UNIVERSITY OF NORTH CAROLINA CHARLOTTE | OFFICE OF OneIT

UNC Charlotte Prospective Vendor Technical Questionnaire

Project Number	
Project Name	

For Questions: Contact OneIT Planning and Projects

Management Office oneit-ppmo@uncc.edu

Last Updated: December 14, 2022

UNC Charlotte Prospective Vendor Technical Questionnaire

Contents

Introduction

When considering any IT software solution, due diligence must be taken to ensure that we have done all that we can to protect our investment and UNC Charlotte assets.
(Please answer the questions as applicable to your project)

*****To be completed by UNC Charlotte Resource*****

1 Project Information

Project Name -

Requester Name -

Project Sponsor -

Vendor Name -

Vendor Contact -

Vendor Email -

Vendor Phone -

2 Infrastructure

2.1.1 Is the solution Cloud Based or hosted on UNC Charlotte Infrastructure?

□ Vendor-hosted □ Hosted on-premise UNC Charlotte Infrastructure □ Co-Hosted by Vendor and UNCC

2.1.2 If vendor-hosted, does the vendor use their own servers or a cloud provider (AWS, Azure, etc.)?

2.1.3 Who will manage the system if hosted at UNC Charlotte? <please explain>

3 Product

3.1 Accessibility Requirements

3.1.1 Does vendor comply with Section 508 of the Rehabilitation Act of 1973, as amended, or WCAG 2.0 AA with respect to accessibility for individuals with disabilities? Yes ○ No ○

3.1.2 Does the product support UNC Charlotte branding standards? Yes ○ No ○

UNCC Website Conventions and Style Guide

3.2 System Access

3.2.1 If web-based, check all the browsers the vendor supports

name other:

Safari □ Firefox □ Explorer □ Chrome □ Opera □ Edge □ Other □

3.2.2 Does UNC Charlotte need a new website URL? Yes ○ No ○

3.2.3 If application offers mobile version check all the versions it supports

Blackberry □ Windows □ IOS □ Android □

3.2.4 Is VPN or secure access required to access the application from off campus? Yes ○ No ○

3.3 Peripheral Equipment

3.3.1 Does the application require additional equipment? Yes ○ No ○

<Please list all the peripheral equipment required. E.g. – scanners, printers, point of sale equipment etc. >

4 Integration

<This is a Required Section>

4.1 Authorization

4.1.1 Will the product/service appear to the end user as a service UNC Charlotte is providing directly? Yes ○ No ○

4.1.2 If 4.1.1 is NO, then will the end user understand that they are making use of an external non UNC Charlotte resource? Yes ○ No ○

4.1.3 Who will be responsible for the account management operations of the product/services such as password resets, general support, etc.?

UNC Charlotte □ UNC Charlotte Department □

ITS External Vendor □ Other □

<If other, please explain>

4.1.4 What data are needed from other systems (student/staff/faculty)? *<Please explain >*

4.1.5 As a project sponsor, do you have appropriate approvals from the data owners? Yes ○ No ○
(e.g., staff/faculty = HR, Student = Registrar)

4.1.6 At what frequency to do you need this data?
Real Time □ Daily □ On Demand □ Other □ *<If Other, please explain >*

4.1.7 Is there a need for custom API development? Yes ○ No ○

4.1.8 Does UNC Charlotte have the technical expertise to develop the custom API? Yes ○ No ○
ITS □ Business □

5 IT Security

5.1 Regulatory Compliance *<This is a Required Section>*

5.1.1 Will the application store, process, and/or transmit any of the following regulatory compliance data?

- Social Security Numbers (SSN) Yes ○ No ○
- Protected Health Information (PHI)? E.g. HIPAA Yes ○ No ○
- Credit Cardholder Data (CHD)? E.g.PCI-DSS Yes ○ No ○
- Personally Identifiable Information (PII)? Yes ○ No ○
- Personally Identifiable Student Education Records? E.g. FERPA Yes ○ No ○
- Clinical Research Data? E.g.FDA CFR 21 Part 11 Yes ○ No ○
- Federally Funded or Contracted? E.g.FISMA Yes ○ No ○
- Personally Identifiable Financial Information? E.g.GLBA Yes ○ No ○

5.2 Auditing and Reporting

5.2.1 Does the application support audit/logging capabilities to a syslog/SIEM solution? Yes ○ No ○

5.2.2 Are there any audits to verify or reports on access? Access by: Yes ○ No ○
UNCC affiliated staff/faculty/students □ The vendor □ The public □

To be completed by Vendor

5.3 Data Encryption *<This is a Required Section>*

5.3.1 Does the vendor have any rights to use and share UNCC data (aggregated or not)? Yes ○ No ○

5.3.2 Is there a provision that the service provider holds UNCC data “in trust” for us, making it a legal fiduciary? Yes ○ No ○

