

Nebraska Department of Health   
and Human Services Licensure System RFP

Attachment 3  
   
Technical Requirements   
Traceability Matrix

June 15, 2020

**ATTACHMENT THREE**

**Technical Requirements Traceability Matrix**

**Request for Proposal Number 6249 Z1**

**Bidder Name: MST Solutions**

Bidders must describe in detail how the proposed system meets the conformance specification outlined within each Technical Requirement. It is not sufficient for the Bidder to simply state that it intends to meet the requirements of the RFP. The traceability matrix must indicate how the Bidder intends to comply with each requirement and the effort required to achieve that compliance.

The traceability matrix is used to document and track the project requirements from the proposal through testing to verify that the requirements have been met. The Contractor will be responsible for maintaining the contract set of Baseline Requirements. This traceability matrix will form one of the key artifacts required for testing and validation that each requirement has been complied with (i.e., 100% fulfilled).

The bidder must ensure that the original requirement identifier and requirement description are maintained from the traceability matrix.

How to complete the traceability matrix:

|  |  |
| --- | --- |
| Column Description | Bidder Responsibility |
| Req # | The unique identifier for the requirement as assigned by DHHS, followed by the specific requirement number. This column is dictated by this RFP and must not be modified by the Bidder. |
| Requirement | The description of the requirement to which the Bidder must respond. This language is specified in the RFP and must not be modified by the Bidder. |
| (1) Comply | Bidder must insert an "X" if the system complies with the requirement. Describe in the response how the system meets the requirement. If the system does not comply with the requirement, the Bidder must address the following:   1. Capability does not currently exist in the system, but is planned in the near future (within the next few months) 2. Capability not available, is not planned, or requires extensive source-code design and customization to be considered part of the Bidder's standard capability 3. Capability requires an extensive integration effort of more than 500 hours |
| (a) Core | Bidder must insert an "X" if the requirement is met by existing capabilities of the core system or with minor modifications or configuration to existing functionality. |
| (b) Custom | Bidder must insert an "X" if the Bidder proposes to custom develop the capability to meet this requirement. Indicate "custom" for those features that require substantial or "from the ground up" development efforts. |
| (c) 3rd Party | Bidder must insert an "X" if the Bidder proposed to meet this requirement using a 3rd party component or product (e.g., a COTS vendor or other 3rd party). The Bidder must describe the product, including product name, functionality, and benefits in the response. |

**TECHNICAL REQUIREMENTS**

The following requirements describe what is needed to support DHHS technical project operations.

Each requirement is identified by the following first three characters:

|  |  |
| --- | --- |
| TEC | General Technical Requirements |
| STN | Standards Requirements |
| ERR | Error Handling Requirements |
| DBM | Database/Data Management Requirements |
| BKP | Backup and System Recovery Requirements |
| SEC | Security Requirements |
| DAC | Data Conversion Requirements |
| PTT | Production, Test and Training Requirements |
| INT | Interfaces/Imports/Exports Requirements |
| PER | System Performance Requirements |
| DOC | System and User Documentation |

