Annotated Request For Proposals Examples - Table of Contents

Annotated Example Request For Proposal (RFP) Bibliography

Disclaimer – the examples included in this document are for informational purposes only and do not necessarily reflect all best practices. Please consult with legal counsel for legal advice or questions regarding any of the resources in this document.

From the Toolkit:

> **Prescriptive requirements** work best when you can provide a detailed, comprehensive list of privacy and security requirements for the product or service. Prescriptive requirements make it clear at the start to vendors about what you expect, but this approach does not allow vendors to elaborate on their answers to the requirements.
>
> **Descriptive requirements** allow the vendor to explain in detail how they meet the specific requirement. This approach lets libraries find out how vendors approach privacy without having to compile a comprehensive list, which can be time consuming and prone to missing a key privacy risk. At the same time, the library might have to spend more time with vendors who don't provide enough detail in their initial answers.

Prescriptive Functional Requirements

New York City Department of Education

https://forallschools.s3.amazonaws.com/static/images/forallrubrics-home/DOE%20RFP%20Information%20Security%20Requirements%2007-02-2014%20(Final).pdf

What to look for:

- Section describing federal, state, local, organizational, and industry regulations and policies that product must comply with
- Request for vendor information security policies containing specific areas of information security policies and practices
- Requirement for specific details and updates to vendor privacy policy
- Granular technical functional requirements for critical features and functions of the system
- Granular procedural functional requirements for vendor privacy and security practices

SUNY

https://librarytechnology.org/docs/librfp-123-main.pdf

What to look for:

- List of network security and required third party vulnerability assessments, with sharing the assessment results with the customer (SUNY)
- Geographic limitations for storage of data (restricted to US)
- Requirements around incident breach notification
- Prescriptive requirements around subcontracting and data processing under Data Privacy section

Descriptive Functional Requirements Examples

Chicago Public Library

https://librarytechnology.org/docs/librfp-8-main.pdf

What to look for:

- List of federal, state, local, organizational, and industry regulations and policies that product must comply with
- Requests information about disaster recovery including with subcontractors
- Exhibit 8 lists a number of prescriptive functional requirements, showing a hybrid approach to functional requirement types
  - Vendor is given the opportunity to describe how they meet or not meet these requirements in the Data Security and Access section
- Data policy includes all subcontractors hired by the vendor to provide the service or application
- Definitions for contractor, breach, and protected information
- Listing of industry standards in both sections of the RFP
- Data sanitation and end of agreement data handling expectations listed in Exhibit 8

Orbis Cascade Alliance

https://www.odin.nodak.edu/sites/default/files/rfp_shared_library_management_service_final.pdf

What to look for:

- Request for information around data recovery, including aspects of partial data recovery and full system data recovery
- Audit trails for changes to records, as well as possibly accessing previous versions of edited data records
- Identity management section contains a number of important functional requirements for securing and protecting data, including role management and

access, group and user privileges, and handling users with multiple accounts in multiple organizations

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 Infromation from unauthorized disclosure or abuse can have severe legal, financial and reputation consequences for the DOE, itsstudents, 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, 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, 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 equivelant 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 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 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.

RFP B

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 (HIPPAA), 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 safe-keeping 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 verity 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.

RFP C

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.
7) ~~Meet Federal & State (New York) Accessibility Guidelines and Law; specifically including WCAG2.0AA and Section 508 Technical Requirement Standards. See https://www.w3.org/WAI/ and https://www.access-board.gov/guidelines-and-standards for additional details~~. **Removed 2/16/2017.**

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]

RFP D

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).