UTHSC Information Technology Services (ITS)
IT Vendor Questionnaire

The purpose of this questionnaire is to collect information about a proposed application or system to be implemented at UTHSC for use on the UTHSC network and computing resources and/or to access UTHSC data. ITS will use this information to evaluate the vendor and technology's capabilities and compliance with institutional policies, applicable laws and regulations, and industry standards; and determine system and support requirements. Please respond to all questions (indicate "NA" where not applicable).

Question	Response
BASIC APPLICATION/SYSTEM INFORMATION	
1. Company name:	
2. Primary point of contact (name, phone, email):	
3. Application name:	
4. Description of application:	
5. Who will use the application?	
6. Operating system and version:	
7. Database type/versions supported:	
8. Database type/version in which application is developed:	
9. Server requirements (if local hosting):	
10. Networking requirements:	
11. Web browser requirements:	
12. Other system requirements:	
13. What support do you provide for this system/application and its users?	
14. What are your support hours?	
15. What is the average response time for support calls?	
16. What support will UTHSC be responsible for providing for the system/application and its users?	
DATA MANAGEMENT AND INTEGRATION	
17. What type of data will be stored, transmitted, or accessed by this system/application?	
18. Indicate if the following data types will be stored, transmitted, or accessed by this application/system:	
a. Patient Health Information (PHI)	
b. Personally Identifiable Information (PII)	
c. Payment Card Information (PCI)	
d. Other financial information	
e. Family Educational Rights and Privacy Act (FERPA)	
f. Intellectual property	
g. Research data	
19. Where will this data be hosted?	
20. Who will have access to this data (i.e., vendor, faculty, staff, students, public, etc.)?	
21. How will this data be accessed (e.g., application interface, web portal, or third party application)?	
22. Does this application or system use cloud services?	
23. Are users of the system able to download/extract data to their local machines?	

24. Describe any integration requirements that require exchanging data with other UTHSC systems.	
25. Will a user-data import/integration be required to populate the system? If so:	
a. What file formats are acceptable (e.g., CSV)? Attach interface documentation if available.	
b. Can the import be automated, and if so, for what intervals (e.g., daily, weekly, etc.)?	
c. What are the acceptable import-file delivery methods (e.g., SFTP)?	
d. Will the planned data exchange be uni-directional only (from UTHSC systems to your application/system), or is a bi-directional integration desired or needed?	
e. What type of data will be required to populate the system (e.g., student data, employee data)?	
f. Is an API available to handle the user-data exchange?	
AUTHENTICATION, AUTHORIZATION & ACCESS MANAGEMENT	
26. What are the integration requirements for authentication and/or authorization?	
27. What methods of authentication can be used to authenticate users to the system application?	
28. Is there additional cost for authentication setup?	
29. What user access control mechanisms does the system/application provide (e.g., role-based access)? Include internal application access controls as well.	
30. Provide a list of all accounts required to manage the system and/or application, along with who is responsible for each account.	
31. Who is responsible for provisioning user access (i.e., adding/modifying/removing) to the system and application?	
32. How does your organization manage accountability for generic accounts and functional IDs?	
33. List the security controls that are in place to prevent unauthorized access by other customers or third parties to UTHSC data housed in this system/application.	
ACCOUNT AND PASSWORD MANAGEMENT	
34. FOR INTERNAL PASSWORD MANAGEMENT ONLY: Describe the system/application's password requirements (e.g., re-use, required character types, etc.)	
35. Does the system/application require initial password change after a user's first login?	
36. Is the system/application configured with the following account security standards:	
a. Account lockout after no more than 6 failed logon attempts	
b. Lockout duration of at least 30 minutes or until an administrator resets the account	
c. User session inactivity expiration timeout duration	
NETWORK ACCESS AND DATA PROTECTION	