***General Technical Requirements***

This section presents the overall technical requirements that apply to the software. Describe in the response how the system meets the requirement.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Req #** | **Requirement** | (1) Comply | (a) Core | | | | (b) Custom | | | (c) 3rd Party |
| TEC-1 | Provide a description and diagram of the technical architecture. Include all database/web/networking hardware, software, tools, etc. Indicate where the system is hosted. Indicate if any components are needed on the client and/or loaded on servers, etc. Solution will only be server/cloud technology in nature.  DHHS envisions one domain to be hosted for all applications.  Currently, online renewal applications for individuals and businesses subject to the Uniform Credentialing Act are handled by System Automation.  Online initial applications for Nursing and online renewal applications for Long-Term Care are submitted via Nebraska Interactive. | X | X | | | |  | | |  |
| Response:  **100% Multi-Tenant, Cloud Application**  Salesforce offers the market leading Platform as a Service (PaaS) and market leading Software as a Service (SaaS) solutions.  Salesforce is a multi-tenant, cloud-based web application. No additional software or infrastructure is required. Salesforce hosts the entire solution, thus freeing up the State to manage its mission, not manage an infrastructure solution. Additionally, Salesforce is browser agnostic and supports all major browsers (Firefox, Chrome, Safari, IE, Edge). No installations on users’ laptops or desktops are required and thus the solution is accessible from anywhere an internet connection and supported browser are available, including mobile devices.  The fully documented list of supported browsers and mobile devices for the full Salesforce site and Salesforce Mobile is available in the following articles in online our Help & Training Portal: https://help.salesforce.com/HTViewHelpDoc?id=getstart\_browser\_overview.htm&language=en\_US and <https://help.salesforce.com/articleView?id=sf1_requirements.htm&type=0&language=en_US&release=206.5>.  **Solution Architecture**  Our proposed Software as a Service (SaaS) solution is built on the Salesforce Lightning Platform and includes all needed infrastructure, which is fully hosted, managed, and maintained by Salesforce. Salesforce only requires a computer that can run a web browser and an Internet connection or a mobile device. No other software or hardware is required. Salesforce applications are delivered on-demand over the Internet, so the State will not need to worry about licensing software or setting up and managing hardware platforms.  The Salesforce Platform as a Service (PaaS) is built for cloud computing, with multi tenancy inherent in its design. To meet the high demands of its large user population, the Salesforce Platform's foundation is a metadata-driven software architecture that enables multi-tenant applications.  Salesforce combines several different persistence technologies, including a custom-designed relational database schema, which are innately designed for clouds and multi tenancy—no virtualization required.    Salesforce Lightning Platform’s core technology uses a runtime engine that materializes all application data from metadata—data about the data itself. In Salesforce Lightning Platform’s well-defined metadata-driven architecture, there is a clear separation of the compiled runtime database engine (kernel), tenant data, and the metadata that describes each application. These distinct boundaries make it possible to independently update the system kernel and tenant-specific applications and schemas, with virtually no risk of one affecting the others.    Every logical database object that Salesforce exposes is internally managed using metadata. Objects, (tables in traditional relational database parlance), fields, stored procedures, and database triggers are all abstract constructs that exist merely as metadata in Salesforce Lightning Platform’s Universal Data Dictionary (UDD). For example, when you define a new application object or write some procedural code, Salesforce does not create an actual table in a database or compile any code. Instead, Salesforce simply stores metadata that the system’s engine can use to generate the virtual application components at runtime. When you need to modify or customize something about the application schema, like modify an existing field in an object, all that’s required is a simple non-blocking update to the corresponding metadata.  Because metadata is a key ingredient of Salesforce applications, the system’s runtime engine must optimize access to metadata; otherwise, frequent metadata access would prevent the service from scaling. With this potential bottleneck in mind, Salesforce uses massive and sophisticated metadata caches to maintain the most recently used metadata in memory, avoid performance-sapping disk I/O and code recompilations, and improve application response times.  The multitenant architecture and secure logical controls address separation of Customer Data. The Salesforce infrastructure is divided into a modular architecture based on “instances”. Each instance is capable of supporting several thousand customers in a secure and efficient manner. Salesforce uses the instance architecture to continue to scale and meet the demands of our customers. There are appropriate controls in place designed to prevent any given customer’s Salesforce instance from being compromised. This functionality has been designed and undergoes robust testing through an on-going process by both Salesforce and its customers.    These papers further explain the technology that makes the Salesforce Lightning Platform fast, scalable, and secure for any type of application:  <https://developer.salesforce.com/page/Multi_Tenant_Architecture>  <https://developer.salesforce.com/page/Secure_Private_Trustworthy_Force.com_Whitepaper>  <https://developer.salesforce.com/page/An_Overview_of_Force.com_Security>  **Government Cloud**  Salesforce was the first Cloud Service Provider granted a FedRAMP Authority to Operate (ATO) for both Software as a Service (SaaS) and Platform as a Service (PaaS), consistent with the FedRAMP moderate baseline controls.    On May 23, 2014 Salesforce was granted a FedRAMP ATO at the moderate impact level issued by the Department of Health and Human Services (HHS) for the Salesforce Government Cloud. Testing for the ATO was performed by a third-party assessment organization (3PAO).    The Salesforce Government Cloud information system and authorization boundary, is comprised of the Salesforce Platform\*, Sales, Service, Communities, Analytics, Salesforce Mobile, and Industry Solutions, as well as the backend infrastructure (e.g., servers, network devices, databases, storage arrays) that support the operations of these products, referred to as the General Support System (GSS).    To obtain compliance with FedRAMP, Salesforce conducted security assessment and authorization activities in accordance with FedRAMP guidance, NIST SP 800-37, and HHS requirements. As part of this process Salesforce documented a System Security Plan (SSP) for the Salesforce Government Cloud service offering. The SSP is developed in accordance with NIST SP 800-18. The SSP identifies control implementations for the GSS and in-scope customer facing products (e.g., Lightning Platform, applicable Salesforce Services) according to the FedRAMP moderate baseline and HHS security control parameters. A security assessment of the information system was conducted by a 3PAO in accordance with FedRAMP Moderate requirements. The security assessment testing determined the adequacy of the management, operational, and technical security controls used to protect the confidentiality, integrity, and availability of Salesforce's Government Cloud service offering and the Customer Data it stores, transmits and processes.    To maintain compliance with FedRAMP, Salesforce conducts continuous monitoring, which includes ongoing technical vulnerability detection, remediation of open compliance related findings, and at least annual independent assessment of security controls by a 3PAO. As part of the current FedRAMP annual assessment, Salesforce is aligned with NIST SP 800-53 Revision 4.    Federal customers have the ability to access Salesforce's FedRAMP ATO package through the OMB MAX information portal upon filling out the Package Access Request form on the FedRAMP PMO website:<https://marketplace.fedramp.gov/#/product/salesforce-government-cloud?sort=productName>.  Additionally, under the Salesforce Government Cloud Compliance Information Non-Disclosure Agreement, other applicable customers approved for the Government Cloud can be provided the Salesforce Government Cloud FedRAMP ATO package outside of OMB MAX.  For more information on the Salesforce Government Cloud please see the [Salesforce Government Cloud whitepaper](https://org62.my.salesforce.com/sfc/p/#000000000062/a/0M000000Q8ar/moggeD49GPYM4jsNqrIjHnLlcqW7Zc7VwHfyKfuEmbs).    \*Only the Salesforce Platform is included within the FedRAMP Authorization Boundary for the Salesforce Government Cloud.    For more information on the Salesforce Government cloud please see the Salesforce Government Cloud white paper: <https://org62.my.salesforce.com/sfc/p/000000000062/a/0M000000Q8ar/moggeD49GPYM4jsNqrIjHnLlcqW7Zc7VwHfyKfuEmbs>. | | | | | | | | | | |
| TEC-2 | Describe how the system is responsive to mobile technology and works with mobile devices such as smart phones or tablets. | X | X | | | |  | | |  |
| Response:  **Salesforce Mobile**  Mobility is a native capability of the Salesforce Platform. The Salesforce mobile app is built on the Salesforce Platform and provides the State’s users with a completely unified mobile experience across a variety of mobile devices, including iOS and Android smartphones and tablets. Virtually all functions in the application proper can be accessed through our Salesforce mobile app such as collaboration, workflow and approvals and much more. Mobile support is standard, out-of-the-box functionality and requires no customization or third-party mobile application development tools. Configure your enterprise app once and it’s instantly mobile from the get-go.    The Salesforce mobile app allows the State’s users to access Salesforce solutions from anywhere, bringing all of the Salesforce customizations, configurations, settings, and data to any device. Salesforce mobile app can be instantly distributed to mobile users each time a new app is created – with no deployment headaches. With the power of the platform, administrators can build applications on the desktop and then mobile-enable them with just a few clicks. From custom tabs and configurations to Salesforce pages and more, the State can tailor mobile deployments for individual users or groups so that everyone is ultra-productive, no matter where they are located. Mobile enables the State to: develop and run mobile and desktop apps on a single cloud computing platform; create customized mobile profiles that are specific to a user or group’s needs; and push customizations over the air automatically so users never have to sync devices.    Salesforce Mobile Partner Applications  The Salesforce AppExchange provides a rich ecosystem of applications built by Salesforce's partners. This ecosystem supports and enables a wide variety of use cases, many of which are enabled on mobile devices. There are over 900 partner apps listed on the AppExchange: <https://appexchange.salesforce.com/appxSearchKeywordResults?keywords=mobile>.    Mobile Field Workers  The State's mobile field workers would be able to access their Salesforce environment to update service requests and manage assignments from the field via the Salesforce mobile app. The Salesforce mobile app is built on the Salesforce Platform and provides mobile field workers with a completely unified mobile experience across a variety of mobile devices, including iOS and Android smartphones and tablets. Virtually all functions in the application proper can be accessed through our Salesforce mobile app. The mobile app also allows users to logout when they have completed their tasks, and another user could login using their credentials, enabling multiple field workers to access the environment from one device.    Customer Mobile Access  The State's customers would be able to access information, such as knowledge articles, service request status, reported issues as well as report new issues and create service requests via a mobile device. The self-service, or community interface leverages HTML5 and therefore is accessible via the browser on a mobile device and re-factors to run optimally on the mobile device. Therefore, the functionality that a user has access to via the self-service application, including searching the knowledge base, creating, updating and viewing service requests, are available from a mobile device. Additionally, users can receive email on their mobile device, and with setup workflow rules, users can receive alerts when there are changes in the status of a service request. Salesforce offers several community templates that can be used to create a seamless self-service experience regardless of what device and channel the customer chooses to engage. Community templates allow the State to quickly and easily build a self-service community that gives customers the same visual and functional experience whether they use a tablet, a mobile device, or their desktop.    Salesforce Mobile SDK  If the State desires a more customized mobile application, the Salesforce Mobile SDK is an open-source suite of familiar technologies that will allow the State to rapidly build HTML5, native and hybrid mobile apps that connect to the Salesforce Platform. Using the SDK, the State can develop cross-platform HTML5 web apps, native iOS apps using Objective-C, or Android apps written with Java. The State can also create HTML5-based hybrid apps using the SDK’s Mobile container, a wrapper based on Apache Cordova (PhoneGap) that enables HTML5-based applications to leverage device features like the camera and microphone. Additionally, the SDK provides libraries for key enterprise requirements, such as authentication and secure offline storage, effectively providing an enterprise-ready mobile application container. For more details, see <https://developer.salesforce.com/devcenter/mobile>. | | | | | | | | | | |
| TEC-3 | Describe any third-party components that are proposed as part of the system, i.e. using Crystal Reports as a reporting tool. | X | X | | | | | |  |  |
| Response:  As part of the modular and scalable approach of the Salesforce platform there is a wide arrange of choices when it comes to what you implement and how. Often, it makes most sense to buy a pre-configured product off the shelf when it meets your use case and requirements to an acceptable extent. Additionally, this allows platform owners to put together best in breed technologies woven together through scalable, configurable an secure infrastructure.  For this project we have identified the following 3rd party products as part of a potential solution.   |  | | --- | | * Calendar Anything for Salesforce | | * Survey Monkey | | * Chargent Payment Gateway | | * Nintex DocGen (FedRamp) * Smarty Streets | | * Nintex eSign | | * DocuSign |   These products are proven in the market yet should be test further against NE DHHS requirements. Regarding ancillary benefits of the Salesforce platform there is a powerful suite of analytics and reporting tools to help you view and analyze your data. It lets you examine the data in almost infinite combinations, display it in easy-to-understand formats, and share the resulting insights with others. Following are the major components of the report builder:  Salesforce analytics consists of several integrated parts:    **Report Types**  A report type defines the set of records and fields available to a report based on the relationships between a primary object and its related objects. Reports display only records that meet the criteria defined in the report type. Salesforce provides a set of pre-defined standard report types; administrators can create custom report types as well. For example, an administrator can create a report type that shows only job applications that have an associated resume; applications without resumes won't show up in reports using that type. An administrator can also show records that may have related records—for example, applications with or without resumes. In this case, all applications, whether or not they have resumes, are available to reports using that type.    Report Formats  Salesforce reports can use the tabular, summary, matrix, or joined format:  *Tabular reports* are the simplest and fastest way to look at data. Similar to a spreadsheet, they consist simply of an ordered set of fields in columns, with each matching record listed in a row. Tabular reports are best for creating lists of records or a list with a single grand total. Examples include contact mailing lists and activity reports.  *Summary reports* are similar to tabular reports, but also allow users to group rows of data, view subtotals, and create charts. They can be used as the source report for dashboard components. This type of report can be used to show subtotals based on the value of a particular field or when a hierarchical list is desired, such as all Cases for your team, subtotaled by Status and Owner.  *Matrix reports* are similar to summary reports but allow users to group and summarize data by both rows and columns. This type of report can be used for comparing related totals, especially if there are large amounts of data to summarize and users need to compare values in several different fields, or users want to look at data by date and by type, person, or geography.  *Joined reports* let users create multiple report blocks that provide different views of the data. Each block acts like a “sub-report,” with its own fields, columns, sorting, and filtering. A joined report can even contain data from different report types.  *Tableau visualizations* give you a new way to see and understand your data. These are very strong in showing visual aspects of your data to quickly convey the importance of certain values and outliers.  Reports  A report returns a set of records that meets certain criteria and displays it in organized rows and columns. Report data can be filtered, grouped, and displayed graphically as a chart. Reports are stored in folders, which control who has access. To help you monitor the State, Salesforce offers a wide range of standard reports, accessible in the standard reports folders on the Reports tab. All our standard reports are "templates" so they can be used as report starting points from which users can alter fields, criteria, etc. and use the "Save As" function to easily capture a version more specific to their unique needs. Users can also create new custom reports to access exactly the information they need. Subtotal and limit data to help users analyze trends and get a concise picture of what is happening in the State.      *Figures: Example Salesforce Report for YTD Service Cases initiated from a customer on the Salesforce Customer Community web portal*    *A Tableau visualization with a fictitious example of abuse victims* | | | | | | | | | | |
| TEC-4 | Describe how the system is designed so that business rule parameters and code lookup tables can be easily updated without changing the overall application program logic. | X | X | | | |  | | |  |
| Response:  Business rules and processes can be created and assigned to specific fields. Business process management supported by Salesforce include:   * **Validation Rules** allow you to define rules for valid data entry values. Validation rules come complete with the ability to create your own error messages. This is a point-and-click, wizard-driven process. * **Workflow** allows you to create business rules to act on the entered data. Workflow rules may notify people if a field is changed, update another field based on the edit of the first field, or call out to some external process (a SOAP endpoint) where execution logic may fire. Workflow rules may have both multiple immediate actions and multiple time-based actions. Workflow rule management is a point-and-click, wizard-driven exercise. Also, note that you can set up field history on data records to track changes to any standard out-of-box or custom-created field. * **Process Builder** allows you to map out business rules with multiple criteria via a visual interface. Process Builder works for field updates and record creation, and can be invoked via other processes. Process Builder supports time-based actions. * **Cloud Flow Designer** allows you to not only design complex business rules via a visual interface, but allows you to expose those automated processes to your customers via Community pages, Visualforce pages, or even by clicking a button or a link. Cloud Flow Designer supports time-based actions.   For more information, please visit <https://help.salesforce.com/articleView?id=process_which_tool.htm&type=5>. | | | | | | | | | | |
