.

3.2 Holdings Data means all the ownership and license data in relation to Institution’s collection (including electronic resources).

3.3 Hosted Services means the hosted services made available by OCLC which Institution may access pursuant to this Agreement. The Hosted Services are described in detail in the applicable Product Descriptions but do not include services (including API’s and the like) provided by third parties.

3.4 Institution Data means (i) the Holdings Data in relation to Institution’s collection; (ii) all the data that forms part of the library process or the internal operations of the Institution, such as circulation, patron, and acquisition data; and (iii) all other data and content that is produced, sent or reproduced through the Services by the Institution or made available to OCLC in connection with the Services.

3.5 Internal Data means Institution Data intended exclusively for internal use by the Institution.

3.6 Product Descriptions means the descriptions of the Products and Hosted Services as made available at www.oclc.org and as updated from time to time by OCLC.

3.7 Products mean the OCLC software, hardware, and other products licensed to Institution pursuant to this Agreement. The Products are described in detail in the applicable Product Descriptions but do not include products provided by third parties.

3.8 Professional Services means the services that OCLC provides to Institution under this Agreement in connection with the Products or Hosted Services, such as data migration, configuration, consultancy, support, and training.

3.9 Services mean the Hosted Services and Professional Services.

3.10 Shared Data means the Institution Data made available by Institution to the public or to third parties selected by the Institution (such as other participants or users) or that by its nature is intended for use outside the Institution’s organization, such as Bibliographic Data, Holdings Data, and other data not considered Internal Data.

3.11 Systems mean the facilities, server(s), equipment, operating software, and connectivity used to provide the Services.

3.12 WorldCat means the databases of Bibliographic Data, Holdings Data, and related files maintained by OCLC.

Section 4  Products and Services

4.1 General. OCLC will provide Institution those Products and Services to which it subscribes, in accordance with this Agreement and as described in the version of each Product or Service’s respective Product Description active on the Effective Date. Product Descriptions and brochures can be found at https://www.oclc.org/en/services.html. Institution shall provide OCLC with the assistance and information OCLC reasonably needs to perform the Services properly or where OCLC otherwise reasonably requests. OCLC shall not be liable for any failure to perform its obligations arising from Institution’s failure to provide such assistance or information.

4.2 License. Subject to the terms of this Agreement and the applicable Schedule(s), Institution’s license to use the Products and Services identified in the executed Schedules may be pursuant to a hosted license (for Hosted Services) or a non-hosted license (for Products). For Products paid for by Institution, OCLC grants Institution a nonexclusive, nontransferable license to install and use the Product solely for the noncommercial purposes described in the Product Description and the applicable Schedule. For Hosted Services subscribed to by Institution, OCLC will provide access to the Hosted Service, and if applicable a license to install and use any local software components of the Hosted Service, all solely for the noncommercial purposes described in the Product Description and the applicable Schedule.

4.3 Modifications. OCLC may change or modify a Product or Service from time to time in its discretion. OCLC shall notify Institution should there be any material changes to the respective Product or Service by such means as reasonably determined by OCLC. Any new Product or Service functionality made available by OCLC shall be subject to this Agreement.

4.4 Support. Support services will be provided in accordance with the support service description available at http://www.oclc.org/support/home_en.html. Generally email support is available at support@oclc.org and telephone support is available at 1-800-848-5800.

4.5 OCLC Intellectual Property. OCLC and/or its licensors or suppliers are the exclusive owners of and retain all right, title, and interest (including all copyrights, trademarks, patents, and any other proprietary rights) to the Products, Services, WorldCat, and all other materials produced or provided by OCLC. All rights not expressly granted by OCLC are reserved.

4.6 Limitations. Institution shall only use the Products and Services in accordance with the terms of this Agreement and for the purposes specified in the Product Descriptions.
Section 5  Term and Termination

5.1 Term. This Agreement shall commence on the Effective Date and shall remain in full force and effect until all active Schedules are terminated in accordance with Section 5.2. Unless otherwise specified in a pricing document, individual Schedules shall commence upon execution and shall remain in full force and effect for the duration that Institution has access to the applicable Products or Services.

