NEW YORK STATE TEACHERS' RETIREMENT SYSTEM
10 Corporate Woods Drive, Albany, NY 12211-2395

NYSTRS ON-PREM/HYBRID TECHNICAL CHECKLIST

SYSTEM NAME

SYSTEM OWNER CONTACT INFORMATION

Contact Person	Email	Phone Number

VENDOR CONTACT INFORMATION (if applicable)

Vendor Name	Contact Person	Email	Phone Number

PRODUCT

Product Name	Version

NOTE: Any system diagrams to be included with your answers should be attached to the email generated by using the submit button to send this form to NYSTRS. Attach them separately from the form.

QUESTION	ANSWER
General Technology	
Please Describe Your System Requirements, Including: • Desktop Requirements • Browser Compatibility • Database Server Requirements • Web Server Requirements • Application Server Requirements • File Server Requirements • Compatibility with VMWARE vSphere/ESXi Virtual Server Environment • Compatibility with Citrix XenApp/XenDesktop Virtualization • Required 3rd Party Software Components	
Please describe your System Architecture, including diagrams: • Server/Application Components • High Availability Components Identified • Network Requirements • Storage Requirements • Replication	

QUESTION	ANSWER
General Technology	
Please give an overview of the implementation: • Installation pre-requisites and installation guides • Administration guides • Product Upgrades • Support options/Service Level Agreements	
Is the entire solution hosted on premises or is any part of the solution hosted off-site?	
How are system upgrades / maintenance patches handled? Explain how you ensure vulnerability mitigation.	
Please identify any and all ports and services that are required for this solution to function.	
General SLA and Contractual	
Please list the hours of availability for your application (if applicable).	
Please indicate your uptime and performance standards. What actions will you take in the event that these standards are not met?	
Please explain your support offering(s) and how each are handled.	
How is the product licensed? (Subscription, Site, named user, etc…)	

QUESTION	ANSWER
Security	
Describe the steps taken to harden the application and its underlying components.	
If the code for this solution is open source, has it been reviewed by any third party in any manner?	
Please explain the security controls you exercise to mitigate the OWASP Top 10.	
Identity, Authentication and Access Management	
What mechanisms and practices are in place and practiced for identity management, including integration (MFA, single-sign-on, federation, local accounts, etc.)?	
What mechanisms are supported for system authentication and authorization?	
Describe the granularity of access controls available and how access privileges and controls for data access are managed.	
Please describe the user roles for this system and the level of access required for each of these roles.	

QUESTION	ANSWER
Identity, Authentication and Access Management	
What type of client-side data export is possible through the systems described, including reports? Can this be controlled?	
What features are provided for access logging? Is all access, including administrative accounts, controlled and logged (i.e. firewalls, file system permissions, ACLs, database table permissions, packet logs, etc.)? If not, please explain.	
What features are provided for auditing and reporting access privileges, account maintenance, segregation of duties, etc.?	
Web-based Interfaces & TLS Implementations	
Does the product rely on Java, Adobe Flash Player, or similar technologies on the client side for access of a web-based system? If so, what policies are in place to ensure the latest security updates for required client-side components don't conflict with product requirements?	
If there is a web-based interface as part of this solution, does the interface enforce encryption? If encryption is enforced, will the system require the use of TLS or will it allow SSL? If TLS is required, will the system only allow the use of TLS 1.2 or higher?	
Is the cipher suite supported 256 bits or greater?	
What is the key strength of your TLS implementation?	

QUESTION	ANSWER
Encryption	
Describe the encryption implemented for data in transit. Is/will data be transmitted in an encrypted form at all times? Provide details of encryption mechanisms, ciphers, and key sizes used. Are minimum standards enforced? If so, what are these? Are cryptographic modules in use FIPS 140-2 compliant?	
Describe the encryption implemented for data at rest, including backups. Is/will data be stored in an encrypted form at all times? Provide details of encryption mechanisms, ciphers, and key sizes used. Are minimum standards enforced? If so, what are these? Are cryptographic modules in use FIPS 140-2 compliant?	
Describe the controls and safeguards in place and practices and procedures followed to ensure secure and proper encryption key management.	
Describe the data-loss and data-leakage prevention technologies and process in place to protect against customer data loss/leakage.	
Resilience	
Describe business continuity and disaster recovery provisions and guarantees provided with solution proposed. What are your current, tested plans?	