| TEC-5 | Describe the upgrade and maintenance process for the system. Downtime and impact to the users must be minimized. | X | X | | |  | | | |  |
| Response:  **Upgrades and Maintenance**  All upgrades, patches, and other system maintenance are provided as part of the subscription service with no additional cost to the State. In addition, Salesforce releases 3 complimentary upgrades each year, in Winter, Spring, and Summer versions. All Salesforce users are always on the latest version of our platform because everyone gets instant upgrades (typically on an opt-in basis). Each time Salesforce releases a new version of the application and the platform, the entire community can take advantage of the latest innovations from our product development team. Because of our multi-tenant architecture, Salesforce is able to provide all of our customers with a service based on a single version of our application. We are able to upgrade all of our customers at the same time with each release. As a result, we do not have to maintain multiple versions of our application. Each release will be delivered automatically in a transparent manner and will not break your configurations.  When maintenance is scheduled, Salesforce publishes the dates and times of the maintenance windows on trust.salesforce.com which show a forward 12-month view of the maintenance windows Salesforce plans to take. Premier Alerts are sent via email when the maintenance windows are posted to trust.salesforce.com. Approximately one week prior to the scheduled maintenance, Salesforce communicates those dates and times via the in-application pop-up window upon login to Salesforce. In the event of planned maintenance that requires customer action in advance (e.g. updating network settings in preparation for additional login pools), Salesforce endeavors to communicate via email to system administrators of the State months prior to the maintenance.    Please note: If emergency system maintenance is required, customers may be notified less than one (1) week in advance.    There are two types of maintenance at Salesforce: System Maintenance and Release Maintenance.   1. System Maintenance is for sustaining the security, availability, and performance of the infrastructure supporting Salesforce services. 2. Release Maintenance is for upgrading Salesforce services to the latest product version to deliver enhanced features and functionality. There are three different kinds of release maintenance: major releases, patch releases, and emergency releases.     Major Release Maintenance dates and times are posted on trust.salesforce.com approximately one year before the release date. To see the schedule for your instance click on <https://status.salesforce.com/status> and select the relevant instance. On the calendar click the release date to view further information. Major release maintenance occurs three times per year during the windows listed below. The instance will be unavailable for up to five minutes during the release window.    Patch Releases and Emergency Releases are used to deliver scheduled and ad hoc application fixes and are typically seamless to customers. Whenever possible, patches and emergency releases are deployed during off-peak hours and without downtime. Patch releases are scheduled weekly and are usually deployed to instances on Tuesday, Wednesday or Thursday, with release to Asia-Pacific instances the following day. Emergency releases are conducted on an as-needed basis and can occur any day of the week.    Please refer to the following Help & Training article for more information: <https://help.salesforce.com/apex/HTViewSolution?id=000176208&language=en_US>. | | | | | | | | | | |
| TEC-6 | Describe any impact on customizations made to the system for upgrades and maintenance processes. Downtime and impact to the users must be minimized. | X | X | | | |  | | |  |
| Response:  We will work with customer to understand the window available for upgrades and maintenance process and will devise strategy to minimize the disruption to the business. As part of this strategy, we will perform tests in the full copy instance, which is a replica of production, to ensure that the deployments can be done within the specified maintenance window. In addition, Salesforce releases 3 upgrades each year and more information about their deployment strategy can be found in TEC-6.  In addition, each Salesforce release will be delivered automatically in a transparent manner without breaking any of the customizations built in the system. | | | | | | | | | | |
| TEC-7 | Describe any redundancy built into the system to limit any downtime. | X | X | | | |  | | |  |
| Response:  To maximize availability, the service is delivered using multiple world-class data centers supporting primary and replicated disaster recovery instances, plus a separate production-class lab facility. The infrastructure utilizes carrier-class components designed to support millions of users. Extensive use of high-availability servers and network technologies, and a carrier-neutral network strategy, help to minimize the risk of single points of failure, and provide a highly resilient environment with maximum uptime and performance.    The Salesforce Services are configured to be N+1 redundant at a minimum, where N is the number of components of a given type needed for the service to operate, and +1 is the redundancy. In many cases, Salesforce has more than one piece of redundant equipment for a given function. | | | | | | | | | | |
| TEC-8 | Describe how the system has the ability to share data securely, including importing and exporting of data to/from other application software tools, such as a Microsoft Excel file, XML, comma separated value (csv) file, etc. | X | X | | |  | | | |  |
| Response:  **Import/Export Utilities**  The Salesforce Platform includes the following import/export options for data:   * Data Import Wizard - An in-browser wizard that imports data for many standard Salesforce objects, including accounts, contacts, leads, solutions, campaign members, and person accounts. You can also import data for custom objects. * Salesforce Data Loader - Data Loader is a free, client application for the bulk import or export of data. Use it to insert, update, delete or export Salesforce records. * Direct Export - Data can be exported directly into CSV (comma separated values) file, or Excel files with a button click. This can be done from either a standard or custom list view, or from a report. This is the most common method utilized by end users. * Salesforce API - Data can be exported to and from the system through our API at any time or via a number of built in features. * Partner Tools - There are also many pre-integrated partner tools, some of which you may already own that may be leveraged. Examples of these include, but are not limited to, Informatica, Pervasive, CastIron, Boomi, etc.     We also offer a weekly export service (WES) for those customers requiring a local backup copy of their data or a data set for import into other applications (such as an ERP system). Exported file links can be included to assist with data migrations, data integrations, and provide more thorough backup and restore. | | | | | | | | | | |
| TEC-9 | Describe how the system has the ability to archive data and documents per the DHHS’ required record retention schedules, which provides different retention periods for different document types. Describe the method and ability to adjust to changes in the retention schedule. | X | X | | | |  | | |  |
| Response:  Active customer data stays on disk until the customer deletes or changes it. Customer-deleted data is temporarily available (15 days) to customers online from the Recycle Bin. The retention policy for backup media is 90 days (30 days for sandboxes). Deleted / modified data cannot be recovered after 90 days (30 days for sandboxes).    Salesforce customers are responsible for complying with their company's data retention requirements in their use of the Salesforce Services. If a Salesforce customer must preserve data and the retention procedures above are insufficient, they may schedule a weekly export of data or copy to a sandbox account. Exports of Customer Data are available in comma separated value (.csv) format by request via Salesforce's Customer Support department. In addition, many exports can be manually pulled by the designated org administrators. | | | | | | | | | | |
| TEC-10 | Describe how the system has the ability to provide audit information on all data accessed or changed within the system. | X | | X | | | |  | |  |
| Response:  **Core Auditing Capabilities**  Within Salesforce, the creator and last updater, as well as timestamps, are recorded for every record. Additionally, the Salesforce Platform and Salesforce Applications have a multitude of history tracking and auditing features that provide valuable information about the use of an organization’s applications and data, which in turn can be a critical tool in diagnosing potential or real security issues. Auditing features include:    Record Modification Fields - All objects include fields to store the name of the user who created the record and who last modified the record. This provides some basic auditing information.    Field History Tracking - Enable auditing for individual fields (up to 20 fields per object), which will automatically track any changes in the values of selected fields. Although auditing is available for all custom objects, only some standard objects allow field-level auditing.    Login History - Review up to 20,000 successful and failed login attempts to the State for the past six months. The State can also track the geographic location of the IP addresses of your logins in your personal settings. You can track the geographic location of the login IP addresses for any of your users in the user’s detail page. To get more detailed geographic information, such as city and postal code, you can download the login history. Due to the nature of geolocation technology, the accuracy of geolocation fields (for example, country, city, postal code) can vary.    Identity Verification History - Review up to 20,000 records of your org users’ identity verification attempts from the past six months. For example, suppose that two-factor authentication is enabled when a user logs in. When the user successfully provides a time-based, one-time password as proof of identity, that information is recorded in Identity Verification History.    Setup Audit Trail - Administrators can view a Setup Audit Trail for the past six months within Salesforce, which logs when modifications are made to the State's configuration.    While the Login History and Setup Audit Trail are available for six months within Salesforce, they can be downloaded and stored locally to meet longer audit log retention requirements. Additionally, historic event logs which provide more information can be provided for a fee. For more information, please see<https://help.salesforce.com/articleView?id=000336835&language=en_US&type=1&mode=1>.  **Event Monitoring**  In addition to Salesforce’s core auditing capabilities, Salesforce offers Event Monitoring as an additional license option. The State can use event monitoring to discover how often and at what times your users are logging into and out of the State. This includes insight into what Salesforce applications are being adopted by users, who is logging in and from where, what pages users are viewing, what knowledge articles users are viewing, what reports users are running and exporting, which search terms users are using and what individual users click, and other aspects of application usage. This capability helps you discriminate between valid and invalid login requests and also track user login patterns for future reference. For example, depending on your org settings, admins can log into Salesforce as another user. You can use Login As event type data to review those actions to identify any security breaches or vulnerabilities, and also to inform your users what occurred. Not only can the State better understand how your apps are being utilized, you can also monitor if users download large amounts of data that might put the State at risk. In addition, the State can also determine if an employee is unnecessarily downloading sensitive customer information, pinpointing the exact time and location of that event. Event Monitoring is delivered as an API-first feature and there are Salesforce partners with visualization tools available.    Use the SOAP API and REST API resources to retrieve event log files that contain information useful for assessing organizational usage trends and user behavior. Because event log files are accessed through the Salesforce Platform SOAP API and REST API, you can integrate log data with your own back-end storage and data marts so that you can correlate data from multiple organizations and across disparate systems easily. When using event monitoring, keep the following in mind:   * Log data can be deleted by your Salesforce administrator. You can’t insert or update log data. * Use the Event Type field to determine which files were generated for the State. * An event generates log data in real time. However, log files are generated the day after an event takes place, during non peak hours. Therefore, daily log file data is unavailable for at least one day after an event. For hourly log files, depending on event delivery and final processing time, an event is expected to take three to six hours from the time of the event to be available in the log file. However, it can take longer. * Log files, represented by the Event Type field, are only generated if there is at least one event of that type for the day or hour. If no events took place, the file isn't generated. * Log files are available based on Created Date for the last 30 days when organizations purchase User Event Monitoring * All event monitoring logs are exposed to the API through the Event Logfile object. However, there is no access through the user interface, except through the Event Monitoring Analytics app. * Hourly event log files are provided for you to review events in your orgs on an accelerated basis. However, it’s possible that you don’t get all event log data in hourly event log files, especially during site switches, instance refreshes, or unplanned system outages. For complete data, use the daily log files.     Event monitoring can be used with 49 different event types. For more information please see:<https://developer.salesforce.com/docs/atlas.en-us.api.meta/api/sforce_api_objects_eventlogfile_supportedeventtypes.htm>.    Event Monitoring Transaction Security  Transaction Security policies give the State the ability to take real-time security actions based on event triggers. With Transaction Security, you can monitor events according to the policies that you establish. When a policy is triggered, you can receive a notification and/or take an action.    For example, suppose that you activate a policy to limit the number of concurrent sessions per user to three. A user with three login sessions tries to create a fourth session. The State can require a user to end one of their existing sessions before proceeding with the new session. At the same time, you are notified that the policy was triggered. For more information, please see:<https://help.salesforce.com/articleView?id=security_transactions.htm>.    Real-Time Event Monitoring  With the Real-Time Event Monitoring feature, you can stream and store event data and create transaction security policies for several new events in Salesforce, all in real time. When you enable Real-Time Event Monitoring, you automatically get Enhanced Transaction Security—Salesforce’s latest and greatest feature for creating transaction security policies. Use Event Manager to view and monitor events in your org. For more information, please see: <https://help.salesforce.com/articleView?id=real_time_event_monitoring_overview.htm>.    Event Monitoring Analytics App  The State can use the built-in Event Monitoring Analytics App to explore your monitoring data in Salesforce. The Event Monitoring Analytics App integrates with Event Monitoring and Setup Audit Trail data to give you insights into your user and org behavior. App creation is easy and with its pre built dashboards and datasets, you can start exploring right away. This app helps you drill into your org’s data and swiftly identify suspicious behavior, slow page performance, and poor user adoption. Get valuable information instantly from your Salesforce event logs, such as the number of people and IP addresses accessing your org, which Visualforce requests are timing out, and which users make changes in Setup. The State can detect performance problems early, such as queries taking too much time, by getting notifications when a KPI value exceeds your established threshold. Hourly event log file integration with the Event Monitoring Analytics app is unavailable. Data is refreshed once a day in the app. For more information, please see: <https://help.salesforce.com/articleView?id=bi_app_admin_wave.htm>.  **Field Audit Trail**  Organizations desire certainty that their data is accurate, complete and reliable, enabling them to meet stringent industry regulations. With the addition of Field Audit Trail, the State's ability to track changes at the field level increases from 20 fields (core auditing) to 60 fields per object (Field Audit Trail), and the audit logs availability increases from 18 months (core auditing) to 10 years (Field Audit Trail). The State can also set different policies for each Salesforce object to ensure data is purged when no longer needed.    For more information, please see [https://help.salesforce.com/articleView?id=field\_audit\_trail.htm&type=5.](https://help.salesforce.com/articleView?id=field_audit_trail.htm&type=5) | | | | | | | | | | |
| TEC-11 | Describe how the system allows multiple users to use the software applications and database concurrently. | X | X | | | |  | | |  |
| Response:  Since we are a web application, we support a concurrency model inline with the web delivery model that allows concurrent access to the same record. In a web application model, record-level locking is not best practice. Rather, Salesforce services supports a rich data security model to easily control what users have access to records and what type of access they have to support effective collaboration. Under this, we support a last-in-change-wins model.    If multiple users are updating the same record simultaneously the system will notify a user if a record was updated during their current transaction. They will not be able to perform their change until they cancel their current attempt to change the record and start over. Additional information around Record Locking can be found here: <https://developer.salesforce.com/docs/atlas.en-us.draes.meta/draes/draes_object_relationships_record_level_locking.htm>. | | | | | | | | | | |
| TEC-12 | Describe how the system is scalable and flexible enough to accommodate any changes required by the DHHS, or by any federal statute, federal mandate, federal decision or federal policy. | X | X | | | |  | | |  |
| Response:  Configurability is one of the central tenet of our system so that it is flexible to easily accommodate changes that are mandated by federal policies or other circumstances. Our system allows to easily setup new license types along with the associated business processes through configuration rather than through code. Some of the processes that can be configured are as follows:    **Scalability**  Salesforce is a pure multi-tenant, cloud-based web application. Multi-tenancy gives applications elasticity. Salesforce applications can automatically scale from one to millions of users. Processing more than 5 billion transactions each day, Salesforce is used for large-scale deployments. Any application that runs on the Salesforce Platform is automatically architected to seamlessly scale from 1 user to millions of users without the customer having to do anything differently.    All applications (including mobile, offline, and read-only options) and data running on the Salesforce Platform are deployed to and replicated across multiple data centers in different geographies. Every application, no matter how large or small, gets the full benefits of the backup, failover, disaster recovery, and other infrastructure services required for an organization’s mission-critical applications. | | | | | | | | | | |
| TEC-13 | Describe how the system is able to scan, attach, and store different document types (pictures, documents, PDF file, etc.) within the system. | X |  | | | | | |  | X |