5.2 Termination. This Agreement or individual Schedules may be terminated in one of the following ways:

a) By either party, effective at the end of the initial subscription period or any renewal period, by providing the other party with at least 30 days prior written notice of its desire to not renew a Product or Service;

b) By either party if the other party becomes insolvent, makes a general assignment for the benefit of creditors, suffers or permits the appointment of a receiver for all or a substantial part of its property, is subject to any proceeding under any bankruptcy or insolvency law, or has wound up or liquidated, voluntarily or otherwise;

c) By the non-breaching party if a party commits a material breach of its obligations under this Agreement and has not cured such breach or failure within 30 days of receiving written notice from the non-breaching party. OCLC reserves the right, however, to immediately suspend Institution’s access to the OCLC Services in the event of Institution’s material breach until such time as the material breach is cured; or

d) As otherwise explicitly provided in this Agreement.

5.3 Effect of Termination. Termination of this Agreement shall terminate all Schedules, termination of a Schedule will not terminate the Agreement or any other Schedule. Upon termination of this Agreement or any Schedule, the rights granted by OCLC in the applicable Schedule or Agreement are terminated unless otherwise provided in such Schedule. After termination and upon request, OCLC will promptly return or destroy all applicable Institution Data, except however, OCLC may retain Institution Data in back-up files provided that the confidentiality and security obligations contained herein shall apply. OCLC will provide Institution access to Institution Data for 90 days after the effective date of termination, after which, OCLC shall have no obligation to maintain any Institution Data.

Section 6  Fees and Payment Terms

6.1 Fees. Institution shall pay the applicable charges based on their agreed upon pricing document or, in the absence of an agreed upon pricing document, OCLC’s prevailing price for the Products and Services. Fees are exclusive of any taxes and shall be paid in the currency and to the address stated on the invoice. Institution shall pay such tax to OCLC or other entity, as appropriate. Institutions exempt from taxation shall supply a valid exemption certificate upon request. Institution’s failure to fully pay any fees or taxes within 60 days after the applicable due date will be deemed a material breach of this Agreement, justifying OCLC’s suspension of Products and Services.

6.2 Price Changes. OCLC reserves the right to change any price/fee, provided that OCLC provides Institution written notice of the change at least 60 days prior to the date the change is to become effective. Notwithstanding the foregoing, OCLC will not change any prices/fees contained in an agreed to price quote or renewal notice prior to the expiration of the quote or renewal notice.

6.3 Non-refundable. Institution will not be entitled to a refund of any implementation or pre-paid fees under this Agreement unless (i) OCLC terminates the Agreement or a Schedule pursuant to Section 5.2 (a), or (ii) Institution terminates the Agreement or a Schedule pursuant to Section 5.2 (c); in which event, OCLC will refund that portion of fees pre-paid by Institution corresponding to the period after termination.

Section 7  Disclaimer

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, THE PRODUCTS AND SERVICES ARE PROVIDED “AS IS” AND OCLC AND ITS THIRD PARTY SUPPLIERS DO NOT MAKE ANY REPRESENTATIONS OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, WITH RESPECT TO THE PERFORMANCE OF THE PRODUCTS OR SERVICES, INCLUDING, BUT NOT LIMITED TO, ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT OR ANY IMPLIED WARRANTY ARISING BY USAGE OF TRADE, COURSE OF DEALING OR COURSE OF PERFORMANCE. OCLC MAKES NO REPRESENTATIONS OR WARRANTIES THAT THE PRODUCTS AND SERVICES WILL ALWAYS BE ACCESSIBLE, FREE OF HARMFUL COMPONENTS, ACCURATE OR ERROR-FREE. IN NO EVENT WILL OCLC BE LIABLE FOR ANY LOSS ARISING OUT OF FAILURE OF THIRD PARTY PRODUCTS OR SERVICES OR OTHER EVENTS OUTSIDE OF OCLC’S REASONABLE CONTROL. THIS SECTION WILL NOT APPLY TO DAMAGES THAT CANNOT BE EXCLUDED BY LAW (IN WHICH EVENT THE LIABILITY SHALL BE LIMITED TO THE FULLEST EXTENT PERMITTED).

Section 8  Privacy and Security

8.1 Data Security. OCLC has implemented and shall maintain commercially appropriate, reasonable and customary controls to ensure the security, confidentiality, and protection against unauthorized access to, use, or disclosure of Internal Data. Institution shall obtain and maintain all necessary consents from all users for OCLC to provide the Service and for Institution’s and users’ access, monitoring, use, disclosure, and transfer of Internal Data.