5.3.3 Does the vendor have policies and procedures in place to ensure that their own staff do not have access to UNCC data? Yes ○ No ○

5.3.4 Does the vendor have policies and procedures in place to detect, prevent and mitigate identity theft? *<If Yes, please explain>* Yes ○ No ○

5.3.5 Will the application data be encrypted at rest using modern day encryption standards? *<If NO, provide compensating controls>* Yes ○ No ○

5.3.6 Will the application data be encrypted in-transit using SSL, TLS or VPN? *<If NO, provide compensating controls>* Yes ○ No ○

5.3.7 Does the application leverage back-end database? (Oracle, MS-SQL, MySQL, etc.) Yes ○ No ○

5.3.8 If yes, can the database be encrypted at-rest? Yes ○ No ○

5.3.9 Will the software be integrated with other UNC Charlotte systems like Banner? Yes ○ No ○

5.3.10 If the solution has data integration options available, please describe the types of data integration options utilized (e.g., APIs, .csv import/export).

5.4 Support

5.4.1 Does the application use an embedded support tool that communicates in/outbound (e.g., GoToMyPC, Team Viewer, VNC, etc.)? Yes ○ No ○

<If Yes, name the support tool>?

5.5 Access Controls and Security

5.5.1 Does the vendor support login methods by Shibboleth? Yes ○ No ○

5.5.2 For web-based solutions, can it leverage UNCC ITS SAML Based Authentication? Yes ○ No ○

<If NO, provide description of authentication mechanism and its security controls>

5.5.3 Does the vendor support CAS-based authentication? Yes ○ No ○

5.5.4 Does the vendor have its own authentication? <If Yes, please explain> Yes ○ No ○

5.5.5 If the vendor has their own Authentication, please explain password complexity rules and how often they need to be reset.

5.5.6 Does the vendor support login methods through Two Factor Authentication? Yes ○ No ○

5.6 Cloud Specific Compliance *<This is a Required Section>*

5.6.1 Can the vendor provide a third party audit report describing the security features in place at the organization? E.g. Service Organization Control (SOC) 2 Report or equivalent attestation report?

Yes ○ No ○

<If you or your infrastructure provider are working towards any of these certifications please state that and gives us a timeframe by which this certification will be accomplished>

5.6.2 Who is the vendor's Cloud Service Provider (CSP)?

5.6.3 What is the vendor's Cloud Computing Architecture?

□ SaaS Single – Tenancy □ SaaS Multi–Tenancy

□ PaaS □ IaaS

5.6.4 How is UNCC data secured and segregated from that of other customers?
< Please explain>

5.6.5 In which country (or countries) will the data reside?

□ USA □ Other, Please Indicate:

5.6.6 Upon termination of the contract, will the vendor's process completely purge University information from their organization's /infrastructure provider's systems and backups?

□ Yes □ No, explain: □

5.6.7 Do we have the right to audit, annual site visit?

□ Yes □ No, explain: □

6 Infrastructure and Operational Considerations

6.0 At a high level, please list the elements and versions of your technical stack.

□

6.1 Data Center *<This is a Required Section>*

6.1.1 Does the vendor have a Data center? Yes ○ No ○

6.1.2 Can the vendor provide external certification in the form of a SAS 70 Type 2 Audit? Yes ○ No ○

6.1.3 Is the vendor's data center certified? Yes ○ No ○
< If Yes, please provide all data center certifications (SOC2, SOC3, ISO, etc.)>

□

6.1.4 Is the Data center owned and operated by the vendor or outsourced to a third party such as AWS or a hybrid? < *Please explain*> Yes ○ No ○

□

6.2 Business Continuity and Disaster Recovery

<This is Required Section>

6.2.1 Does the vendor have a clearly defined, documented and formally approved Business Continuity Plan Policy? Yes ○ No ○

6.2.2 Does the vendor have dedicated resources with assigned responsibilities for the BCP? Yes ○ No ○

6.2.3 Has the vendor defined critical business functions that must be recovered in case of an emergency? *<If Yes, please explain>* Yes ○ No ○

6.2.4 Does the vendor have defined strategies to ensure the protection and recoverability of UNC Charlotte’s key information records, application and data. Please describe the means and time frame at which these may be restored or replaced (physically or electronically?) Yes ○ No ○

6.2.5 Has the vendor provisioned for testing their BCP annually? Yes ○ No ○

6.2.6 Has the vendor provisioned for testing their Disaster Recovery plans annually? Yes ○ No ○

6.2.7 Will UNC Charlotte staff and students be able to have continued access to the assets shorty after an emergency or interruption? Yes ○ No ○

6.2.8 Does the vendor have clearly defined back up procedures for key applications, hardware and data? *<If Yes, please explain>* Yes ○ No ○

6.2.9 Does the vendor review and update their plans annually? Yes ○ No ○

<If Yes, please explain>

6.2.10 Where applicable, has the vendor established pre- designated alternate sites, located a prudent distance from primary sites? *<If Yes, please explain>* Yes ○ No ○