| Response:  CCScan is a 3rd party app from the Salesforce AppExchange that is used for scanning. Features include:  Capture scan & import digitized documents directly Salesforce with no extra steps saving massive amounts of time and effort.  Quick to set-up and intuitive to use, CCScan is user friendly regardless of your technical expertise. Scan or Import documents to Salesforce effortlessly.  Administrator modes allow for advanced users to setup and lock complex processes.  Eliminate manual steps and automate job, processing documents with minimal or no human activity beyond setup. Our software comes equipped with Barcode and OCR capabilities to further speed digitization, data access and archiving.  Scan or import documents to Salesforce Attachments, using automatically extracted data to identify, lookup record and populate fields.   Run unattended jobs to import electronic faxes and attach them automatically to existing or newly created Salesforce records.  Create PDF Attachments from scanned or imported documents and update fields with information extracted from the document in a single, fully automated step.  Use database lookup to retrieve key data to populate fields or lookup records in Salesforce.  Use intelligent technologies such as Barcode Detection, Zonal OCR and text pattern search with Regular Expressions to automate uploading, updating and creating Standard and Custom records and objects. Also store and access Attachments in Google Drive.  **Salesforce Content and Document Management Capabilities**  Salesforce offers the following different ways to store, publish, and tag files and documents. All file types are supported from traditional business documents such as Microsoft® PowerPoint presentations to audio files, video files, Web pages, and Google® docs.    Files Tab: Upload, store, find, follow, share, and collaborate on Salesforce files in the cloud. For example, upload a file in Chatter and store it there privately until you're ready to share it. Share the file with coworkers and groups to collaborate and get feedback. Attach files to posts in a Chatter feed on the Home tab, Chatter tab, a profile, a record, or a group. Salesforce Files can be used with or without Chatter. With Chatter turned off, the Files tab (Files home) is available: upload, share, view, and manage files. You can manage topics for your files right from the detail page. Use topics to find files more easily and connect them to other records. You can update, add, delete, and track library members all from one place. Library admins can create and manage library memberships from Files Home. External users automatically get an “external badge” in the Current Member section to identify external partners, customer community members, portal, and Chatter users. For more information on Files see: <https://help.salesforce.com/articleView?id=collab_salesforce_files_parent.htm&type=5>.    Salesforce Content: Publish and share official corporate files with coworkers and deliver them to customers. Documents are uploaded in Salesforce Content via a graphical user interface and a structured workflow process. This process captures key information related to the document, including file name, description, author, tags, document type, and any custom criteria you choose to collect. For example, Create, clone, or modify a document and save it so only you can see it and work on it. When you're ready, publish it so other users in the State have access to it. Create a content pack and send it to customers. In Lightning, the State can create public links to share folders, giving recipients inside or outside the State access to sets of files. The public link is an encrypted URL. Folder Sharing in Lightning Experience provides an alternative to Content Packs in Classic. Anyone with the link can view and download the files in the folder. You can change the folder’s contents at any time, and the changes occur in real time. To remove access to the folder, delete the link. To make the folder public again, create a new link. For more information on Salesforce Content see: <https://help.salesforce.com/articleView?id=content_parent.htm&type=5>.    Salesforce Libraries: In Lightning Experience, you can make libraries available to all users or a subset of users with or without Salesforce Content. In libraries, you can add multiple files to a library, update and delete library files, and move folders within a library. You can customize the fields and layout of the Files detail page and choose from standard fields to show when the file was last updated, file size, file type, and more. For additional information, please see: <http://releasenotes.docs.salesforce.com/en-us/summer17/release-notes/rn_files.htm?edition=&impact=> and <https://help.salesforce.com/articleView?id=collab_files_libraries_parent.htm&type=5>.    Salesforce Knowledge: Create and manage content, known as articles, in a knowledge base. Internal users and customers (on your Customer Portal, partner portal, Service Cloud Portal, or Salesforce Platform Sites) can quickly find and view articles they need. For example, write, edit, publish, and archive articles using the Articles Management tab or find and view published articles using the Articles tab. Customers and partners can access articles if Salesforce Knowledge is enabled in your Customer Portal, partner portal, Service Cloud Portal, or Salesforce Platform Sites. Create a public knowledge base so website visitors can view articles. For more information on Salesforce Knowledge see: <https://help.salesforce.com/articleView?id=knowledge_whatis.htm&type=5>.    Documents Tab: Store Web resources, such as, logos, DOT files, and other Visualforce materials in folders without attaching them to records. For example, add a custom logo to meeting requests by uploading your logo to the Documents tab. For more information, please see: <https://help.salesforce.com/articleView?id=docs_upload.htm&type=5>.    Attachments: Attach files to records from the Attachments related list on selected detail pages. For example, add a file to a specific record, like an event, contact, or case by attaching it on the Attachments related list. Attachments exist in Salesforce only in the context of the record they’re attached to. Files that users upload to the Attachments related list on records in Salesforce can also be set to become Salesforce Files objects. Once an Attachment is also a Salesforce File it can be shared with people, groups, libraries, and can be posted in feeds, synced, and updated with new versions.    Additional information on the differences between Files, Salesforce CRM Content, Salesforce Knowledge, Documents, and Attachments can be found at: <https://help.salesforce.com/articleView?id=collab_files_differences.htm&type=5>. | | | | | | | | | | |
| TEC-14 | Describe how the system has the ability to generate reports and ad hoc queries without performance impact to user access or system response time. | X | | | X | | | |  |  |
| Response:  **Core Reports & Dashboards**  Salesforce offers a powerful suite of analytics and reporting tools to help you view and analyze your data. Salesforce analytics consists of several integrated parts:    **Report Types**  A report type defines the set of records and fields available to a report based on the relationships between a primary object and its related objects. Reports display only records that meet the criteria defined in the report type. Salesforce provides a set of pre-defined standard report types; administrators can create custom report types as well. For example, an administrator can create a report type that shows only job applications that have an associated resume; applications without resumes won't show up in reports using that type. An administrator can also show records that may have related records—for example, applications with or without resumes. In this case, all applications, whether or not they have resumes, are available to reports using that type.    Report Formats  Salesforce reports can use the tabular, summary, matrix, or joined format:  *Tabular reports* are the simplest and fastest way to look at data. Similar to a spreadsheet, they consist simply of an ordered set of fields in columns, with each matching record listed in a row. Tabular reports are best for creating lists of records or a list with a single grand total. Examples include contact mailing lists and activity reports.  *Summary reports* are similar to tabular reports, but also allow users to group rows of data, view subtotals, and create charts. They can be used as the source report for dashboard components. This type of report can be used to show subtotals based on the value of a particular field or when a hierarchical list is desired, such as all Cases for your team, subtotaled by Status and Owner.  *Matrix reports* are similar to summary reports but allow users to group and summarize data by both rows and columns. This type of report can be used for comparing related totals, especially if there are large amounts of data to summarize and users need to compare values in several different fields, or users want to look at data by date and by type, person, or geography.  *Joined reports* let users create multiple report blocks that provide different views of the data. Each block acts like a “sub-report,” with its own fields, columns, sorting, and filtering. A joined report can even contain data from different report types.  *Tableau visualizations* give you a new way to see and understand your data. These are very strong in showing visual aspects of your data to quickly convey the importance of certain values and outliers.  Reports  A report returns a set of records that meets certain criteria and displays it in organized rows and columns. Report data can be filtered, grouped, and displayed graphically as a chart. Reports are stored in folders, which control who has access. To help you monitor the State, Salesforce offers a wide range of standard reports, accessible in the standard reports folders on the Reports tab. All our standard reports are "templates" so they can be used as report starting points from which users can alter fields, criteria, etc. and use the "Save As" function to easily capture a version more specific to their unique needs. Users can also create new custom reports to access exactly the information they need. Subtotal and limit data to help users analyze trends and get a concise picture of what is happening in the State.      *Figures: Example Salesforce Report for YTD Service Cases initiated from a customer on the Salesforce Customer Community web portal*    *A Tableau visualization with a fictitious example of abuse victims*  Report performance varies by report complexity, including the number of table joins required to produce report results. Most customer reports are executed in just a few seconds. There are some factors that can cause a report to perform poorly or to time out. Most of them can be addressed by simple changes, such as using the correct filter operators, increasing the number of filters, and reducing the amount of data.View Salesforce's Tutorial on Creating Reports with the Report Builder in Trailhead:  <https://trailhead.salesforce.com/en/modules/reports_dashboards/units/reports_dashboards_getting_started>.    Dashboards  A dashboard shows data from source reports as visual components, which can be charts, gauges, tables, metrics, or custom Visualforce pages. They provide a snapshot of key metrics and performance indicators for the State. Each dashboard can have up to 20 components. Administrators control access to dashboards by storing them in folders with certain visibility settings. Dashboard folders can be public, hidden, or restricted to groups, roles, or territories. If you have access to a folder, you can view its dashboards. To view a dashboard component, users need access to the folder for the underlying source report. Each dashboard has a running user, whose security settings determine which data to display in a dashboard. Your Data with the Lightning Dashboard Builder in Trailhead: <https://trailhead.salesforce.com/modules/lex_implementation_reports_dashboards/units/lex_implementation_reports_dashboards_visualizing_data>.    *Figure: Example customer service dashboard*    *A Tableau visualization with a fictitious example of abuse victims*    Folders  A folder is a place where you can store reports, dashboards, documents, or email templates. Folders can be public, hidden, or shared, and can be set to read-only or read/write. You control who has access to its contents based on roles, permissions, public groups, and license types. You can make a folder available to your entire organization, or make it private so that only the owner has access. \*Help article regarding upcoming retirement of Legacy Folder Sharing: <https://help.salesforce.com/articleView?id=000321245&type=1&mode=1&language=en_US>.    Analytic Snapshots  An analytic snapshot lets you report on historical data. Authorized users can save tabular or summary report results as snapshots on a schedule. Analytic snapshots let you to work with report data similarly to how you work with other records in Salesforce.com. For example, a customer support manager could set up an analytic snapshot that reports on the open cases assigned to his or her team every day at 5:00 PM, and store that data in a custom object to build a history on open cases from which he or she could spot trends via reports. Then the customer support manager could report on point-in-time or trend data stored in the custom object and use the report as a source for a dashboard component.    Other important points about dashboards:   * Dashboard components aren’t simply nice-looking, static pictures. They’re live, actionable objects. You can click on a dashboard component to drill down to the underlying report that generated it, and click on any item in that report to drill down to the source data. So you can quickly understand the reasons behind the results. * Dashboards are full participants in Salesforce’s enterprise social collaboration platform. For example, a manager could post a dashboard snapshot to their Chatter feed to share it with their “followers”, or to a specific Chatter group, along with comments, so that they can find answers, congratulate team members, or issue calls to action. And both dashboards and Chatter are available on mobile devices, as well as PCs. * Salesforce Reports and Dashboards allows users to configure reports in the Lightning Report Builder and add to a new and/or existing dashboard with the click of one button. Dashboard settings for reports can be maintained from the chart settings of a report.     **Tableau Visual Analytics**  Live visual analytics fuel unlimited data exploration. Interactive dashboards help you uncover hidden insights on the fly. Tableau harnesses people’s [natural ability to spot visual patterns](https://www.tableau.com/about/mission#breakthrough) quickly, revealing everyday opportunities and eureka moments alike.  Connect to data on premise or in the cloud—whether it’s big data, a SQL database, a spreadsheet, or cloud apps like Google Analytics and Salesforce. Access and combine disparate data without writing code. Power users can pivot, split, and manage metadata to optimize data sources. Analysis begins with data. Get more from yours with  Tableau.  Quickly build powerful calculations from existing data, drag and drop reference lines and forecasts, and review statistical summaries. Make your point with trend analyses, regressions, and correlations for tried and true statistical understanding. Ask new questions, spot trends, identify opportunities, and make data-driven decisions with confidence.  Create interactive maps automatically. Built-in postal codes mean lightning-fast mapping for more than 50 countries worldwide. Use custom geocodes and territories for personalized regions, like sales areas. We designed [Tableau maps](https://www.tableau.com/stories/topic/maps) specifically to help your data stand out.  **Einstein Analytics**  Einstein Analytics is a cloud-based platform designed for the business user to get answers to questions instantly through powerful, interactive visualizations of any data, on any device.    Salesforce core Reports and Dashboards deliver operational and performance metrics on data that lives solely in Salesforce and allows the State to easily create individual static reports and dashboards to gain real-time views of daily activity.    Einstein Analytics is an analytics system - designed to analyze data not just from within Salesforce, but from across different sources, and be surfaced across the State. More importantly, it is designed to engage users every day by embedding analytics in business processes — a native tab in the business system and on the home page, or an interactive component on your account page or object page.    Einstein Analytics complements native Salesforce Reports and Dashboard by providing:   * Multi-year trending analysis - Supports query and processing of hundreds of millions of rows of data from various sources * Cross Object analysis and faceting * Rich data visualization, including thematic maps     Finally, Einstein Analytics is designed to be API-first. And with the Analytics Web SDK you can extend functionality across Salesforce Lightning or any third-party website.    Einstein Analytics offers:   * Collaboration: Leveraging annotations, sharing and notifications * Actions: Configure Actions with few clicks * Self-service: True, unhindered explorations     Within the State, you may have data everywhere: warehouses, spreadsheets, logs, and in Salesforce. With Einstein Analytics, it’s easy to integrate data from any of these sources, including external data such as SAP or Oracle data, mobile app data, or product sensor data.    With Einstein Analytics, the State will gain powerful interactive visualization tools with a fast, fluid way to drill through data, discover compelling insights, and share the right visuals. The Action Framework enables Salesforce users to take actions directly at the point of insight from within any Einstein Analytics dashboard. | | | | | | | | | | |
| TEC-15 | Describe the help desk operations and support that will be provided with the system. | X | | X | | | |  | |  |
| Response:  **Salesforce Premier+ Success Plan**  Based on your requirements, we are proposing Premier+ Success Plan for the State, which is included as of the overall license subscription we are proposing. The Premier+ Success Plan provides priority case routing, 1-hour response time for critical issues, 24x7 phone support, unlimited usage of our entire online course library, and access to a team of expert Salesforce administrators.  Benefits of the Premier+ Success Plan include:   * 24x7 toll-free phone support * Priority case queuing and routing * Quick initial 1-hour response time for critical issues * On-demand training for administrators, developers, and end users via Trailhead * Access to our pool of Salesforce Certified Administrators who can configure and maintain your Salesforce edition * Access to a library of more than 90 Premier Accelerators (1-on-1 coaching sessions with Salesforce experts help you take advantage of key Salesforce capabilities) * Around-the-clock access to an online, searchable knowledge base, with answers to the most commonly asked support questions * Ability to ask questions and get answers from the Success Community, a thriving hub of Salesforce partners, experts, and customers * Access to Success Managers that are product and market experts who assist with Salesforce product adoption and utilization * Ability to boost productivity with Premier Apps - apps are developed, supported, and maintained by Salesforce to help you automate key features, find the right answers, reduce support cases, and get the most out of Salesforce * Access to Circle of Success interactive group discussions to learn best practices or troubleshoot situations with peers * Developer Support * Premier Success Review to measure usage and trends * More than 100 administrative services * Ability to participate in exclusive events where you can learn best practices and strategies with Salesforce experts   For the Premier+ Success plan terms and conditions, please see:<https://c1.sfdcstatic.com/content/dam/web/en_us/www/documents/legal/Agreements/salesforce-premierplans-with-accelerators-20171130.pdf>.  The Salesforce Government Cloud requires the Government Cloud Premier+ Success Plan, which provides technical support from Qualified US Citizens. Subject to the Government Cloud Premier+ Success Plan, access to systems and permissions which could permit access to Customer Data inside of the Salesforce Government Cloud storing U.S. government, U.S. government contractors, and FFRDC Customer Data will be restricted to Qualified U.S. Citizens. Qualified US Citizens are individuals who are United States citizens and are physically located within the United States when accessing the Salesforce Government Cloud systems; and have completed a background check as a condition of their employment with Salesforce. | | | | | | | | | | |