37. Provide system architecture documentation, including a network diagram of the system and external connections. IP and sensitive vendor information may be omitted.	
38. List the certificate authority (trusted third party) that signs your digital certificate.	
39. List the network protocols or ports required for this system/application.	
40. List the protocols used by the system to encrypt data in transit.	
41. For data encryption at rest, provide the following: a. Encryption vendor b. Encryption algorithm that is implemented c. Is the encryption module FIPS 140-2 validated?	
42. For the enforcement of encryption on portable devices containing sensitive data, provide the following: a. Encryption vendor b. Encryption algorithm that is implemented c. Is the encryption module FIPS 140-2 validated?	
43. Are backups encrypted?	
44. Will access to this application be limited to networks identified by UTHSC?	
45. How are logs secured from tampering?	
46. For remote customer support, describe how you plan to connect to UTHSC's computing environment.	
47. Is the application's database in a shared/clustered environment?	
48. If your company allows access to servers and data from the company's wireless network, how is that access secured?	
49. What systems can connect directly to the database(s)?	
50. How is administrative access to servers restricted (by user, by role, by device or some combination of these)?	
51. Are systems in place to prevent data ex-filtration via the network or a physical device (e.g., USB drive)?	
52. Are there any instances when the application/system is required to use an unsecure service (e.g., ftp) or otherwise store or transmit passwords in clear text?	
AUDITING/LOGGING/MONITORING	
53. Is the system/application configured to log privileged account access (e.g., super-user, administrator, and root) including	
54. Does the system/application maintain a secure audit record each time a user accesses, updates, creates, or deletes information? If so, does the audit record contain the following information:	
a. Unique user identifier	
b. A unique data subject (e.g. patient) identifier	
c. The function performed by the user	
d. The time and date that the function was performed	
55. How long are logs retained? Are they available to UTHSC upon request?	

56. How is the system monitored for suspicious activity? How often are logs reviewed?	
PHYSICAL SECURITY	
57. Describe the physical security controls in place where the system infrastructure is located.	
58. Does your organization maintain a log of users who enter the data center and their reason for entry?	
59. How do you enforce secure destruction of electronic media or hard copy of sensitive or regulated data?	
VULNERABILITY AND THREAT MANAGEMENT	
60. Who will be responsible for maintaining the system updates with the latest security patches or hotfixes?	
61. List the product(s) deployed to protect your systems and application against viruses and malware.	
62. Does your organization perform regular security vulnerability scanning? If so, provide a summary report of your last scan.	
63. Has your organization performed a security penetration test on your environment? If so, provide an executive summary report of your last test.	
64. Do you use any tools to specifically test the security of web applications you develop?	
AVAILABILITY, BACKUP AND RECOVERY	
65. What mechanisms are in place to address fault tolerance and high availability of this system? Provide your Continuity of Business document.	
66. Who will be responsible for the backup and recovery process?	
67. What is the expected recovery time in the event of an unexpected outage?	
68. Is disaster recovery provided? If so, what are the recovery point objective and the recovery time objective?	
69. Is there additional cost for disaster recovery? If so, what is that cost?	
CHANGE MANAGEMENT	
70. Describe your standard change management process.	
71. How are staff changes handled? Specifically, what is the process for removing staff access when they leave?	
72. Do you have a segregated environment for Development, User Acceptance Testing (UAT), and Production?	
73. How do you notify clients and staff when a system/application change is to be implemented?	
COMPLIANCE	
74. Does your organization require employees to take annual security and privacy awareness training?	
75. What processes does your organization have in place to comply with applicable laws, regulations, and industry standards? Attach any applicable certifications (e.g., HITRUST, PCI DSS, SAS70/SSAE 16 Type, II etc.).	
76. Do you have an incident response plan and a breach notification process?	

77. Can you provide documentation that details the operation, architecture and administration of the system/application?	
78. Is the application/system compliant with the Americans with Disabilities Act, standard WCAG 2.0 AA?	
INTERNATIONAL OPERATIONS	
79. Does your organization have any international operations?	
80. Does your organization partner with any vendors or contractors with international operations?	
81. In what countries do your international employees, vendors, or contractors have operations?	
82. Describe your systems, applications, and data that your international employees, vendors, or contractors are able to access AND their access method(s).	
83. What IT security controls are implemented to ensure that data is transmitted securely with your international employees, vendors, or contractors?	
84. What IT security controls are implemented to ensure that data is stored securely on the systems of your international employees, vendors, or contractors?	
85. Provide the vendor names, product names, and versions of the workstation antivirus and encryption software used by your international employees, vendors, or contractors.	