8.2 Audit. OCLC will (i) implement administrative, physical, and technical safeguards in accordance with accepted industry practices including conducting audits in accordance with the ISO/IEC 27001 standard (or subsequent comparable standard) and (ii) as reasonably requested by Institution, provide Institution with a copy of the certificate of registration for such standard along with any relevant reported deficiencies regarding non-compliance together with corrective action plans for addressing such deficiencies identified in the report.
8.3 Nondisclosure of Internal Data. OCLC shall hold all Internal Data in strict confidence and with the same standard of care it uses to protect its own information of a similar nature and shall not use Internal Data for any purpose other than to provide the Service or as may be authorized in writing by Institution. OCLC shall not disclose Internal Data to any other party except: (a) to OCLC employees, agents, subcontractors and service providers, to whom Internal Data needs to be disclosed for the purpose of providing the Service; (b) as required by law, or to respond to duly authorized information requests of police and governmental authorities or to comply with any facially valid subpoena or court order; (c) to protect the rights or property of OCLC or OCLC customers, including the enforcement of OCLC agreements or policies governing Institution’s use of the Service; (d) to involve and cooperate with law enforcement or the appropriate legal authorities in investigations, and to protect Systems and OCLC’s customers, or (e) as authorized by Institution in writing.

8.4 Prohibitions. Institution expressly warrants that it will not enter, submit, transfer, or store in the Service any of the following types of information: Social Security Numbers (or other national identification numbers), financial account numbers, credit card or debit card numbers. OCLC will have no liability, and Institution expressly releases OCLC from any liability, associated with the loss, theft, disclosure or misuse of such information.

8.5 Data Transfer. As part of providing Services, OCLC may store and process Institution Data in the United States or any other country in which OCLC or its affiliates, subsidiaries, or agents maintain facilities. By using the Service, Institution consents to this transfer, processing, and storage of Institution Data to or by OCLC, its service providers, and affiliates subsidiaries or agents, over state and international borders as necessary to provide the Service in accordance with OCLC’s standard business practices.

8.6 Unauthorized Disclosures. OCLC will promptly notify Institution in the event of a verified breach of non-public personal data unless such breach is unlikely to result in material harm to Institution or the data subject, or as otherwise provided by law. Institution agrees that it shall be Institution’s sole responsibility to determine whether a breach is subject to state, federal or national breach notification laws and requires breach notification (“Breach Notification”). In the event that Institution determines that a breach requires Breach Notification, OCLC agrees that it will reasonably cooperate with Institution in regards to Institution’s Breach Notification obligations as specified in the applicable law, including Institution’s investigation, enforcement, monitoring, document preparation, Breach Notification requirements, and reporting. Institution shall be solely responsible for notifying all individuals subject to Breach Notification, however OCLC reserves the right to first review all notifications before they are sent.

Section 9 Limitation of Liability

OCLC will have no liability for any indirect, consequential, exemplary, special, incidental, or punitive damages for any matter arising from or relating to this Agreement or the Products and Services, including but not limited to any unauthorized access to, or alteration, theft, loss, inaccuracy, or destruction of information or data collected, stored, distributed, or made available via the Products and Services, Institution’s use or inability to use the Products and Services, any changes to or inaccessibility of the Products and Services, any delay or failure of the Services, or for lost profits, or costs of procurement of substitute goods or services, even if OCLC has been advised of the possibility of such damages. In any event, OCLC’s liability to Institution for any reason and upon any cause of action will be limited to the amount Institution actually paid OCLC for the individual implicated OCLC Products or Services covered under this Agreement over the 12 months prior to which such claim arose. This limitation applies to all causes of action in the aggregate, including, but not limited to, breach of contract, breach of warranty, negligence, strict liability, misrepresentations, and other torts. Fees under this Agreement are based upon this allocation of risk. This Section will not apply to damages that cannot be limited or excluded by law (in which event the liability shall be limited to the fullest extent permitted).

Section 10 Use of Products and Services

10.1 Institution Data

a) Ownership. Institution, and/or its suppliers and affiliates, retains all right, title and interest (including, without limitation, all proprietary rights) to Institution Data, except for rights granted to OCLC and its affiliates under this Agreement. Institution is solely responsible for the accuracy, completeness, and legality of Institution Data. Institution is responsible for obtaining all permission and other rights necessary to provide Institution Data to OCLC. Institution will not provide OCLC with Institution Data that Institution does not have the right to provide for use in connection with the Products or Services.

b) License Rights. Institution grants OCLC a global, non-exclusive, royalty-free, transferable and sub-licensable right to use the Internal Data to the extent necessary for the provision of the Products and Services. Institution grants OCLC, OCLC participants, non-participant users, and OCLC designees a global, perpetual, non-exclusive, royalty-free, transferable, and sub-licensable right to host, reproduce, transmit, store, publish, distribute, modify, create derivative works from, and otherwise use Shared Data. Institution Data shall be supplied to OCLC in a format compatible for use with the Products and Services.
10.2 Confidentiality. Institution agrees to maintain the confidentiality of OCLC’s pricing information for 3 years from receipt by Institution. It shall not be a violation of this section to disclose information as required by applicable law (including public records acts), valid court order, or legal process.