***Standards Requirements***

DHHS currently operates its computer system in compliance with many technology and operational standards. These standards originate from internal development, industry best practices and governmental mandates. The Bidder must describe how all applications operate in compliance with these standards and practices.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Req #** | **Requirement** | (1) Comply | (a) Core | (b) Custom | (c) 3rd Party |
| STN-1 | If web-based system applications are required, describe what industry standard browsers are supported by the system. If the system requires additional components, describe the technical details of those components. | X | X |  |  |
| Response:  **100% Multi-Tenant, Cloud Application**  Salesforce offers the market leading Platform as a Service (PaaS) and market leading Software as a Service (SaaS) solutions.  Salesforce is a multi-tenant, cloud-based web application. No additional software or infrastructure is required. Salesforce hosts the entire solution, thus freeing up the State to manage its mission, not manage an infrastructure solution. Additionally, Salesforce is browser agnostic and supports all major browsers (Firefox, Chrome, Safari, IE, Edge). No installations on users’ laptops or desktops are required and thus the solution is accessible from anywhere an internet connection and supported browser are available, including mobile devices.  The fully documented list of supported browsers and mobile devices for the full Salesforce site and Salesforce Mobile is available in the following articles in online our Help & Training Portal: <https://help.salesforce.com/HTViewHelpDoc?id=getstart_browser_overview.htm&language=en_US> and <https://help.salesforce.com/articleView?id=sf1_requirements.htm&type=0&language=en_US&release=206.5>. | | | | | |
| STN-2 | The system must store data in federally compliant data centers residing within the continental United States of America. | X | X |  |  |
| Response:  The Salesforce Government Cloud hosts and stores all data within the United States.  Salesforce was the first Cloud Service Provider granted a FedRAMP Authority to Operate (ATO) for both Software as a Service (SaaS) and Platform as a Service (PaaS), consistent with the FedRAMP moderate baseline controls.    On May 23, 2014 Salesforce was granted a FedRAMP ATO at the moderate impact level issued by the Department of Health and Human Services (HHS) for the Salesforce Government Cloud. Testing for the ATO was performed by a third-party assessment organization (3PAO).    The Salesforce Government Cloud information system and authorization boundary, is comprised of the Salesforce Platform\*, Sales, Service, Communities, Analytics, Salesforce Mobile, and Industry Solutions, as well as the backend infrastructure (e.g., servers, network devices, databases, storage arrays) that support the operations of these products, referred to as the General Support System (GSS).    To obtain compliance with FedRAMP, Salesforce conducted security assessment and authorization activities in accordance with FedRAMP guidance, NIST SP 800-37, and HHS requirements. As part of this process Salesforce documented a System Security Plan (SSP) for the Salesforce Government Cloud service offering. The SSP is developed in accordance with NIST SP 800-18. The SSP identifies control implementations for the GSS and in-scope customer facing products (e.g., Lightning Platform, applicable Salesforce Services) according to the FedRAMP moderate baseline and HHS security control parameters. A security assessment of the information system was conducted by a 3PAO in accordance with FedRAMP Moderate requirements. The security assessment testing determined the adequacy of the management, operational, and technical security controls used to protect the confidentiality, integrity, and availability of Salesforce's Government Cloud service offering and the Customer Data it stores, transmits and processes.    To maintain compliance with FedRAMP, Salesforce conducts continuous monitoring, which includes ongoing technical vulnerability detection, remediation of open compliance related findings, and at least annual independent assessment of security controls by a 3PAO. As part of the current FedRAMP annual assessment, Salesforce is aligned with NIST SP 800-53 Revision 4.    Government Cloud eligible non-U.S. Federal Government authorizing officials and customers can request the below Salesforce Government Cloud FedRAMP materials after completing applicable NDAs:   * Partner System Security Plan * Control Implementation Summary/Customer Responsibility Matrix * Customer Configuration User Guide * Disaster Recovery Plan (DRP) * Incident Response Plan (IRP) * FedRAMP Authority to Operate (ATO) Letter   For more information on the Salesforce Government Cloud please see the [Salesforce Government Cloud whitepaper](https://org62.my.salesforce.com/sfc/p/#000000000062/a/0M000000Q8ar/moggeD49GPYM4jsNqrIjHnLlcqW7Zc7VwHfyKfuEmbs).    \*Only the Salesforce Platform is included within the FedRAMP Authorization Boundary for the Salesforce Government Cloud.    For more information on the Salesforce Government cloud please see the Salesforce Government Cloud white paper: <https://org62.my.salesforce.com/sfc/p/000000000062/a/0M000000Q8ar/moggeD49GPYM4jsNqrIjHnLlcqW7Zc7VwHfyKfuEmbs>. | | | | | |
| STN-3 | All data is the property of DHHS, and DHHS will retain the exclusive rights of use now and in perpetuity. | X | X |  |  |
| Response:  We are proposing a cloud-based SaaS solution that will be configured to meet the State’s specific requirements. Salesforce is not creating any new Intellectual Property for the State. The State retains ownership of their data and artifacts at all times. Data and artifacts can be exported using scheduling capabilities, or on demand. In the event of an export, all data visibility and record access rules are enforced, and the requestor only obtains the data allowed under the State’s security policy. | | | | | |
| STN-4 | The system must comply with accessibility requirements described in 45 CFR 85 and with State of Nebraska accessibility requirements located at: <https://nitc.nebraska.gov/standards/2-101.pdf>. | X | X |  |  |
| Response:  We will ensure that any custom pages developed within the Salesforce community using Lightning components comply with the WCAG 2.0 Level AA standards.  Salesforce is committed to providing on-demand enterprise applications accessible to all individuals. This includes users working with assistive technology, such as speech recognition software and screen readers. To help meet our goal of accessible design, Salesforce follows the internationally recognized best practices in Section 508 of the Rehabilitation Act and the Web Content Accessibility Guidelines (WCAG) 2.0 Level AA.  Salesforce introduced the Lightning User Experience, which brings a re-imagined user interface that is modern, efficient, and highly accessible. The Lightning Experience is engineered with Accessible Rich Internet Application (ARIA) features built in that help assistive technology users have the best possible experience with Salesforce. We provide software releases three times a year, ensuring that our customers can easily take advantage of the accessibility features introduced in each release.  The Salesforce Lightning Experience Voluntary Product Accessibility Template (<http://salesforce.com/company/legal/508_accessibility.jsp>) serves as a guide in evaluating conformance to Section 508 of the Rehabilitation Act and WCAG within Salesforce Lightning Experience UI. The accessibility features available within Salesforce applications are dependent on the application UI configuration and Lightning component usage. For this reason, adherence to accessibility requirements should be evaluated throughout the design and final testing of the Salesforce application and not merely on a specific VPAT.  The VPATs are encompassing of the features and functions of Salesforce products and provide an explanation of supporting features. If required, Salesforce will make itself available to review the VPAT and features with the State's Accessibility team to determine the requirements and our ability to ensure accessibility.  Copies of VPATs are available on the Salesforce website at: <https://www.salesforce.com/company/legal/508_accessibility.jsp>. As new or additional VPATs become available, they will be posted to the Salesforce website.  Additional accessibility details can be found at: <https://help.salesforce.com/articleView?id=accessibility_overview.htm&type=5> and <https://www.lightningdesignsystem.com/accessibility/overview/>. | | | | | |
| STN-5 | The system must comply with the sub-parts of Section 508 of the Americans with Disabilities Act (ADA), and any other applicable State or federal disability legislation. Refer to <http://www.ada.gov/508/>. | X | X |  |  |
| Response:  Salesforce is committed to providing on-demand enterprise applications accessible to all individuals. This includes users working with assistive technology, such as speech recognition software and screen readers. To help meet our goal of accessible design, Salesforce follows the internationally recognized best practices in Section 508 of the Rehabilitation Act and the Web Content Accessibility Guidelines (WCAG) 2.0 Level AA. | | | | | |
| STN-6 | Describe how the system complies with digital signature requirements described in the Nebraska Digital Signatures Act, and all other applicable legal requirements in Nebraska for digital signatures. Refer to <http://www.sos.ne.gov/rules-and-regs/regsearch/Rules/Secretary_of_State/Title-437.pdf> for definition and standards in Nebraska. | X | X |  |  |
| Response:  We will be integrating DocuSign app with Salesforce. DocuSign signature is the tested solution that works well with Salesforce and provides standard built in signature component that can be used in Salesforce community. | | | | | |
| STN-7 | The system must comply with all HIPAA and other statutory, regulatory, and policy requirements for protected health information. Refer to <http://dhhs.ne.gov/ITSecurity>. | X | X |  |  |
| Response:  Salesforce's customers are responsible for complying with HIPAA's Privacy Rule and Security and the HITECH Act in their capacity as a covered entity or business associate using the Salesforce services. The services' features permit customers to customize use as per a compliance program for HIPAA (including the HITECH Act) and many customers store protected health information (PHI) on our service. Salesforce can assist customers with their compliance obligations; for example, by discussing entering into business associate agreements (BAA) to address formal legal requirements pertaining to use and disclosure of protected health information (PHI).    Salesforce regularly signs Business Associate Agreements as required by HIPAA, which your licensing attorney can put in place as an addendum to a Master Subscription Agreement (MSA). This document includes details regarding how we comply with requirements under HIPAA and HITECH, including the Privacy Rule, Security Rule, and breach notification requirements. | | | | | |
| STN-8 | If the system requires client software to be installed, describe how the system ensures that all software used for the system can be distributed, installed and configured in an unattended "silent" manner. | X | X |  |  |
| Response:  Not applicable. Salesforce is a multi-tenant, cloud-based web application. No additional software or infrastructure is required. Salesforce hosts the entire solution, thus freeing up the State to manage its mission, not manage an infrastructure solution. Additionally, Salesforce is browser agnostic and supports all major browsers (Firefox, Chrome, Safari, IE, Edge). No installations on users’ laptops or desktops are required and thus the solution is accessible from anywhere an internet connection and supported browser are available, including mobile devices.  **Upgrades**  All upgrades, patches, and other system maintenance are provided as part of the subscription service with no additional cost to the State. In addition, Salesforce releases 3 complimentary upgrades each year, in Winter, Spring, and Summer versions. All Salesforce users are always on the latest version of our platform because everyone gets instant upgrades (typically on an opt-in basis). Each time Salesforce releases a new version of the application and the platform, the entire community can take advantage of the latest innovations from our product development team. Because of our multi-tenant architecture, Salesforce is able to provide all of our customers with a service based on a single version of our application. We are able to upgrade all of our customers at the same time with each release. As a result, we do not have to maintain multiple versions of our application. Each release will be delivered automatically in a transparent manner and will not break your configurations. | | | | | |
| STN-9 | Current DHHS policies prevent users from making administrative changes and downloading software locally to their PC. Describe how the system supports this policy. | X | X |  |  |
|  | | | | | |
| Response:  **User Profiles**  All users and application-level security are defined and maintained by the organization administrator, and not by Salesforce. The organization administrator is appointed by the customer. An organization's sharing model sets the default access that users have to each other's data.    There are four sharing models: Private, Public Read Only, Public Read/Write, and Public Read/Write/Transfer. There are also several sharing model elements: Profiles, Roles, Hierarchy, Record Types, Page Layouts, and Field-Level security. Details about sharing models and sharing model elements are provided below:    Private  Only the record owner, and users above that role in the hierarchy, can view, edit, and report on those records.    Public Read Only  All users can view and report on records but not edit them. Only the owner, and users above that role in the hierarchy, can edit those records.    Public Read/Write  All users can view, edit, and report on all records.    Public Read/Write/Transfer  All users can view, edit, transfer, and report on all records. Only available for cases or leads.    Profiles  A profile contains the settings and permissions that control what users with that profile can do within Salesforce. Profiles control:   * Standard and custom apps the user can view (depending on user license) * Service providers the user can access * Tabs the user can view (depending on user license and other factors, such as access to Salesforce CRM Content) * Administrative and general permissions the user has for managing the organization and apps within it * Object permissions the user is granted to create, read, edit, and delete records * Page layouts a user sees * Field-level security access that the user has to view and edit specific fields * Record types are available to the user * Desktop clients users can access and related options * Hours during which and IP addresses from which the user can log in * Apex classes a user can execute * Visualforce pages a user can access     User Roles  Every user must be assigned to a role, or their data will not display in reports and other displays based on roles. All users that require visibility to the entire organization should be assigned the highest level in the hierarchy. It is not necessary to create individual roles for each title at the organization, rather a hierarchy of roles should be defined to control access of information entered by users in lower level roles. When a user's role is changed, any relevant sharing rules are reevaluated to add or remove access as necessary.    Record Types  If the customer's organization uses record types, edit the record type to modify which pick list values are visible for the record type. A default pick list values can be set based upon the record type for various divisions.    Field-Level Security  Field-level security settings let administrators restrict user's access to view and edit specific fields on detail and edit pages and in related lists, list views, reports, Offline Edition, search results, email and mail merge templates, Custom Links, and when synchronizing data.    The fields that users see in detail and edit pages are a combination of page layouts and field-level security settings. The most restrictive field access settings of the two always apply. For example, if a field is required in the page layout and read-only in the field-level security settings, the field-level security overrides the page layout and the field will be read-only for the user.    Permission Sets  A permission set is a collection of settings and permissions that give users access to various tools and functions. The settings and permissions in permission sets are also found in profiles, but permission sets extend users’ functional access without changing their profiles.    Users can have only one profile but, depending on the Salesforce edition, they can have multiple permission sets. You can assign permission sets to various types of users, regardless of their profiles. The State can create permission sets to grant access among logical groupings of users, regardless of their primary job function.    See more information at: <https://help.salesforce.com/articleView?id=perm_sets_overview.htm&type=5>. | | | | | |
| STN-10 | Current DHHS policies recommend not storing any data locally in the event that a user's desktop PC needs to be reimaged (which deletes locally stored data). Describe how the system supports this policy. | X | X |  |  |
| Response:  Not applicable. Salesforce is a multi-tenant, web-based, cloud application. | | | | | |
| STN-11 | Describe the report design tools and output formats. | X | X |  |  |
| Response:  **Core Reports & Dashboards**  Salesforce offers a powerful suite of analytics and reporting tools to help you view and analyze your data. Salesforce analytics consists of several integrated parts:    **Report Types**  A report type defines the set of records and fields available to a report based on the relationships between a primary object and its related objects. Reports display only records that meet the criteria defined in the report type. Salesforce provides a set of pre-defined standard report types; administrators can create custom report types as well. For example, an administrator can create a report type that shows only job applications that have an associated resume; applications without resumes won't show up in reports using that type. An administrator can also show records that may have related records—for example, applications with or without resumes. In this case, all applications, whether or not they have resumes, are available to reports using that type.    Report Formats  Salesforce reports can use the tabular, summary, matrix, or joined format:  *Tabular reports* are the simplest and fastest way to look at data. Similar to a spreadsheet, they consist simply of an ordered set of fields in columns, with each matching record listed in a row. Tabular reports are best for creating lists of records or a list with a single grand total. Examples include contact mailing lists and activity reports.  *Summary reports* are similar to tabular reports, but also allow users to group rows of data, view subtotals, and create charts. They can be used as the source report for dashboard components. This type of report can be used to show subtotals based on the value of a particular field or when a hierarchical list is desired, such as all Cases for your team, subtotaled by Status and Owner.  *Matrix reports* are similar to summary reports but allow users to group and summarize data by both rows and columns. This type of report can be used for comparing related totals, especially if there are large amounts of data to summarize and users need to compare values in several different fields, or users want to look at data by date and by type, person, or geography.  *Joined reports* let users create multiple report blocks that provide different views of the data. Each block acts like a “sub-report,” with its own fields, columns, sorting, and filtering. A joined report can even contain data from different report types.  *Tableau visualizations* give you a new way to see and understand your data. These are very strong in showing visual aspects of your data to quickly convey the importance of certain values and outliers.  Reports  A report returns a set of records that meets certain criteria, and displays it in organized rows and columns. Report data can be filtered, grouped, and displayed graphically as a chart. Reports are stored in folders, which control who has access. To help you monitor the State, Salesforce offers a wide range of standard reports, accessible in the standard reports folders on the Reports tab. All our standard reports are "templates" so they can be used as report starting points from which users can alter fields, criteria, etc. and use the "Save As" function to easily capture a version more specific to their unique needs. Users can also create new custom reports to access exactly the information they need. Subtotal and limit data to help users analyze trends and get a concise picture of what is happening in the State.      *Figures: Example Salesforce Report for YTD Service Cases initiated from a customer on the Salesforce Customer Community web portal*    *A Tableau visualization with a fictitious example of abuse victims*  Report performance varies by report complexity, including the number of table joins required to produce report results. Most customer reports are executed in just a few seconds. There are some factors that can cause a report to perform poorly or to time out. Most of them can be addressed by simple changes, such as using the correct filter operators, increasing the number of filters, and reducing the amount of data.View Salesforce's Tutorial on Creating Reports with the Report Builder in Trailhead:  <https://trailhead.salesforce.com/en/modules/reports_dashboards/units/reports_dashboards_getting_started>.    Dashboards  A dashboard shows data from source reports as visual components, which can be charts, gauges, tables, metrics, or custom Visualforce pages. They provide a snapshot of key metrics and performance indicators for the State. Each dashboard can have up to 20 components. Administrators control access to dashboards by storing them in folders with certain visibility settings. Dashboard folders can be public, hidden, or restricted to groups, roles, or territories. If you have access to a folder, you can view its dashboards. To view a dashboard component, users need access to the folder for the underlying source report. Each dashboard has a running user, whose security settings determine which data to display in a dashboard. Your Data with the Lightning Dashboard Builder in Trailhead: <https://trailhead.salesforce.com/modules/lex_implementation_reports_dashboards/units/lex_implementation_reports_dashboards_visualizing_data>.    *Figure: Example customer service dashboard*    *A Tableau visualization with a fictitious example of abuse victims*    Folders  A folder is a place where you can store reports, dashboards, documents, or email templates. Folders can be public, hidden, or shared, and can be set to read-only or read/write. You control who has access to its contents based on roles, permissions, public groups, and license types. You can make a folder available to your entire organization, or make it private so that only the owner has access. \*Help article regarding upcoming retirement of Legacy Folder Sharing: <https://help.salesforce.com/articleView?id=000321245&type=1&mode=1&language=en_US>.    Analytic Snapshots  An analytic snapshot lets you report on historical data. Authorized users can save tabular or summary report results as snapshots on a schedule. Analytic snapshots let you to work with report data similarly to how you work with other records in Salesforce.com. For example, a customer support manager could set up an analytic snapshot that reports on the open cases assigned to his or her team every day at 5:00 PM, and store that data in a custom object to build a history on open cases from which he or she could spot trends via reports. Then the customer support manager could report on point-in-time or trend data stored in the custom object and use the report as a source for a dashboard component.    Other important points about dashboards:   * Dashboard components aren’t simply nice-looking, static pictures. They’re live, actionable objects. You can click on a dashboard component to drill down to the underlying report that generated it, and click on any item in that report to drill down to the source data. So you can quickly understand the reasons behind the results. * Dashboards are full participants in Salesforce’s enterprise social collaboration platform. For example, a manager could post a dashboard snapshot to their Chatter feed to share it with their “followers”, or to a specific Chatter group, along with comments, so that they can find answers, congratulate team members, or issue calls to action. And both dashboards and Chatter are available on mobile devices, as well as PCs. * Salesforce Reports and Dashboards allows users to configure reports in the Lightning Report Builder and add to a new and/or existing dashboard with the click of one button. Dashboard settings for reports can be maintained from the chart settings of a report.     **Tableau Visual Analytics**  Live visual analytics fuel unlimited data exploration. Interactive dashboards help you uncover hidden insights on the fly. Tableau harnesses people’s [natural ability to spot visual patterns](https://www.tableau.com/about/mission#breakthrough) quickly, revealing everyday opportunities and eureka moments alike.  Connect to data on premise or in the cloud—whether it’s big data, a SQL database, a spreadsheet, or cloud apps like Google Analytics and Salesforce. Access and combine disparate data without writing code. Power users can pivot, split, and manage metadata to optimize data sources. Analysis begins with data. Get more from yours with  Tableau.  Quickly build powerful calculations from existing data, drag and drop reference lines and forecasts, and review statistical summaries. Make your point with trend analyses, regressions, and correlations for tried and true statistical understanding. Ask new questions, spot trends, identify opportunities, and make data-driven decisions with confidence.  Create interactive maps automatically. Built-in postal codes mean lightning-fast mapping for more than 50 countries worldwide. Use custom geocodes and territories for personalized regions, like sales areas. We designed [Tableau maps](https://www.tableau.com/stories/topic/maps) specifically to help your data stand out.  **Einstein Analytics**  Einstein Analytics is a cloud-based platform designed for the business user to get answers to questions instantly through powerful, interactive visualizations of any data, on any device.    Salesforce core Reports and Dashboards deliver operational and performance metrics on data that lives solely in Salesforce and allows the State to easily create individual static reports and dashboards to gain real-time views of daily activity.    Einstein Analytics is an analytics system - designed to analyze data not just from within Salesforce, but from across different sources, and be surfaced across the State. More importantly, it is designed to engage users every day by embedding analytics in business processes — a native tab in the business system and on the home page, or an interactive component on your account page or object page.    Einstein Analytics complements native Salesforce Reports and Dashboard by providing:   * Multi-year trending analysis - Supports query and processing of hundreds of millions of rows of data from various sources * Cross Object analysis and faceting * Rich data visualization, including thematic maps     Finally, Einstein Analytics is designed to be API-first. And with the Analytics Web SDK you can extend functionality across Salesforce Lightning or any third-party website.    Einstein Analytics offers:   * Collaboration: Leveraging annotations, sharing and notifications * Actions: Configure Actions with few clicks * Self-service: True, unhindered explorations   Within the State, you may have data everywhere: warehouses, spreadsheets, logs, and in Salesforce. With Einstein Analytics, it’s easy to integrate data from any of these sources, including external data such as SAP or Oracle data, mobile app data, or product sensor data.  With Einstein Analytics, the State will gain powerful interactive visualization tools with a fast, fluid way to drill through data, discover compelling insights, and share the right visuals. The Action Framework enables Salesforce users to take actions directly at the point of insight from within any Einstein Analytics dashboard. | | | | | |
| STN-12 | Describe how the system maintains licensed software, including all third-party software, no more than two supported versions behind the latest release, and updated with latest security patches. | x | X |  |  |
| Response:  All upgrades, patches, and other system maintenance are provided as part of the subscription service with no additional cost to the State. In addition, Salesforce releases 3 complimentary upgrades each year, in Winter, Spring, and Summer versions. All Salesforce users are always on the latest version of our platform because everyone gets instant upgrades (typically on an opt-in basis). Each time Salesforce releases a new version of the application and the platform, the entire community can take advantage of the latest innovations from our product development team. Because of our multi-tenant architecture, Salesforce is able to provide all of our customers with a service based on a single version of our application. We are able to upgrade all of our customers at the same time with each release. As a result, we do not have to maintain multiple versions of our application. Each release will be delivered automatically in a transparent manner, and will not break your configurations. | | | | | |