QUESTION	ANSWER
Resilience	
Describe all levels of redundancy or high availability that this system has. (Geographic high availability, local clustering, hot/cold standby, etc.)	
Describe your data backup processes (frequency, security) as well as the anticipated storage capacity requirements for these backups. For example, the system requires X GB per backup and Y days of backups.	
What are your Recovery Time Objectives and Recovery Point Objectives for this system?	
Data Management	
For all data collected or created via the service offering, how many instances/copies of data resources will exist, and where will these be located?	
What system and data access management, reporting, and record keeping tools are available for data and systems associated with this service offering?	
It is the expectation of NYSTRS that our data will not be shared without our knowledge and permission. Will NYSTRS data be shared with or hosted by any third parties? Briefly explain why each of these third parties will have access to NYSTRS data, and what you do to insure the security of the data in this case.	

QUESTION	ANSWER
Data Retention	
Describe how you ensure that the system supports data retention and disposition as required by the NYSTRS record retention requirements, for the duration of the engaged contract, if this is a deemed system of record.	
Describe the process the provider uses to respond to customer requests for system audit, legal discovery requests/holds, etc.? Who is responsible for preserving/ retrieving data for purposes of litigation? What costs?	
Application Development and Integration	
What coding language and framework is the product developed with and what platform is it developed on? (Objective-c, Swift, Java, .NET, 4.5 Framework, WPF, ASP, Angular, Spring, jQuery, etc.)	
What API's, web service, or other integration points are provided?	
How are customizations requested and implemented as part of the deployment program?	
Is source code made available to clients for extending uses or closed source?	
What environments are provided other than production (DEV/TST/QAT)? Is there additional cost for these environments? How is the refresh process for such environments handled?	

QUESTION	ANSWER
Application Development and Integration	
Does the product support SAML 2.0 for use of SSO? What about OpenID Connect (OIDC)/OAuth? Do you support Azure SSO? Is there any additional cost or additional licensing associated with SSO?	
Specific to Vendor-Managed On-Premises Solutions	
Is there a documented change management plan for the management of upgrades and patches?	
Describe the provisions taken to ensure the security of customer data in the solution. • Describe the steps taken to harden the application and its underlying components. • Please explain the Intrusion Detection/Prevention Systems in use. • Please describe any other controls in place (for example web application firewalls).	
Please explain how your systems, accounts, and data are segregated.	
What base level of assurances of privacy and security does the vendor provide, in terms of policies/standards?	

QUESTION	ANSWER
Specific to Vendor-Managed On-Premises Solutions	
Please explain the vendor's anticipated role in Incident Response and how coordination with NYSTRS would occur in the event of an incident.	
In the event of a breach, what responsibilities will the vendor have in terms of breach notifications to NYSTRS?	
Describe the methods and mechanisms used for record and document transmission, including: • Accepting submission of data from your organization • Disseminating reports and records to your organization Safeguards against accidental misrouting of data (e.g., if e-mail based, etc.)	
In the event NYSTRS decides to not continue or renew a service arrangement, describe the process /methods / costs associated to 1.) providing any data stored to NYSTRS and 2.) guarantee data has been securely purged from hosted environment, including backups	
If the provider discontinues service, what assurances are made on the ability to move organization data to either a system owned by your organization or another vendor? How portable is the data/files? Can it be exporting out to customer-side data backups or archives? What assurances are granted that all instances of NYSTRS data are fully and securely deleted, including instances on backup (including tape) and on all providers and locations where multi-sourced/multi-sited?	

Submit