10.3 Acceptable Use Policy (“AUP”)

a) General. Institution agrees not to use, and not to allow third parties including users to use the Products or Services: (a) to distribute viruses, worms, Trojan horses, corrupted files, or other items of a destructive or deceptive nature; (b) to engage in or promote any unlawful, invasive, infringing, defamatory, or fraudulent activity; (c) to violate, or encourage the violation of, the legal rights of others; (d) to interfere with the use of a Product or Service, or the equipment used to provide Products or Services; (e) to use the Products or Services, or any part thereof, in a manner that violates the terms of service of any other Products or Services; (f) to generate, distribute, publish or facilitate unsolicited mass email, promotions, advertisings or other solicitations (“spam”); (g) to alter, reverse-engineer, interfere with, circumvent, copy, or create a derivative work of any aspect of the Product or Service (except with the express, written consent of OCLC or applicable law specifically prohibits this restriction); (h) to omit, obscure or hide from any user any notice of a limitation of warranty, disclaimer, copyright, patent, trademark, trade secret or usage limitation or any splash screen or any other terms or conditions intended to be displayed to a user by OCLC or OCLC supplier; or (i) to post, send, or make available software or technical information in violation of applicable export controls laws. Institution agrees that OCLC is authorized to monitor communications into and out of the System to prevent the introduction of viruses or other hostile code, to prevent intrusions, provide support, and to otherwise enforce the terms of this Agreement. Institution agrees to reimburse OCLC for all reasonable and verifiable costs associated with OCLC’s compliance with governmental requests relating to Institution or Institution Data, including, but not limited to, warrants, subpoenas, and judicial orders. Notwithstanding the foregoing and to the extent permitted by law and law enforcement, OCLC will make reasonable efforts to notify Institution when a disclosure of Institution Data has or is to be made.

b) Credentials. Institution shall exercise all commercially reasonable efforts to prevent unauthorized use of the Products and Services and is solely responsible for any and all use, including unauthorized use, of the Products and Services initiated using Institution’s credentials. Institution shall immediately notify OCLC of a suspected or actual loss, theft or disclosure of any credentials and of any unauthorized use of a Product or Service. Should OCLC become aware of unauthorized use of Institution’s credentials or unauthorized access to a Product or Service, OCLC may notify Institution and deauthenticate affected credentials. OCLC will provide Institution with administrative credentials to access and use the applicable Product or Service. Institution is responsible for authorizing user access to the Products or Services, assigning privileges, and creating, maintaining, and terminating accounts.

c) Enforcement by OCLC. OCLC reserves the right to: (i) investigate any violation of this AUP or misuse of Products or Services; (ii) enforce this AUP; and (iii) remove or disable access, screen, or edit any Institution Data that violates these provisions. Without limitation, OCLC also reserves the right to report any activity (including the disclosure of appropriate Institution Data) that it suspects violates any law or regulation to appropriate law enforcement, regulators, or other appropriate third parties. OCLC may cooperate with appropriate law enforcement by providing network and systems information related to allegedly illegal or harmful content. VIOLATION OF THIS AUP MAY RESULT IN THE SUSPENSION OF OCLC SERVICES AND SUCH OTHER ACTION AS OCLC REASONABLY DEEMS APPROPRIATE. REPEATED OR WILLFUL VIOLATION OF THIS AUP MAY, IN OCLC’S SOLE DISCRETION RESULT IN THE TERMINATION OF THE AGREEMENT, ANY SCHEDULE, OR OCLC SERVICE.

Section 11 Warranties

OCLC warrants that any Professional Services will be performed in a professional and workman-like manner and that, when operated in accordance with the Product Description, the Products and Hosted Services will be capable of performing substantially in accordance with the functional specifications set forth in such Product Description. If any Products or Services fail to comply with the warranty set forth above, OCLC will make reasonable efforts to correct the noncompliance provided that OCLC is given notice of the noncompliance within 30 days and OCLC is able to reproduce the noncompliance. If OCLC is unable to correct the noncompliance, Institution may terminate the Schedule for the relevant Product or Hosted Service in accordance with Section 5.2(c) and, as its sole remedy, will be entitled to a refund of an equitable portion of fees paid for the relevant Product or Hosted Service after such noncompliance was reported. OCLC and Institution each warrant that its entry into this Agreement does not violate any other agreement to which it is a party, and that its performance under this Agreement will be in conformance with all applicable laws and government rules and regulations. Institution warrants that it possesses all rights necessary to enter into this Agreement and grants the rights described in this Agreement such that OCLC will not infringe upon or otherwise violate any intellectual property rights or other rights of a third party or violate any laws by exercising the rights and licenses granted under this Agreement. To the extent permitted by law, Institution hereby indemnifies OCLC from any such claims in this respect.