***Error Handling Requirements***

The management of the system requires that all occurrences of errors be logged for review and that critical errors be accompanied by appropriate alerts. Authorized users need to be able to query and review the error log and configure the alerts.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Req #** | **Requirement** | (1) Comply | (a) Core | (b) Custom | (c) 3rd Party |
| ERR-1 | Describe the error handling functionality. | X | X |  |  |
| Response:  **Data Validation**  Within the State’s organization, the administrator and project sponsor are responsible for monitoring proper data entry. Using pick list fields extensively in the application helps to minimize poor data entry. The Salesforce application is built on a relational database. Relational databases help ensure the integrity of the data model. In addition, field validations and the application itself help ensure data integrity. Salesforce offers many features to ensure the capture of effective and relevant customer data. The system offers features such as validation rules with red-highlighted error messages, administrator-defined field picklists, field default values, required fields, and bubble help text on data entry screens. Additionally, we provide field history tracking that records all field changes, with user, date and changed value, for selected tracking fields.    Refer to this Help & Training article for additional information on Validation Rules: <https://help.salesforce.com/apex/HTViewHelpDoc?id=fields_defining_field_validation_rules.htm&language=en>. | | | | | |
| ERR-2 | Describe how the system provides a comprehensive set of edits at the point of data entry to minimize data errors and provide immediate feedback in order for incorrect data to be corrected before further processing (e.g., spell check, zip codes, etc.). | X | X |  |  |
| Response:  Salesforce offers many features to ensure the capture of effective and relevant customer data. The system offers features such as validation rules with red-highlighted error messages, administrator-defined field picklists, field default values, required fields, and bubble help text on data entry screens. Additionally, we provide field history tracking that records all field changes, with user, date and changed value, for selected tracking fields.    These are the most common attributes of Salesforce fields:   * All entity names must be non-null * All dates and times must be parsable with respect to the user's chosen locale setting * All email addresses must contain an '@' symbol * US-style phone numbers with 10 digits are formatted as (xxx) xxx-xxxx. | | | | | |
| ERR-3 | Describe how the system ensures all errors are written and categorized to an error log. Describe how the system allows for a user to view, filter, sort, and search the error log. | X |  |  |  |
| Response:  Within the State’s organization, the administrator and project sponsor are responsible for monitoring proper data entry. Using pick list fields extensively in the application helps to minimize poor data entry. The Salesforce application is built on a relational database. Relational databases help ensure the integrity of the data model. In addition, field validations and the application itself help ensure data integrity. Salesforce offers many features to ensure the capture of effective and relevant customer data. The system offers features such as validation rules with red-highlighted error messages, administrator-defined field picklists, field default values, required fields, and bubble help text on data entry screens. Additionally, we provide field history tracking that records all field changes, with user, date and changed value, for selected tracking fields.    Refer to this Help & Training article for additional information on Validation Rules: <https://help.salesforce.com/apex/HTViewHelpDoc?id=fields_defining_field_validation_rules.htm&language=en>. | | | | | |
| ERR-4 | Describe how the system allows for user-defined alerts of errors, including those to external communication mechanisms (e.g., e-mail and text messaging). | X | X |  |  |
| Response:  Salesforce allows you to configure time-based workflows that automatically trigger reminders and even re-routes when the workflow ages    Email alerts are emails generated by an automated process and sent to designated recipients. These actions consist of the standard text and list of recipients for an email. You can associate email alerts with processes, flows, workflow rules, approval processes, or entitlement processes. | | | | | |
| ERR-5 | Describe how the system provides for the generation of standard and customizable error reports. | X |  |  |  |
| Response:  Within the State’s organization, the administrator and project sponsor are responsible for monitoring proper data entry. Using pick list fields extensively in the application helps to minimize poor data entry. The Salesforce application is built on a relational database. Relational databases help ensure the integrity of the data model. In addition, field validations and the application itself help ensure data integrity. Salesforce offers many features to ensure the capture of effective and relevant customer data. The system offers features such as validation rules with red-highlighted error messages, administrator-defined field picklists, field default values, required fields, and bubble help text on data entry screens. Additionally, we provide field history tracking that records all field changes, with user, date and changed value, for selected tracking fields.    Refer to this Help & Training article for additional information on Validation Rules: <https://help.salesforce.com/apex/HTViewHelpDoc?id=fields_defining_field_validation_rules.htm&language=en>. | | | | | |
| ERR-6 | Describe how the system includes a comprehensive list of error messages with unique message identifiers. | X | X |  |  |
| Response:  Within the State’s organization, the administrator and project sponsor are responsible for monitoring proper data entry and are highly capable of doing so based on Salesforce’ inherent data quality tools and error message handling.. Using pick list fields extensively in the application helps to minimize poor data entry. The Salesforce application is built on a relational database. Relational databases help ensure the integrity of the data model. In addition, field validations and the application itself help ensure data integrity. Salesforce offers many features to ensure the capture of effective and relevant customer data. The system offers features such as validation rules with red-highlighted error messages, administrator-defined field picklists, field default values, required fields, and bubble help text on data entry screens. Additionally, we provide field history tracking that records all field changes, with user, date and changed value, for selected tracking fields.    Refer to this Help & Training article for additional information on Validation Rules: <https://help.salesforce.com/apex/HTViewHelpDoc?id=fields_defining_field_validation_rules.htm&language=en>. | | | | | |
| ERR-7 | Describe how the system displays errors to the user/operator in real-time whenever an error is encountered. | X | X |  |  |
| Response:  Error handling is provided clearly and intuitively at the user interaction level. Within the State’s organization, the administrator and project sponsor are responsible for monitoring proper data entry. Using pick list fields extensively in the application helps to minimize poor data entry. The Salesforce application is built on a relational database. Relational databases help ensure the integrity of the data model. In addition, field validations and the application itself help ensure data integrity. Salesforce offers many features to ensure the capture of effective and relevant customer data. The system offers features such as validation rules with red-highlighted error messages, administrator-defined field picklists, field default values, required fields, and bubble help text on data entry screens. Additionally, we provide field history tracking that records all field changes, with user, date and changed value, for selected tracking fields.    Refer to this Help & Training article for additional information on Validation Rules: <https://help.salesforce.com/apex/HTViewHelpDoc?id=fields_defining_field_validation_rules.htm&language=en>. | | | | | |
| ERR-8 | Describe how the system has the ability to suppress error messages based upon user-defined criteria. | X |  |  |  |
| Response:  Salesforce has the capability to user-based error messaging which means the errors and data entry/security requirements are configured based on a user profile and down to the field itself. Within the State’s organization, the administrator and project sponsor are responsible for monitoring proper data entry. Using pick list fields extensively in the application helps to minimize poor data entry. The Salesforce application is built on a relational database. Relational databases help ensure the integrity of the data model. In addition, field validations and the application itself help ensure data integrity. Salesforce offers many features to ensure the capture of effective and relevant customer data. The system offers features such as validation rules with red-highlighted error messages, administrator-defined field picklists, field default values, required fields, and bubble help text on data entry screens. Additionally, we provide field history tracking that records all field changes, with user, date and changed value, for selected tracking fields.    Refer to this Help & Training article for additional information on Validation Rules: <https://help.salesforce.com/apex/HTViewHelpDoc?id=fields_defining_field_validation_rules.htm&language=en>. | | | | | |

