|  |  |
| --- | --- |
|  | Infrastructure |
| INF 1.1 | Provide infrastructure requirements (or options) and specification including storage requirements and ports for app/web servers |
| INF 1.2 | Provide list of supported Operating systems/Versions and upgrade/certification process  |
| INF 1.3 | Provide list of supported Web Browsers/Versions and upgrade/certification process |
| INF 1.4 | Provide full inventory of all software needed for your system |
| INF 1.5 | Provide recommended OS/Hardware Upgrade Policy - For internally hosted |
| INF 1.6 | Describe Mobile devices (smartphones, tablets) support |
| INF 1.7 | Describe deployment process of Application fixes/enhancements - For internally hosted |
| INF 1.8 | Describe Application Upgrade Process - For internally hosted |
| INF 1.9 | Explain ability to refresh data and configuration on demand for non-production environment – For internally hosted |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

|  |  |
| --- | --- |
|  | Security |
| SEC 1.1 | Ability to provide Application for UCSF operating system vulnerability scan |
| SEC 1.2 | What are your authentication protocols? |
| SEC 1.3 | Describe SSO solutions and ability to integrate with Shibboleth |
| SEC 1.4 | Describe Application Access Audit and monitoring capability |
| SEC 1.5 | Describe any server/application configuration options for security (i.e. timeout, lockout) |
| SEC 1.6 | Describe how security configuration is managed for hardware and/or software (including OS) |
| SEC 1.7 | Provide Security risk/vulnerability assessment Results |
| SEC 1.8 | Describe continuous security vulnerability assessment & Remediation process |
| SEC 1.9 | Describe methodology on staying current with latest security standards |
| SEC 1.10 | Describe Security Patch process |
| SEC 1.11 | Describe authenticated (Privileged) scan process |
| SEC 1.12 | Describe User Account provision/de-provision/change Process (include infrastructure, configuration management and software) |
| SEC 1.13 | Describe User Account review process |
| SEC 1.14 | Describe intrusion detection process |
| SEC 1.15 | Describe password mandates |
| SEC 1.16 | Describe data encryptions for all sensitive data |
| SEC 1.17 | Describe password/passphrase complexity |
| SEC 1.18 | Describe encryption in Transit between all devices and servers |
| SEC 1.19 | Describe encryption on Mobile devices and removable storage media |
| SEC 1.20 | Describe secure deletion process upon decommission |
| SEC 1.21 | Describe control access to the application via its incorporated interface |
| SEC 1.22 | Describe control access to the underlying data via direct and third-party tools |
| SEC 1.23 | Describe control access across different user roles |
| SEC 1.24 | Describe security at the field level, screen level and user role level |
| SEC 1.25 | Describe privacy and security training in your organization |
| SEC 1.26 | Describe reports available for all audits within the system |
|  |  |
| SEC 1.1 | Ability to provide Application for UCSF operating system vulnerability scan (authenticated at all privilege levels and unauthenticated) |
| SEC 1.2 | Ability to provide Application for UCSF application vulnerability scan (authenticated at all privilege levels and unauthenticated) |
| SEC 1.3 | What are your authentication protocols? |
| SEC 1.4 | Describe SSO solutions and ability to integrate with Shibboleth |
| SEC 1.5 | Describe Application Access Audit and monitoring capability |
| SEC 1.6 | Describe any server/application configuration options for security (i.e. timeout, lockout) |
| SEC 1.7 | Describe how security configuration is managed for hardware and/or software (including OS) |
| SEC 1.8 | Provide Security risk/vulnerability assessment Results |
| SEC 1.9 | Describe continuous security vulnerability assessment & Remediation process |
| SEC 1.10 | Describe methodology on staying current with latest security standards |
| SEC 1.11 | Describe Security Patch process |
| SEC 1.12 | Describe authenticated (Privileged) scan process |
| SEC 1.13 | Describe User Account provision/de-provision/change Process (include infrastructure, configuration management and software) |
| SEC 1.14 | Describe User Account review process |
| SEC 1.15 | Describe intrusion detection process |
| SEC 1.16 | Describe password mandates |
| SEC 1.17 | Describe data encryption for all restricted data in transmission |
| SEC 1.18 | Describe password/passphrase complexity |
| SEC 1.19 | Describe encryption in Transit between all devices and servers |
| SEC 1.20 | Describe encryption on Mobile devices and removable storage media |
| SEC 1.21 | Describe secure deletion process upon decommission |