Section 12 General

12.1 OCLC Membership. As a subscriber to OCLC’s Services and Products as described in this Agreement, Institution – and each library owned or operated by Institution – may be eligible for membership in the OCLC cooperative. Membership qualifications for the OCLC cooperative can be found at http://www.oclc.org/content/dam/oclc/membership/Membership-Criteria-EY15.pdf. If Institution’s subscription qualifies it as a member, Institution permits OCLC Member Relations to contact its library staff directly in separate communications, to provide new member information regarding voting and updates, Member groups, councils, and events, for OCLC Global and Regional Councils specific to Institution’s region. As a member, Institution agrees to abide by the requirements and policies applicable to OCLC members.
12.2 No Assignment. Institution may not assign, without the prior written consent of OCLC, any rights, duties, or obligations under this Agreement to any person or entity, in whole or in part.

12.3 Independent Contractors. The relationship of the parties is that of independent contractors, and no agency, employment, partnership, joint venture, or any other relationship is created by this Agreement.

12.4 Force Majeure. Neither party shall be responsible for losses or damages to the other occasioned by delays in the performance or the non-performance of any of said party's obligations (other than the obligation to make payments when due) when caused by acts of God, acts of the other party or any other cause beyond the control of said party and without its fault or negligence.

12.5 Non-Waiver. A failure or delay in enforcing an obligation under this Agreement does not prevent enforcement of the provision at a later date. A waiver of a breach of one obligation does not amount to a waiver of any other obligation, and it will not prevent a party from subsequently requiring compliance with that obligation.

12.6 Severability. If any provisions of this Agreement shall be found by any court of competent jurisdiction to be invalid or unenforceable, the invalidity or unenforceability of such provision shall not affect the other provisions of this Agreement.

12.7 Entire Agreement. This Agreement and any Schedules constitute the complete agreement between the parties and supersedes and replaces all prior agreements, oral and written, between the parties relating to the subject matter of this Agreement. If Institution's accounting representatives require the use of a purchase order to facilitate payment for Products and Services contemplated in this Agreement, Institution agrees any and all terms and conditions contained in such purchase order are null and void, and do not apply to this Agreement. OCLC will provide invoices in response to purchase orders solely to facilitate payment and for the convenience of Institution; in no case, however, will OCLC's issuance of an invoice constitute an acceptance of terms contained in a purchase order. OCLC provides Services and Products to Institution solely pursuant to this Agreement; OCLC shall never provide Services or Products pursuant to, or as a result of, a purchase order. Except as otherwise provided herein, this Agreement may not be amended or supplemented except in a writing duly executed by both parties.

12.8 Notice. Except as stated elsewhere in the Agreement all notices shall be in writing and shall be deemed sufficient if (a) received by a party via e-mail to the e-mail address for such party set forth in Section 1, (b) delivered by hand, or (c) sent by certified or registered mail, return receipt requested, to the address for such party set forth in Section 1, or to such other address as has been furnished by means of a notice given in accordance with this Section.

Notices Address for OCLC:
OCLC
6565 Kilgour Place
Dublin, Ohio 43017-3395
FAX: 614-764-0740
Attention: Legal Department
E-mail: legal@oclc.org

12.9 Counterparts. This Agreement may be executed in counterparts and/or via facsimile transmission or electronic copy, any one or form of which will be deemed to constitute an original, but all of which will constitute one instrument.

Section 13 Special Terms for Group Orders Only
Where a lead institution in a consortium (the "Group Administrator") is ordering on behalf of itself and other consortium members, Section 13 applies:

13.1 Ordering. Group Administrator may order the Service on behalf of consortium members by completing the relevant portions of the agreed upon pricing or order document and agreeing to this Agreement. Group Administrator also orders and allocates authorizations and passwords for the Service on behalf of consortium members listed on the agreed upon pricing or order document. Group Administrator is not a buyer of the Service for resale. Any material change in group membership or group participation may result in commensurate changes in the fees for the applicable Service.

