**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** | | | |
| First Name | Last Name | HSC NetID | Phone |
|  |  |  |  |

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

|  |  |  |  |
| --- | --- | --- | --- |
| **Required Documentation** | | | |
|  | Check the URL where data is uploaded or downloaded and verify that the certificate passes. | |  |
|  | Check the URL where the user logs in and verify that the login process is legitimate and that all credentials are being transmitted while encrypted (verify certificate if different than general data transfers). | |  |
|  | Check the vendor’s terms and conditions, privacy statement, security statement if any. | |  |
|  | Verify the data classification (what will be created or uploaded)   * Indicate any accessed by the vendor or someone outside UNM | |  |
|  | Single or multiple accounts, account roles (specifically local application administrator role assigned to the department). | |  |
|  | Procedures for authorizing, creating and reviewing account in policy | |  |
|  | UNM Records retention/backup requirements and vendor agreement alignment | |  |
|  | Business continuity/disaster recovery requirements satisfied | |  |
|  | HSC infrastructure services integration consideration (most commonly SAML authentication)? | |  |
|  | License type: Individual’s use or for the department’s use (if business what administrative tools will be used)   * Consumer grade license * Business grade license?   Administrative Tools   * Account administrator – define password requirements, acct expiration, grant access to different roles (all data, personal data only). Responsible for any backup/BC needs. Can you set the complexity of the password, reset passwords, have access to manage the accounts in regards to expiration & active/inactive, ability to assign users to different roles (read only/read+write). | |  |
|  | Description of business records that will be stored in application. | |  |
|  | Review and approval for the use of records no owned by the department (patient, student, employee, research, etc.) | |  |
|  | \*\*\*Special Note: Any request that involves confidential information (PHI, FERPA (student regulated), employee, research records, etc.) must include attached approvals from the appropriate data stewards at the institution level (or their delegates). | |  |
|  | 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: | |