***Database/Data Management Requirements***

DHHS requires the benefits inherent with a relational database management system (RDBMS). The accessibility, flexibility and maintainability achieved through normalized data structures are essential to achieving the business objectives outlined in this RFP.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Req #** | **Requirement** | (1) Comply | (a) Core | (b) Custom | (c) 3rd Party |
| DBM-1 | Describe the database architecture, including the database software that is supported by the system. | X | X |  |  |
| Response:  Salesforce Lightning Platform’s core technology uses a runtime engine that materializes all application data from metadata—data about the data itself. In Salesforce Lightning Platform’s well-defined metadata-driven architecture, there is a clear separation of the compiled runtime database engine (kernel), tenant data, and the metadata that describes each application. These distinct boundaries make it possible to independently update the system kernel and tenant-specific applications and schemas, with virtually no risk of one affecting the others.    Every logical database object that Salesforce exposes is internally managed using metadata. Objects, (tables in traditional relational database parlance), fields, stored procedures, and database triggers are all abstract constructs that exist merely as metadata in Salesforce Lightning Platform’s Universal Data Dictionary (UDD). For example, when you define a new application object or write some procedural code, Salesforce does not create an actual table in a database or compile any code. Instead, Salesforce simply stores metadata that the system’s engine can use to generate the virtual application components at runtime. When you need to modify or customize something about the application schema, like modify an existing field in an object, all that’s required is a simple non-blocking update to the corresponding metadata.  Because metadata is a key ingredient of Salesforce applications, the system’s runtime engine must optimize access to metadata; otherwise, frequent metadata access would prevent the service from scaling. With this potential bottleneck in mind, Salesforce uses massive and sophisticated metadata caches to maintain the most recently used metadata in memory, avoid performance-sapping disk I/O and code recompilations, and improve application response times.  The multitenant architecture and secure logical controls address separation of Customer Data. The Salesforce infrastructure is divided into a modular architecture based on “instances”. Each instance is capable of supporting several thousand customers in a secure and efficient manner. Salesforce uses the instance architecture to continue to scale and meet the demands of our customers. There are appropriate controls in place designed to prevent any given customer’s Salesforce instance from being compromised. This functionality has been designed and undergoes robust testing through an on-going process by both Salesforce and its customers.    These papers further explain the technology that makes the Salesforce Lightning Platform fast, scalable, and secure for any type of application:  <https://developer.salesforce.com/page/Multi_Tenant_Architecture>  <https://developer.salesforce.com/page/Secure_Private_Trustworthy_Force.com_Whitepaper>  <https://developer.salesforce.com/page/An_Overview_of_Force.com_Security> | | | | | |
| DBM-2 | Describe how the system allows changes to be made available immediately on-line. | X | X |  |  |
| Response:  **Design Your Own Data Model**  Schema Builder provides a dynamic environment for viewing and modifying all the objects and relationships in your app. This greatly simplifies the task of designing, implementing, and modifying your data model, or schema. Schema Builder is great for visualization, but you can also use it to customize your data model. For example, you can manage the permissions for your custom fields directly in Schema Builder. Just right-click the field name and click Manage Field Permissions. You can also create objects using Schema Builder. You can drag these objects around the canvas. This doesn’t change your objects or relationships, but it can help you visualize your data model in a useful way. Schema Builder is a handy tool for introducing your Salesforce customizations to a co-worker or explaining the way data flows throughout your system. View more information at:<https://help.salesforce.com/articleView?id=schema_builder.htm&type=5>.  **Configuration vs. Customization**  Salesforce offers the State a scalable, no-code, low-code development platform that will allow you to quickly develop and deploy a solution for the State. Salesforce’s low-code development platform promotes configuration over custom code, coupled with a market leading user experience for the State’s end users.  Salesforce's best practice is to have solutions that are 80 percent, or more, configuration based with the remaining functionality being customizations. In an ideal setting a solution would be 90 percent configuration. Regardless of the development approach, the State should aim to achieve this goal even if it means reengineering existing business processes.    It is important to note that not all vendor solutions define approaches to out of the box, configuration, and customization of their software the same way. Additionally, third party products are pre-built solutions powered and integrated with the Salesforce Platform.    For example, the State may require custom fields for your solution. In order to meet this requirement, some vendors need to actually program “code or physically extend their RDBMS schema with non-programming “configuration tools"; and some vendors, like Salesforce, have pre-built “Administration Screens” where systems administrators or business analysts can go to quickly add new fields, pick list values, workflows, create users, add validation rules, etc. through a simple wizard-based point and click interface and system setup parameters. Salesforce considers these types of common system changes to be “administrative” changes rather than “configuration” or “programming”.    The Salesforce Platform allows customers to build apps fast with just a few clicks, designed for desktop and mobile devices, all from a single canvas, including pre-built AppExchange solutions. To help IT deliver apps faster, the Salesforce Platform offers a simple yet powerful set of declarative, point-and-click tools that anyone can use to achieve business goals at lightning speed. Without writing code, developers and business users alike can quickly and easily create custom apps on the Salesforce Platform with complex business logic and beautiful user interfaces designed specific to every screen. Salesforce Lightning Builder tools allow the State to work in alignment with agile development methodologies as IT meets business demands faster.    If and where it may be needed, Developers can leverage the Apex programming language. Apex is an object-oriented, on-demand language. It is like Java, with similar syntax and notation, and is strongly-typed, compiled on demand, and fully integrated into the Platform. All of the application services come right out of the box, from a powerful workflow engine to API services, integration services, authentication, event log framework, analytics, and collaboration. | | | | | |
| DBM-3 | Describe how the system facilitates data structure changes to accommodate expanding scope, new services, changing requirements and legislative mandates. | X | X |  |  |
| Response:  **Configuration vs. Customization**  Salesforce offers the State a scalable, no-code, low-code development platform that will allow you to quickly develop and deploy a solution for the State. Salesforce’s low-code development platform promotes configuration over custom code, coupled with a market leading user experience for the State’s end users.  Salesforce's best practice is to have solutions that are 80 percent, or more, configuration based with the remaining functionality being customizations. In an ideal setting a solution would be 90 percent configuration. Regardless of the development approach, the State should aim to achieve this goal even if it means reengineering existing business processes.    It is important to note that not all vendor solutions define approaches to out of the box, configuration, and customization of their software the same way. Additionally, third party products are pre-built solutions powered and integrated with the Salesforce Platform.    For example, the State may require custom fields for your solution. In order to meet this requirement, some vendors need to actually program “code or physically extend their RDBMS schema with non-programming “configuration tools"; and some vendors, like Salesforce, have pre-built “Administration Screens” where systems administrators or business analysts can go to quickly add new fields, pick list values, workflows, create users, add validation rules, etc. through a simple wizard-based point and click interface and system setup parameters. Salesforce considers these types of common system changes to be “administrative” changes rather than “configuration” or “programming”.    The Salesforce Platform allows customers to build apps fast with just a few clicks, designed for desktop and mobile devices, all from a single canvas, including pre-built AppExchange solutions. To help IT deliver apps faster, the Salesforce Platform offers a simple yet powerful set of declarative, point-and-click tools that anyone can use to achieve business goals at lightning speed. Without writing code, developers and business users alike can quickly and easily create custom apps on the Salesforce Platform with complex business logic and beautiful user interfaces designed specific to every screen. Salesforce Lightning Builder tools allow the State to work in alignment with agile development methodologies as IT meets business demands faster.    If and where it may be needed, Developers can leverage the Apex programming language. Apex is an object-oriented, on-demand language. It is like Java, with similar syntax and notation, and is strongly-typed, compiled on demand, and fully integrated into the Platform. All of the application services come right out of the box, from a powerful workflow engine to API services, integration services, authentication, event log framework, analytics, and collaboration. | | | | | |
| DBM-4 | Describe the standard software development life cycle (SDLC) for deploying software. Describe the process for planning, creating, testing and deploying the system. | X | X |  |  |
| Response:  Salesforce implements FedRAMP moderate requirements from NIST SP 800-53 Rev. 4 including controls SA-3, Life Cycle Support, and RA-5, Vulnerability Scanning. NIST SP 800-53 Rev. 4 requirements are aligned with NIST SP 800-64, requirements for Security Considerations in the System Development Life Cycle.    Salesforce performs the following tasks to assure security in the development lifecycle: Architecture Reviews, Development, Quality Assurance, Security Review, Definition of Done (requires that the new functionality meets all defined acceptance criteria in the areas of user stories, code development, quality assurance, security, performance/scalability, user experience, localization, documentation, product metrics, and vulnerability/bug analysis and remediation). As part of the coding, Salesforce includes practices including those specified by Open Web Application Security Project (OWASP). The third party vulnerability assessment includes checks against the OWASP Top Ten Most Critical Web Application Security Vulnerabilities and an external application security assessment.    Salesforce incorporates security into its development processes at all stages. From initial architecture considerations to post-release, all aspects of software development incorporate security.     * Design phase – Guiding security principles and security training help ensure Salesforce engineers make the best security decisions possible. Threat assessments on high-risk features help to identify potential security issues as early in the development lifecycle as possible [SA-3, SA-8]. * Coding phase – Salesforce addresses standard vulnerability types through the use of secure coding patterns and anti-patterns, and uses static code analysis tools to identify security flaws [SA-10]. Secure code development during design, development, and release is controlled through a secure code repository. * Testing phase – Internal Salesforce staff and independent security consultants use scanners and proprietary tools along with manual security testing to identify potential security issues [SA-11]. * Prior to release – Salesforce validates that the functionality being developed and maintained meets its internal security requirements. Code is tested and approved prior to release. Post-release, Salesforce uses independent security service providers to analyze and monitor the product for potential security issues [SA-11].     The Salesforce security team receives and reviews threat alerts from a variety of sources including SANS, US-CERT, DHS CISCP, and OWASP. Threats that are deemed critical are escalated to the appropriate resource to respond [SI-5].    For additional information check out the [Application Lifecycle and Development Models](https://trailhead.salesforce.com/en/content/learn/modules/application-lifecycle-and-development-models) module in Trailhead. If you want to use change sets, your next step is the [Change Set Development Model](https://trailhead.salesforce.com/content/learn/modules/declarative-change-set-development) module. You can also find other Trailhead modules about the application lifecycle by using the App Lifecycle filter tag at <https://trailhead.salesforce.com/en/modules>. | | | | | |
| DBM-5 | Describe how the system provides the flexibility to extract and load data into standard non-proprietary software formats. | X | X |  |  |
| Response:  **Import/Export Utilities**  The Salesforce Platform includes the following import/export options for data:   * Data Import Wizard - An in-browser wizard that imports data for many standard Salesforce objects, including accounts, contacts, leads, solutions, campaign members, and person accounts. You can also import data for custom objects. * Salesforce Data Loader - Data Loader is a free, client application for the bulk import or export of data. Use it to insert, update, delete or export Salesforce records. * Direct Export - Data can be exported directly into CSV (comma separated values) file, or Excel files with a button click. This can be done from either a standard or custom list view, or from a report. This is the most common method utilized by end users. * Salesforce API - Data can be exported to and from the system through our API at any time or via a number of built in features. * Partner Tools - There are also many pre-integrated partner tools, some of which you may already own that may be leveraged. Examples of these include, but are not limited to, Informatica, Pervasive, CastIron, Boomi, etc.     We also offer a weekly export service (WES) for those customers requiring a local backup copy of their data or a data set for import into other applications (such as an ERP system). Exported file links can be included to assist with data migrations, data integrations, and provide more thorough backup and restore. | | | | | |
| DBM-6 | Describe how the system maintains an automated history of all transactions, including, but not limited to: date and time of change, "before" and "after" data field contents, and operator identifier or source of the update. | X | X |  |  |
| Response:  **Core Auditing Capabilities**  Within Salesforce, the creator and last updater, as well as timestamps, are recorded for every record. Additionally, the Salesforce Platform and Salesforce Applications have a multitude of history tracking and auditing features that provide valuable information about the use of an organization’s applications and data, which in turn can be a critical tool in diagnosing potential or real security issues. Auditing features include:    Record Modification Fields - All objects include fields to store the name of the user who created the record and who last modified the record. This provides some basic auditing information.    Field History Tracking - Enable auditing for individual fields (up to 20 fields per object), which will automatically track any changes in the values of selected fields. Although auditing is available for all custom objects, only some standard objects allow field-level auditing.    Login History - Review up to 20,000 successful and failed login attempts to the State for the past six months. The State can also track the geographic location of the IP addresses of your logins in your personal settings. You can track the geographic location of the login IP addresses for any of your users in the user’s detail page. To get more detailed geographic information, such as city and postal code, you can download the login history. Due to the nature of geolocation technology, the accuracy of geolocation fields (for example, country, city, postal code) can vary.    Identity Verification History - Review up to 20,000 records of your org users’ identity verification attempts from the past six months. For example, suppose that two-factor authentication is enabled when a user logs in. When the user successfully provides a time-based, one-time password as proof of identity, that information is recorded in Identity Verification History.    Setup Audit Trail - Administrators can view a Setup Audit Trail for the past six months within Salesforce, which logs when modifications are made to the State's configuration.    While the Login History and Setup Audit Trail are available for six months within Salesforce, they can be downloaded and stored locally to meet longer audit log retention requirements. Additionally, historic event logs which provide more information can be provided for a fee. For more information, please see<https://help.salesforce.com/articleView?id=000336835&language=en_US&type=1&mode=1>. | | | | | |
| DBM-7 | Describe how the software database conforms to the Open Database Connectivity Standard (ODBC). | X | X |  |  |
| Response:  Data in Salesforce is represented in terms of Standard/Custom object records. These records can be analyzed using standard Reports available in Salesforce.  Additionally, if we must expose part of the information to a third-party system, we can use the REST/SOAP services in Salesforce. We could build custom REST/SOAP solution by extending APEX scripting language. We would be able to build both inbound (consume service) and outbound services in Salesforce.  Salesforce App Exchange products provides a fast and easy way to extend the capabilities of the standard Salesforce system. There are solutions available in the App Exchange that provides standards-based ODBC connectivity from Salesforce.com. These products enable users to access, analyze and report on data with the SQL-based tool of choice  Salesforce is built upon an open standards based services oriented architecture. Architected around the latest standards, including SOAP, WSDL, and WS-I Basic Profile, these services provide the complete set of operations necessary to complete even the most demanding of integration projects. Salesforce does not require a platform to run on. Salesforce solutions are delivered on-demand over the Internet, so you need not worry about licensing software and setting up and managing hardware platforms, operating systems, or relational database management systems (RDBMSs). Salesforce does not conform to the Open Database Connectivity Standard (ODBC). | | | | | |
| DBM-8 | Describe how the system provides utilities or other tools for administrative users to evaluate data relationships between tables. | X | X |  |  |
| Response:  Entity relationship diagrams (ERDs) are available for standard Salesforce objects and illustrate important relationships between objects. Salesforce ERDs use crow’s foot notation. Each ERD includes links to the topics that describe the fields in objects related to the diagram.  Salesforce Schema Builder provides a dynamic environment for viewing and modifying all the objects and relationships in your app. This greatly simplifies the task of designing, implementing, and modifying your data model, or schema. Schema Builder is enabled by default. You can view your existing schema and interactively add new custom objects, custom fields, and relationships, simply by dragging and dropping. Schema Builder automatically implements the changes and saves the layout of your schema any time you move an object. Schema Builder provides details like the field values, required fields, and how objects are related by displaying lookup and master-detail relationships. You can view the fields and relationships for both standard and custom objects. | | | | | |
| DBM-9 | Describe how the system prevents corruption or loss of data already entered into the system in the event of failure. | X | X |  |  |
| Response:  **Backup & Disaster Recovery**  Customer data, up to the last committed transaction, is replicated to disk in near-real time at the designated disaster recovery data center, backed up at the Active data center, and then cloned at a Ready data center. Disaster recovery tests verify our projected recovery times and the integrity of the customer data.  Backups are performed daily at each data center facility without stopping access to the application. Backup cloning is transmitted over an encrypted network (our MPLS network across all data centers). Backups never leave our secure data center facilities, unless they are to be retired and destroyed through a secure destruction process.  The backup retention policy is 90 days (30 days for sandboxes). Deleted / modified data cannot be recovered after 90 days (30 days for sandboxes). If customers want a longer retention, they can use the weekly export feature available in the system.  **RTO/RPO**  Our Recovery Time Objective (RTO) is 12 hours and Recovery Point Objective (RPO) is 4 hours.    Salesforce's disaster recovery plans currently have the following target recovery objectives: (a) restoration of the Service within 12 hours after Salesforce's declaration of a disaster; and (b) maximum Customer Data loss of 4 hours; excluding, however, a disaster or multiple disasters causing the compromise of both multiple Salesforce data centers at the same time, and excluding development and test bed environments, such as the Sandbox service. | | | | | |

***Backup and System Recovery Requirements***

The system must create backup copies of the software and restore and use those backup copies for the basic protection against system problems and data loss. This requirement refers to all application system files, data files, and database data files. The system must provide a comprehensive and easily manageable backup and recovery process.