| SEC 1.22 | Describe control access to the application via its incorporated interface |
| SEC 1.23 | Describe control access to the underlying data via direct and third-party tools |
| SEC 1.24 | Describe control access across different user roles |
| SEC 1.25 | Describe security at the field level, screen level and user role level |
| SEC 1.26 | Describe privacy and security training in your organization |
| SEC 1.27 | Describe reports available for all audits within the system |
| SEC 1.28 | Describe data encryption for all restricted data at rest |
| SEC 1.29 | Describe data encryption for all restricted data during process |
| SEC 1.30 | Describe key management capabilities and lifecycle (key storage, use, distribution, destruction, archiving, offline availability, generation, etc.) |
| SEC 1.31 | Describe encryption algorithms |
| SEC 1.32 | Describe key exchange capabilities |
| SEC 1.33 | Please describe Active Directory integration and support capabilities (leverage LDAP, Active Directory services, forest aware, federated services, non-contiguous DNS domain Active Directory forest of trees, etc.) |
| SEC 1.34 | Describe user account provisioning API's and automation capabilities |
| SEC 1.35 | Describe HIPAA compliance with the security rule administrative safeguards (required and addressable elements) |
| SEC 1.36 | Describe HIPAA compliance with the security rule technical safeguards (required and addressable elements) |
| SEC 1.37 | Describe HIPAA compliance with the security rule physical safeguards (required and addressable elements) |
| SEC 1.38 | Describe your companies risk analysis and risk management processes |
| SEC 1.39 | Describe any audit or certification (e.g. SOC 2 type 2, ISO, etc.) |
| SEC 1.40 | Describe PCI compliance capabilities |
| SEC 1.41 | Describe FERPA compliance capabilities  |
| SEC 1.42 | Describe adherence to SB1386 regulatory compliance |
| SEC 1.43 | Describe user ID/password expiration options (date based, lack of activity based, brute force lock out) and if the solution can meet UCSF policies and standards |
| SEC 1.44 | Does the solution require password changes? Please describe |
| SEC 1.45 | Does the service offer self-service for user based password self-service and/or security questions? Please describe |
| SEC 1.46 | Can your solution provide automatic logoff based on time and/or activity? Please describe |
| SEC 1.47 | Can you solution provide login activity (frequency and anomaly detection? Please describe |
| SEC 1.48 | Can you solution provide login geographic anomaly detection? Please describe |
| SEC 1.49 | Does your solution provide two-factor authentication, partner-based integration with another two-factor authentication solution or a best practice integration reference |
| SEC 1.50 | Are passwords masked when entered in the password field? Please describe |
| SEC 1.51 | Are passwords removed on page reload or when selecting the "back button"? Please describe |
| SEC 1.52 | Does the solution provide user activity reporting? Please describe |
| SEC 1.53 | Does the solution provide administrative roles based access control with pre-built templates? Please describe |
| SEC 1.54 | Does the solution provide user-based roles based access control with pre-built templates? Please describe |
| SEC 1.55 | Describe login auditing detail available in solution. |
| SEC 1.56 | Does the solution provide external/federated authentication or public userID capabilities? Please describe |
| SEC 1.57 | Is data encrypted between application tiers and/or different elements of a distributed system (e.g. encrypted when transmitting information between the web server, the application server, and the web server)? Please describe |
| SEC 1.58 | Does the solution offer offline media encryption? Please describe |
| SEC 1.59 | Describe the log retention capabilities. |
| SEC 1.60 | Please describe the system recovery options for the solution and any customer provided pre-requisites. |
| SEC 1.61 | Does the vendor provide documentation describing best practice architecture and guidance for various recovery time objectives and recovery point objectives?  |
| SEC 1.62 | Please describe the software development lifecycle model and or any standards followed in creating, maintaining, and versioning software. |
| SEC 1.63 | Please describe adherence to development for best practices and to mitigate common vulnerabilities such as XSS, XSRF, SQL injection , etc. |
| SEC 1.64 | Please describe programming practices to protect against buffer overflows, format string attacks, in-memory data exfiltration attacks, etc.  |
| SEC 1.65 | Please describe reference deployment/architecture/configuration penetration and vulnerability testing |