13.2 Consortium Member's Agreement. Group Administrator warrants, as the consortium agent, that it is authorized to and hereby binds consortium members to this Agreement and shall indemnify OCLC from all loss, expense and damage arising from a breach of such warranty. Group Administrator shall provide each consortium member with a copy of this Agreement prior to Product and Service activation. Each order for consortium members shall constitute a binding contract between OCLC and the consortium member.

13.3 Payment by Group Administrator. Group Administrator shall be liable for paying to OCLC all charges and applicable taxes for consortium members for the Products and Services in accordance with the terms of this Agreement.

13.4 Non-exclusivity. Nothing herein shall limit OCLC's right to distribute any Products or Services independent of Group Administrator.
OrangeBoy Services and Software Subscription Agreement SAMPLE

ORANGEBOY SERVICES AND SOFTWARE SUBSCRIPTION AGREEMENT

This ORANGEBOY SERVICES AND SOFTWARE SUBSCRIPTION AGREEMENT ("Agreement") is made and entered on <DATE> by and between OrangeBoy, Inc., an Ohio corporation, whose address is 1042 Ridge Street, Columbus, Ohio 43215 ("OrangeBoy"), and <ENTITY>, a <STATE> corporation, whose address is <ADDRESS> ("Client").

WHEREAS, OrangeBoy produces a hosted software-as-a-service application (SaaS) that is designed to analyze a library’s operations data and provide knowledge and customer insights based on that data, to improve the library’s customer experience and decision-making process;

WHEREAS, OrangeBoy also offers services related to this hosted SaaS application, including training, data handling, and data analysis;

WHEREAS, Client desires to obtain access to OrangeBoy’s hosted SaaS application and to use some or all of OrangeBoy’s related services to help Client analyze, interpret, and apply its own operations data as set forth herein; and

WHEREAS, OrangeBoy and Client desire to memorialize the terms of their agreement pursuant to the terms and conditions set forth herein.

NOW, THEREFORE, in consideration of the mutual covenants by and between the parties hereto and other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the parties, intending to be bound hereby, agree, in writing, as follows:

1. **OrangeBoy’s Obligations.** OrangeBoy agrees to provide Client access to its hosted software-as-a-service application SAVANNAH ("Savannah") and will offer certain services regarding Savannah. The scope of this access, the Savannah features and data analyses that Client will have access to, and the services that Client will be entitled to, are described in Exhibit A.

2. **Payment.** Client agrees to pay OrangeBoy as specified in Exhibit B. Unless otherwise specified: (i) fees are based on the services and access to which Client is entitled, and are not dependent on Client’s actual usage of those services and access, (ii) payment obligations are non-cancelable and fees paid are non-refundable, and (iii) the services and access set out in Exhibit A cannot be modified during the relevant subscription term except by written agreement of the parties. Client agrees that payment is not contingent on the delivery of any Savannah functionality or features other than set out in Exhibit A.

3. **General Terms of Use.** Client agrees to take reasonable steps to ensure that each person who gains access to Savannah by virtue of this Agreement (each “End User”): (i) notifies OrangeBoy immediately if the End User becomes aware of any unauthorized access to or usage of Savannah; (ii) uses Savannah in accordance with applicable local, state and federal laws, government regulations, and Client’s organizational policies; and (iii) does not reveal the End User’s account and password information to others and does not allow the use of any End User account by a person not authorized to use that account, including the End User’s family and other members of his or her household.

4. **End User Departures.** Client agrees to notify OrangeBoy in writing no more than 5 days after an End User’s employment or consulting relationship with Client terminates.

5. **Intellectual Property.** Client hereby acknowledges that certain intellectual property licensed or
developed by OrangeBoy (hereinafter “Intellectual Property”) is incorporated into Savannah and that Client’s rights regarding such Intellectual Property are limited to those necessary to use Savannah pursuant to this Agreement. Client acknowledges that other than that discussed above, no right or title to the Intellectual Property passes to Client by virtue of this Agreement and that Client has no rights to sell, share, copy, or disseminate any portion of the Intellectual Property or any elements derived or produced therefrom.

Client hereby grants OrangeBoy the right to host, copy, transmit, and display any data provided by Client, as well as any other rights reasonably necessary for OrangeBoy to carry out the terms of this Agreement.

6. Data Responsibility. Client understands and agrees that it has the responsibility to input valid, accurate data into Savannah and that failing to do so may result in invalid or inaccurate analysis or results. OrangeBoy accepts no responsibility for invalid or inaccurate data provided by Client.

