**HSC IT Security Checklist for Cloud Application Requests**

Approval to purchase Cloud hosted services.

|  |  |  |  |
| --- | --- | --- | --- |
| **Ticket Number** | **Customer** | **Software Name** | **Requesting Department** |
|  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Application admin or user of the software (if single user app)** | | | |
| First Name | Last Name | HSC NetID\* | Phone |
|  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Department Admin (purchasing the software)** | | | |
| First Name | Last Name | HSC NetID\* | Phone |
|  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Local IT Support Contact (not the HSC IT service desk, this would be your local departmental IT - if you have one)** | | | |
| First Name | Last Name | HSC NetID | Phone |
|  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Manager or Director (approving the purchase)** | | | |
| First Name | Last Name | HSC NetID | Phone |
|  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Required Documentation** | | | |
|  | Provide the URL where data is uploaded or downloaded | |  |
|  | Provide the URL where the user logs in | |  |
|  | Provide the vendor’s terms and conditions, privacy statement and security statement if any. | |  |
|  | Does the application utilize MFA (Multi Factor Authentication)?  **NOTE THAT ANY STORAGE OF PHI AND PII REQUIRES MFA.** Exceptions require senior executive approval. | | Yes  No  If MFA is available, will you be implementing and requiring use of MFA?  Yes (strongly suggested)  No  Will you be tying into the HSC’s Azure?  Yes (strongly suggested)  No (if no how will you enforce use of MFA) |
|  | Is the data stored in the Continental United States? | | Yes  No (if no, where is it stored?) |
|  | Has the vendor been through an independent assessment of their cloud security controls? This is normally a "SOC2" audit. ISO 27001 or FEDRAMP audits are also acceptable. | | SOC 2  ISO 27001  FEDRAMP  None |
|  | Describe the data classification (data created or uploaded to the app)  Examples of data classifications:   * Confidential (PHI and PII) * Restricted (sensitive UNM data) * Unrestricted (data that does not require safeguarding or dissemination controls, e.g., public information)   Will any data be accessed by the vendor or someone outside UNM | | What is the data classification:  Confidential  Restricted  Unrestricted  Will data be accessed by vendor or someone outside UNM:  Yes  No |
|  | Will you have a single account or multiple accounts used to login? What account roles will exist (specifically are they generic user accounts or will you have a local application administrator role assigned to the department or both)? | | Single  Multiple  Account roles: |
|  | Does the application have an AI component | | Yes  No |
|  | Has the Departmental Security Procedure been drafted?  Verify the Security Procedure contains:  Detailed breakdown of info stored in app  Password policies (SAML authentication?)  User Access Management procedure: Procedures for authorizing accounts, creating and reviewing and de-provisioning accounts, logging/monitoring account usage as needed.  Details about training new employees on best practices for using the app  What are your requirements for data retention and backup? (How long do we need to hold onto the data?) | | Yes  No |
|  | Will you be integrating the login with HSC NetID’s (typically SAML authentication is used to integrate)?  Hint: If you don’t know the answer is probably no. | | Yes  No |
|  | Provide a detailed description of the records that will be stored in the application. | |  |
|  | Are any of the records not owned by your department (e.g. owned by the patient, student, employee, research team, outside agency, etc.)? | | Yes  No  If yes, who owns the data and have you/will you receive their consent to store in this application? |
|  | Will you process PHI?  Will you process student information?  Will you only process student “directory information?”  Directory information is a subset of less sensitive student data that may generally be disclosed. For a list of directory information, see: <https://studentprivacy.ed.gov/content/directory-information>.  If you have questions about student PII contact the data steward - Todd Hynson [Thynson@salud.unm.edu](mailto:Thynson@salud.unm.edu). | | Yes  No  Yes  No  Yes  No  If data is PHI or student PII please provide an estimate of how many records:  Less than 500  Greater than 500  NOTE: If you process student information other than directory information, we require MFA for all accounts. |
|  | Security Responsibility?  Institution  Department  Individual | Final assessment:   * Assessment – * Sensitive or confidential information allowed in the application? * Vendor terms and conditions and security safeguards reviewed for meeting minimum standards?   Final Risk Rating: | |