Note from UCSF IT Security:

This check list is not meant to replace meaningful analysis based on the product and/or service being acquired in the RFP. It is to serve as a base method for common security controls and capabilities for software and hardware solutions. This does not address “X as a service” RFP’s in totality and special attention should be paid to these solutions and something similar to NIST’s NIST Publishes Draft Cloud Computing Security or CSA’s CCM should be leveraged to identify and characterize the cloud service being reviewed so that appropriate levels of diligence can be addressed. For further detail please reference NIST guidelines for the specific technological area being reviewed. For all solutions a review of UC and UCSF policies, guidelines, standards, and procedures should be reviewed to ensure appropriate RFP questions are added in. Lastly, all local, state, and federal regulatory requirements should be addressed based on the data type, business function, and/or solution target for the solution being purchased.

|  |  |
| --- | --- |
|  | Development |
| DEV 1.1 | Describe how application is certified in new release of OS or RDBMS |
| DEV 1.2 | Describe Development platform (Programming languages, Frameworks etc.) |
| DEV 1.3 | Describe customer’s ability to customize/extend applications |
| DEV 1.4 | Describe Application Enhancement/Upgrade Process |
| DEV 1.5 | Describe Development/Testing Process  |
| DEV 1.6 | Describe Application patch/fix |
| DEV 1.7 | Describe archive methodology and retrieval of archived data procedure |
| DEV 1.8 | Explain Performance Testing process and Benchmark |
| DEV 1.9 | Describe ability to export data and configurations |
| DEV 1.10 | Describe ability to refresh Dev/Test database on-demand from production DB |
| DEV 1.11 | Describe Data Conversion/migration utility/tools |
| DEV 1.12 | Describe Source Code availability |
| DEV 1.13 | Provide published and documented API |
| DEV 1.14 | Provide Development road map |
| DEV 1.15 | Describe Reporting Solutions |
| DEV 1.16 | Describe how system is Accessibility Compliant |
| DEV 1.17 | Describe experience with integrating with ERP Systems (give specific examples) |
| DEV 1.18 | Describe Application Support process (hours, methods) - For internally hosted |
| DEV 1.19 | Describe Technical Training availability |
|  |  |
|  |  |

|  |  |
| --- | --- |
|  | SaaS |
| SaaS 1.1 | Describe data center physical security |
| SaaS 1.2 | Describe Disaster Recovery/Testing process and provide documentation |
| SaaS 1.3 | Describe how security configuration is managed for hardware, software (including OS) |
| SaaS 1.4 | Describe your environment’s systems firewall configurations |
| SaaS 1.5 | Describe how the infrastructure of the system is separated from other unrelated systems |
| SaaS 1.6 | What control is in place to prevent non-essential staff from accessing customer data |
| SaaS 1.7 | Describe solution to ensure use of authentication on all devices and protects from unauthorized access |
| SaaS 1.8 | Describe available environments (Dev, QA, STG, TRN, PROD etc.) |
| SaaS 1.9 | Explain BAA procedure with Customer |
| SaaS 1.10 | Describe backup/recovery procedures (failover process/procedure) |
| SaaS 1.11 | Describe Technical Support process (hours, methods) |
| SaaS 1.12 | Explain how SaaS can be converted to in-house hosted solution and vice-versa |
| SaaS 1.13 | Explain OS/HW Upgrade Process/Procedures |
| SaaS 1.14 | Describe system availability (24x7) and explain any required downtime |
| SaaS 1.15 | Describe Server maintenance process/procedure |
| SaaS 1.16 | Describe Server and Application Monitoring Process/Procedures |
| SaaS 1.17 | Explain a method for data transfer and destruction in case of conversion to other system |
| SaaS 1.18 | Describe how UCSF personnel can access data |
| SaaS 1.19 | Describe experience with integrating with Shibboleth (UCSF SSO) solution |
| SaaS 1.20 | Describe deployment process of Application fixes/enhancements |
| SaaS 1.21 | Describe Application Upgrade Process |
| SaaS 1.22 | Explain how System environment documents are kept current |
| SaaS 1.23 | Explain ability to refresh data and configuration on demand for non-production environment |