Client is responsible for ensuring that any data submitted to OrangeBoy or Savannah is consistent with Client’s privacy policies and applicable laws. OrangeBoy assumes no responsibility for data submitted by Client that violates the Client’s privacy policies or applicable laws.

7. Confidential Information. Except as provided in this Agreement or by consent of Client, OrangeBoy shall not reveal to any third party or make use of for its own benefit any non-public or confidential information submitted by Client to OrangeBoy or Savannah, including non-public or confidential customer list(s) or customer usage data. For clarity, “non-public or confidential information” shall not include: (1) any information that has become generally available to the public or Client’s industry through no fault of OrangeBoy; (2) any information independently developed by OrangeBoy; (3) any information obtained by OrangeBoy through a source having no obligation to keep the information confidential; or (4) any information required to be disclosed by applicable law; or (5) “industry insights,” as described in paragraph 8 below.

8. Industry Insights. OrangeBoy may derive insights about the library industry from its processing, aggregation, and analysis of data submitted by Client. The parties hereby agree that OrangeBoy shall have the right to use, apply, and disseminate any such insights as it sees fit, except: (1) where otherwise stated in this Agreement; (2) where such use, application, or dissemination would personally identify any of the Client’s customers; or (3) where such use, application, or dissemination would constitute a willful violation of any privacy rights of any of the Client’s customers.

9. Indemnification and Consequential Damages. Client agrees to fully indemnify and hold harmless OrangeBoy from and against any losses, including attorney’s fees and costs that arise out of or relate to any breach of this Agreement by Client.

In no event shall OrangeBoy or its suppliers be liable for any incidental or consequential damages, lost profits or lost data, or any other indirect damages caused by OrangeBoy’s performance or nonperformance of this Agreement, except where such damages arise through OrangeBoy’s failure to take reasonable precautions.
10. **Termination.** Unless otherwise specified in Exhibit A, this Agreement will be effective as of the date of execution and will continue for a term of one year.

Following breach of any material term of this Agreement, the non-breaching party may terminate this agreement by (1) providing the breaching party with written notice of the breach, and (2) if such breach is not cured within 30 days, providing the breaching party with written notice of termination.

Upon termination, the Client remains liable for any payments set out in Exhibit B that were due and owing at the time of the termination.

11. **Governing Law and Venue.** This Agreement and all of its rights and obligations shall be governed by and construed in accordance with the law of the State of Ohio. The parties agree that the only appropriate venue for any claim brought to enforce this agreement shall be in Franklin County, Ohio. The parties further waive any objection to personal jurisdiction and venue with regard to any civil action brought in Franklin County, Ohio pursuant to this provision.

12. **Counterparts.** This agreement may be executed in one or more identical counterparts, each of which shall be deemed an original, but all of which together shall constitute one and the same instrument.

13. **Warranty of Authority.** Each signatory to this agreement hereby warrants that he or she has the authority to execute this agreement on behalf of Client or Orange Boy, respectively; that the execution and performance of this agreement does not conflict with any other agreement by which Client or Orange Boy, respectively, is bound; and that the execution and performance of this agreement does not contravene any term or provision in the charter or by-laws of Client or Orange Boy, respectively.

14. **Miscellaneous.**

a. The parties agree that this Agreement is the complete and exclusive statement of the agreement between the parties and supersedes all proposals or prior agreements, oral or written, and all other communications between the parties related to the subject matter of this Agreement.

b. The parties agree that the provisions of this agreement are severable, and if any such provision is held invalid or unenforceable to any extent, the rest of the agreement shall remain valid and in effect to the greatest extent permitted by law.

c. The parties acknowledge that they have read this Agreement, understand it and agree to be bound by its terms and conditions.

d. All Exhibits referenced in this Agreement are incorporated herein and made a part hereof.

e. No amendment or modification of this Agreement shall be effective unless it is in writing and signed by authorized representatives of both parties.
BY SIGNING AND SENDING THIS DOCUMENT TO Springshare LLC ("SPRINGSHARE" or "LICENSOR") YOU ARE CONSENTING, ON BEHALF OF YOUR INSTITUTION, TO BE BOUND BY THIS AGREEMENT. FURTHERMORE, YOUR AFFIRMATIVE RESPONSE IS A REPRESENTATION THAT YOU HAVE THE AUTHORITY TO BIND YOUR INSTITUTION TO THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, THE INSTALLATION PROCESS WILL NOT CONTINUE.