6.3 Network Standards

6.3.1 Are there any network or telephone connections used by the system? Yes ○ No ○

<If Yes, please explain what type of network or telephone connection is required. Will it require a connection to the internet? If the equipment is connected to the UNC Charlotte network or telephone system, where will it be located?>

6.4 Email Standards

6.4.1 Does the solution need to send email? Yes ○ No ○

6.4.2 If yes, will it send email from a @uncc.edu email address? Yes ○ No ○

□ to campus □ to external people □ to both

6.4.3 Does your application send email to university constituents that originates from a third-party server or that will spoof the uncc.edu email domain? If so, are you able to generate Domain Key Identified Mail (DKIM) signatures, customize the return-path domain to match the spoofed uncc.edu domain, or utilize the university's trusted email relay to send email on behalf of the university? Yes ○ No ○

<If Yes, please explain>

7 Support Model <This is a Required Section>

7.1.1 Is the vendor available for support 24X7? Yes ○ No ○

7.1.2 Is the 24X7 response based on urgency levels? Yes ○ No ○

7.1.3 What is the escalation process to vendor’s management team?
< Please explain>

7.1.4 How will known issues be communicated to UNC Charlotte?
< Please explain>

7.1.5 What is the vendor’s SLA policy?
<Please explain different response times and resolution goals based on the severity of the issue. What determines Severity1 vs 2 vs 3.etc.>

7.1.6 Is there monitoring in place? Yes ○ No ○
<Please explain what kind of monitoring is in place.>

7.1.7 Is there scheduled maintenance in place which will cause the system to be unavailable? If so, how will UNC Charlotte receive advance notifications? Yes ○ No ○

<Please explain when the vendor conducts scheduled maintenance on the system and how it is communicated to customers.>

7.1.8 What is the vendor's upgrade cycle and process

<Please explain.>

8 Licensing and Contract

8.1 Licensing

8.1.1 Can UNC Charlotte leverage the existing licenses, including any consortium agreements that may be in place? Yes ○ No ○

8.1.2 Does the product require other software products to be acquired? E.g. Windows or Red Hat OS, Tomcat, Microsoft Visual Studio, reporting tools, Oracle, SQL Server, Apache, Acrobat Pro, etc.? *<If Yes, please explain>* Yes ○ No ○

8.1.3 Is the licensing concurrent? Yes ○ No ○

<Please explain how usage will be tracked>

8.2 Contract

8.2.1 How can the contract be terminated and what are the penalties?

<Please explain >

8.2.2 Upon termination of the contract, will data be transitioned back to UNCC in a usable format? How does UNC Charlotte get back its data after termination? *<Please explain >* Yes ○ No ○

8.2.3 If the system is custom developed, does UNC Charlotte own the application code base?

<Please explain how the software will be maintained, enhanced, supported and patched for the lifetime of the application> Yes ○ No ○

8.2.4 If the vendor company goes bankrupt, what happens to the application code base and UNC Charlotte's data? How can UNC Charlotte continue use the application?

<Please explain >

9 Signature

Checklist Information provided By (Vendor):

Print Name:

X

Vendor

10 Glossary

Term	Description
HIPAA	Health Insurance Portability and Accountability Act
CHD	Card Holder Data
PCI DSS	The Payment Card Industry Data Security Standard
PII	Personally Identifiable Information
FERPA	Family Educational Rights and Privacy Act
FDA CFR 21 Part 11	US Food and Drug Administration Code of Federal Regulations Title 21 Part 11. The regulations in this part set forth the criteria under which the agency considers electronic records, electronic signatures, and handwritten signatures executed to electronic records to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper
FISMA	The Federal Information Security Act
GLBA	Gramm-Leach –Bliley Act – is a federal law enacted in the US to control the ways financial institutions deal with the private information of individuals
SIEM	Security Information and Event Management. Provide real-time analysis of security alerts generated by network hardware and applications
Syslog	Syslog is a way for network devices to send event messages to a logging serve
AES -128	Advanced Encryption Standard
RSA – 3072	RSA is an algorithm used by modern computers to encrypt and decrypt messages
SHA -256	Secure Hash Algorithm
SSL	SSL (Secure Sockets Layer) is the standard security technology for establishing an encrypted link between a web server and a browser
TLS	Transport Layer Security
VPN	Virtual Private Network
SAML	Security Assertion Markup Language
ADFS	Active Directory Federation Services
Shibboleth	Federated Identity Management Solution
SOC	Report on Controls at a Service Organization Relevant to User Entities’
SaaS	Software as a Service
PaaS	Platform as a Service
IaaS	Infrastructure as a Service
SAS 70 Type 2 Audit	Statement of Auditing Standards
AWS	Amazon Web Services
BCP	Business Continuity Plan
API	Application Program Interface
ADA	Americans with Disabilities Act