AGREEMENT: Subject to payment of applicable license fees, Springshare (801 Brickell Ave. Suite 900, Miami FL 33131) grants to you a non-exclusive license to use its software ("Software") at your Institution.

You may not:
- modify, translate, or create derivative works based on the Software;
- rent, lease, grant a security interest in, or otherwise transfer rights to the Software; or
- reverse engineer or use the Software in order to (a) build a competitive product or service, (b) build a product using similar ideas, features or functions of the Software or (c) copy any ideas, features, or functions of the Software.

This license is granted for one year from the date on which the Software is delivered, unless otherwise agreed by both your institution and Licensor, and may be extended by the mutual agreement of the parties and after payment of the agreed renewal fee (which fee may be increased from time to time).

Licensor may make modifications to this Agreement only with the mutual agreement of the Licensee. Licensee’s only right with respect to any dissatisfaction with any policies or practices of Licensor is to terminate this Agreement by prompt notice to Licensor and immediately cease using the Software.

You represent and warrant to Licensor that you will not transmit any materials that violate the rights of any third party, including intellectual property and contractual rights, or personal or privacy rights. Licensor shall not be responsible for losses, costs, expenses, claims and liabilities (including attorneys’ fees) arising out of or relating to your violation of this Agreement.

In addition to any other rights set forth in this Agreement, either you or Licensor may terminate this Agreement at any time upon thirty (30) days written notice. You agree to immediately cease using the Software upon termination.

THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, AND YOU MAY HAVE OTHER LEGAL RIGHTS THAT VARY BY JURISDICTION.

TITLE: Title, ownership rights, and intellectual property rights in the Software shall remain in Licensor. You have no ownership rights in the Software. The Software is protected by the copyright laws and treaties. Title and related rights in the content accessed through the Software is the property of the applicable content owner and may be protected by applicable law. This License gives you no rights to such content.

TERMINATION: This license shall be terminated if either party commits a material or persistent breach of any term of this License and fails to remedy that breach (if capable of remedy) within thirty (30) days of notification in writing by the other party. On termination, you must cease using the Software.
OWNERSHIP OF DATA: Licensor does not own any data, information or material that you submit to the Software ("Customer Data"). You, not Licensor, shall have sole responsibility for the accuracy, quality, integrity, legality, reliability, appropriateness, and intellectual property ownership or right to use of all Customer Data, and Licensor shall not be responsible or liable for the deletion, correction, destruction, damage, loss or failure to store any Customer Data. In the event this Agreement is terminated, Licensor will make available to you a file of the Customer Data in XML format within 30 days of termination if you so request at the time of termination.

INTERNET DELAYS: Springshare’s services may be subject to limitations, delays, and other problems inherent in the use of the Internet and electronic communications. Licensor is not responsible for any delays, delivery failures, or other damage resulting from such problems.

LIMITATION OF LIABILITY: UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY, TORT, CONTRACT, OR OTHERWISE, SHALL LICENSOR BE LIABLE TO YOU OR ANY OTHER PERSON FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY CHARACTER INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF GOODWILL, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, OR ANY AND ALL OTHER COMMERCIAL DAMAGES OR LOSSES. IN NO EVENT WILL LICENSOR BE LIABLE FOR ANY DAMAGES IN EXCESS OF THE AMOUNT LICENSOR RECEIVED FROM YOU FOR A LICENSE TO THE SOFTWARE, EVEN IF LICENSOR SHALL HAVE BEEN INFORMED OF THE POSSIBILITY OF SUCH DAMAGES, OR FOR ANY CLAIM BY ANY OTHER PARTY. THIS LIMITATION OF LIABILITY SHALL NOT APPLY TO LIABILITY FOR DEATH OR PERSONAL INJURY TO THE EXTENT APPLICABLE LAW PROHIBITS SUCH LIMITATION. IN NO EVENT WILL LICENSOR BE HELD LIABLE FOR ANY DATA LOSS ASSOCIATED WITH THE SOFTWARE; IN NO EVENT WILL LICENSOR BE HELD RESPONSIBLE FOR THE OPERATION OR MAINTENANCE OF HARDWARE, EXCEPT AS PROVIDED IN THIS LICENSE AGREEMENT. FURTHERMORE, SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THIS LIMITATION AND EXCLUSION MAY NOT APPLY TO YOU.

If any provision of this Agreement is held to be unenforceable, such provision shall be reformed only to the extent necessary to make it enforceable.

Agreed by:

Institution: _____________________________
Name (print): _____________________________
Name (sign): _____________________________
Title: _____________________________
Date: _____________________________