The system must have a recovery plan that ensures component failures do not disrupt services. The plan must be completed, implemented, and tested prior to system implementation.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Req #** | **Requirement** | (1) Comply | (a) Core | (b) Custom | (c) 3rd Party |
| BKP-1 | Describe the Backup and System Recovery plan and readiness. Describe the service level agreement on returning the system to service from a backup. Describe the backup retention schedules – daily, weekly, monthly, quarterly, etc. | X | X |  |  |
| Response:  **Backup & Disaster Recovery**  Customer data, up to the last committed transaction, is replicated to disk in near-real time at the designated disaster recovery data center, backed up at the Active data center, and then cloned at a Ready data center. Disaster recovery tests verify our projected recovery times and the integrity of the customer data.  Backups are performed daily at each data center facility without stopping access to the application. Backup cloning is transmitted over an encrypted network (our MPLS network across all data centers). Backups never leave our secure data center facilities, unless they are to be retired and destroyed through a secure destruction process.  The backup retention policy is 90 days (30 days for sandboxes). Deleted / modified data cannot be recovered after 90 days (30 days for sandboxes). If customers want a longer retention, they can use the weekly export feature available in the system.  **Superior Uptime**  Salesforce has maintained high levels of availability across all Salesforce instances since inception. As the only on-demand vendor to provide daily service-quality data on a public Web site (https://trust.salesforce.com), Salesforce proves that we are the leader in availability. And by making its track record completely transparent, Salesforce proves we are worthy of our customers’ trust. To ensure maximum uptime and continuous availability, Salesforce provides the best redundant data protection and most advanced facilities protection available, along with a complete data recovery plan—all without affecting performance.  Salesforce uses commercially reasonable efforts to make its on-demand services available to its customers 24/7, except for planned downtime, for which Salesforce gives customers prior notice, and force majeure events. Excellent availability statistics are critical to Salesforce's customers’ success and to the success of Salesforce as a company. Live availability status and historical availability is publicly published at https://trust.salesforce.com/en/#systemStatus.  The persistence layer underlying the Salesforce Platform is proven database technology that powers all of Salesforce’s products today, serving more than 150,000 organizations and over 5 billion transactions per day with an average request response time of less than 200 milliseconds, all with an average uptime of 99.9+ percent.  Salesforce does not typically offer Service Level Agreements as part of the base service offering. Our approach is to offer a service with high availability and fast resolution of problems. If a customer requires an SLA it will be negotiated separately. | | | | | |
| BKP-2 | Describe all needed hardware, software, and tools, and define all roles, responsibilities, processes, and procedures. The system must be sufficiently flexible to integrate with existing DHHS capabilities and accommodate future changes. | X | X |  |  |
| Response:  **100% Multi-Tenant, Cloud Application**  Salesforce offers the market leading Platform as a Service (PaaS) and market leading Software as a Service (SaaS) solutions.  Salesforce is a multi-tenant, cloud-based web application. No additional software or infrastructure is required. Salesforce hosts the entire solution, thus freeing up the State to manage its mission, not manage an infrastructure solution. Additionally, Salesforce is browser agnostic and supports all major browsers (Firefox, Chrome, Safari, IE, Edge). No installations on users’ laptops or desktops are required and thus the solution is accessible from anywhere an internet connection and supported browser are available, including mobile devices.  The fully documented list of supported browsers and mobile devices for the full Salesforce site and Salesforce Mobile is available in the following articles in online our Help & Training Portal: <https://help.salesforce.com/HTViewHelpDoc?id=getstart_browser_overview.htm&language=en_US> and <https://help.salesforce.com/articleView?id=sf1_requirements.htm&type=0&language=en_US&release=206.5>. | | | | | |
| BKP-3 | Describe the Disaster Recovery Plan. Describe the service level agreement on returning the system back to operational service. | X | X |  |  |
| Response:  **Backup & Disaster Recovery**  Customer data, up to the last committed transaction, is replicated to disk in near-real time at the designated disaster recovery data center, backed up at the Active data center, and then cloned at a Ready data center. Disaster recovery tests verify our projected recovery times and the integrity of the customer data.  Backups are performed daily at each data center facility without stopping access to the application. Backup cloning is transmitted over an encrypted network (our MPLS network across all data centers). Backups never leave our secure data center facilities, unless they are to be retired and destroyed through a secure destruction process.  The backup retention policy is 90 days (30 days for sandboxes). Deleted / modified data cannot be recovered after 90 days (30 days for sandboxes). If customers want a longer retention, they can use the weekly export feature available in the system.  **Superior Uptime**  Salesforce has maintained high levels of availability across all Salesforce instances since inception. As the only on-demand vendor to provide daily service-quality data on a public Web site (https://trust.salesforce.com), Salesforce proves that we are the leader in availability. And by making its track record completely transparent, Salesforce proves we are worthy of our customers’ trust. To ensure maximum uptime and continuous availability, Salesforce provides the best redundant data protection and most advanced facilities protection available, along with a complete data recovery plan—all without affecting performance.  Salesforce uses commercially reasonable efforts to make its on-demand services available to its customers 24/7, except for planned downtime, for which Salesforce gives customers prior notice, and force majeure events. Excellent availability statistics are critical to Salesforce's customers’ success and to the success of Salesforce as a company. Live availability status and historical availability is publicly published at https://trust.salesforce.com/en/#systemStatus.  The persistence layer underlying the Salesforce Platform is proven database technology that powers all of Salesforce’s products today, serving more than 150,000 organizations and over 5 billion transactions per day with an average request response time of less than 200 milliseconds, all with an average uptime of 99.9+ percent.  Salesforce does not typically offer Service Level Agreements as part of the base service offering. Our approach is to offer a service with high availability and fast resolution of problems. If a customer requires an SLA it will be negotiated separately. | | | | | |
| BKP-4 | Describe how backups of the system are able to be scheduled without user intervention and without interruption to the system. | X | X |  |  |
| Response:  **Backup & Disaster Recovery**  Customer data, up to the last committed transaction, is replicated to disk in near-real time at the designated disaster recovery data center, backed up at the Active data center, and then cloned at a Ready data center. Disaster recovery tests verify our projected recovery times and the integrity of the customer data.  Backups are performed daily at each data center facility without stopping access to the application. Backup cloning is transmitted over an encrypted network (our MPLS network across all data centers). Backups never leave our secure data center facilities, unless they are to be retired and destroyed through a secure destruction process.  The backup retention policy is 90 days (30 days for sandboxes). Deleted / modified data cannot be recovered after 90 days (30 days for sandboxes). If customers want a longer retention, they can use the weekly export feature available in the system.  **Superior Uptime**  Salesforce has maintained high levels of availability across all Salesforce instances since inception. As the only on-demand vendor to provide daily service-quality data on a public Web site (https://trust.salesforce.com), Salesforce proves that we are the leader in availability. And by making its track record completely transparent, Salesforce proves we are worthy of our customers’ trust. To ensure maximum uptime and continuous availability, Salesforce provides the best redundant data protection and most advanced facilities protection available, along with a complete data recovery plan—all without affecting performance.  Salesforce uses commercially reasonable efforts to make its on-demand services available to its customers 24/7, except for planned downtime, for which Salesforce gives customers prior notice, and force majeure events. Excellent availability statistics are critical to Salesforce's customers’ success and to the success of Salesforce as a company. Live availability status and historical availability is publicly published at https://trust.salesforce.com/en/#systemStatus.  The persistence layer underlying the Salesforce Platform is proven database technology that powers all of Salesforce’s products today, serving more than 150,000 organizations and over 5 billion transactions per day with an average request response time of less than 200 milliseconds, all with an average uptime of 99.9+ percent.  Salesforce does not typically offer Service Level Agreements as part of the base service offering. Our approach is to offer a service with high availability and fast resolution of problems. If a customer requires an SLA it will be negotiated separately. | | | | | |
| BKP-5 | Describe how the system provides testing and validation processes for all of the backup requirements listed previously (BKP-1, BKP-2, BKP-3 and BKP-4). | X | X |  |  |
| Response:  **Backup & Disaster Recovery**  Customer data, up to the last committed transaction, is replicated to disk in near-real time at the designated disaster recovery data center, backed up at the Active data center, and then cloned at a Ready data center. Disaster recovery tests verify our projected recovery times and the integrity of the customer data.  Backups are performed daily at each data center facility without stopping access to the application. Backup cloning is transmitted over an encrypted network (our MPLS network across all data centers). Backups never leave our secure data center facilities, unless they are to be retired and destroyed through a secure destruction process.  The backup retention policy is 90 days (30 days for sandboxes). Deleted / modified data cannot be recovered after 90 days (30 days for sandboxes). If customers want a longer retention, they can use the weekly export feature available in the system.  **Superior Uptime**  Salesforce has maintained high levels of availability across all Salesforce instances since inception. As the only on-demand vendor to provide daily service-quality data on a public Web site (https://trust.salesforce.com), Salesforce proves that we are the leader in availability. And by making its track record completely transparent, Salesforce proves we are worthy of our customers’ trust. To ensure maximum uptime and continuous availability, Salesforce provides the best redundant data protection and most advanced facilities protection available, along with a complete data recovery plan—all without affecting performance.  Salesforce uses commercially reasonable efforts to make its on-demand services available to its customers 24/7, except for planned downtime, for which Salesforce gives customers prior notice, and force majeure events. Excellent availability statistics are critical to Salesforce's customers’ success and to the success of Salesforce as a company. Live availability status and historical availability is publicly published at https://trust.salesforce.com/en/#systemStatus.  The persistence layer underlying the Salesforce Platform is proven database technology that powers all of Salesforce’s products today, serving more than 150,000 organizations and over 5 billion transactions per day with an average request response time of less than 200 milliseconds, all with an average uptime of 99.9+ percent.  Salesforce does not typically offer Service Level Agreements as part of the base service offering. Our approach is to offer a service with high availability and fast resolution of problems. If a customer requires an SLA it will be negotiated separately. | | | | | |
| BKP-6 | If there is a backup failure or downtime, describe the method and timing of communication to DHHS. | X | X |  |  |
| Response:  Salesforce maintains an Incident Response Plan and has an established Security Incident Response Process. During a security incident, the process guides Salesforce personnel in management, communication, and resolution activities. | | | | | |

***Security and Audit Requirements***

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Req #** | **Requirement** | (1) Comply | (a) Core | (b) Custom | (c) 3rd Party |
| SEC-1 | Describe the security safeguards integrated into their application and how these safeguards address DHHS security.  Refer, for example, to DHHS Information Technology (IT) Access Control Standard ((DHHS-IT-2018-001B) for specific requirements: <http://dhhs.ne.gov/ITSecurity> | X | X |  |  |
| Response:  **Government Trusted Security and Infrastructure**  Salesforce understands that the confidentiality, integrity, and availability of our customers’ information are vital to their business operations and Salesforce's own success. Salesforce uses a multi-layered approach to protect that key information, constantly monitoring and improving our application, systems, and processes to meet the growing demands and challenges of security.    Independent audits confirm that our security goes far beyond what most companies have been able to achieve on their own. Using the latest firewall protection, intrusion detection systems, and TLS encryption, Salesforce gives you the peace of mind only a world-class security infrastructure can provide.    Third-party validation  Security is a multidimensional business imperative that demands consideration at multiple levels, from security for applications to physical facilities and network security. In addition to the latest technologies, world-class security requires ongoing adherence to best-practice policies. To ensure this adherence, we continually seek relevant third-party certification, including ISO 27001, the SysTrust audit (the recognized standard for system security), and SSAE 16 SOC 1 audit (an examination and assessment of internal corporate controls, previously known as SAS 70 Type II). SOC1, SOC2 and SOC3 audits are performed by a third-party auditor annually at a minimum. Additional audits and certifications include CSA ‘Consensus Assessments Initiative’, JIPDC (Japan Privacy Seal), Tuv (Germany Privacy Mark), and TRUSTe.    Protection at the application level  Salesforce protects customer data by ensuring that only authorized users can access it. Administrators assign data security rules that determine which data users can access. Sharing models define organization-wide defaults and data access based on a role hierarchy. All data is encrypted in transfer. All access is governed by strict password security policies. All passwords are stored in SHA 256 one-way hash format. Applications are continually monitored for security violation attempts.    Protection at the facilities level  Salesforce security standards are stringent and designed with demanding customers in mind, including the world’s most security-conscious financial institutions. Authorized personnel must pass through five levels of biometric scanning to reach the Salesforce system cages. All buildings are completely anonymous, with bullet-resistant exterior walls and embassy-grade concrete posts and planters around the perimeter. All exterior entrances feature silent alarm systems that notify law enforcement in the event of suspicion or intrusion. Data is backed up to disk. These backups provide a second level of physical protection and disks never leave the data center.    Protection at the network level  Multilevel security products from leading security vendors and proven security practices ensure network security. To prevent malicious attacks through unmonitored ports, external firewalls allow only http and https traffic on ports 80 and 443, along with ICMP traffic. Switches ensure that the network complies with the RFC 1918 standard, and address translation technologies further enhance network security. IDS sensors protect all network segments. Internal software systems are protected by two-factor authentication, along with the extensive use of technology that controls points of entry. All networks are certified through third-party vulnerability assessment programs.    Trust.salesforce.com is the Salesforce community’s home for real-time information on system performance and security. On this site you'll find:   * Up-to-the minute information on planned maintenance * Phishing, malicious software, and social engineering threats * Best security practices for the State * Information on how we safeguard your data     These papers further explain the technology that makes the Salesforce Platform fast, scalable, and secure for any type of application:  <https://developer.salesforce.com/page/Multi_Tenant_Architecture>  <https://trust.salesforce.com/en/trust-and-compliance-documentation/>  **Government Cloud**  Salesforce was the first Cloud Service Provider granted a FedRAMP Authority to Operate (ATO) for both Software as a Service (SaaS) and Platform as a Service (PaaS), consistent with the FedRAMP moderate baseline controls.    On May 23, 2014 Salesforce was granted a FedRAMP ATO at the moderate impact level issued by the Department of Health and Human Services (HHS) for the Salesforce Government Cloud. Testing for the ATO was performed by a third party assessment organization (3PAO).    The Salesforce Government Cloud information system and authorization boundary, is comprised of the Salesforce Platform\*, Sales, Service, Communities, Analytics, Salesforce Mobile, and Industry Solutions, as well as the backend infrastructure (e.g., servers, network devices, databases, storage arrays) that support the operations of these products, referred to as the General Support System (GSS).    To obtain compliance with FedRAMP, Salesforce conducted security assessment and authorization activities in accordance with FedRAMP guidance, NIST SP 800-37, and HHS requirements. As part of this process Salesforce documented a System Security Plan (SSP) for the Salesforce Government Cloud service offering. The SSP is developed in accordance with NIST SP 800-18. The SSP identifies control implementations for the GSS and in-scope customer facing products (e.g., Lightning Platform, applicable Salesforce Services) according to the FedRAMP moderate baseline and HHS security control parameters. A security assessment of the information system was conducted by a 3PAO in accordance with FedRAMP Moderate requirements. The security assessment testing determined the adequacy of the management, operational, and technical security controls used to protect the confidentiality, integrity, and availability of Salesforce's Government Cloud service offering and the Customer Data it stores, transmits and processes.    To maintain compliance with FedRAMP, Salesforce conducts continuous monitoring, which includes ongoing technical vulnerability detection, remediation of open compliance related findings, and at least annual independent assessment of security controls by a 3PAO. As part of the current FedRAMP annual assessment, Salesforce is aligned with NIST SP 800-53 Revision 4.    Government Cloud eligible non-U.S. Federal Government authorizing officials and customers can request the below Salesforce Government Cloud FedRAMP materials after completing applicable NDAs:   * Partner System Security Plan * Control Implementation Summary/Customer Responsibility Matrix * Customer Configuration User Guide * Disaster Recovery Plan (DRP) * Incident Response Plan (IRP) * FedRAMP Authority to Operate (ATO) Letter   For more information on the Salesforce Government Cloud please see the [Salesforce Government Cloud whitepaper](https://org62.my.salesforce.com/sfc/p/#000000000062/a/0M000000Q8ar/moggeD49GPYM4jsNqrIjHnLlcqW7Zc7VwHfyKfuEmbs).    \*Only the Salesforce Platform is included within the FedRAMP Authorization Boundary for the Salesforce Government Cloud.    For more information on the Salesforce Government cloud please see the Salesforce Government Cloud white paper: <https://org62.my.salesforce.com/sfc/p/000000000062/a/0M000000Q8ar/moggeD49GPYM4jsNqrIjHnLlcqW7Zc7VwHfyKfuEmbs>. | | | | | |
| SEC-2 | The system must comply with Federal, State, and division-specific security requirements including but not limited to:   1. Health Insurance Portability and Accountability Act (HIPAA) of 1996 2. Health Information Technology for Economic and Clinical Health Act (HITECH) of 2009 3. Nebraska Electronic Signature Statute <http://www.nebraskalegislature.gov/laws/statutes.php?statute=86-611> 4. Privacy Act of 1974 5. 45 CFR 164 Security standards for PHI   Refer to the Nebraska DHHS Information Systems and Technology Security Policies and Standards for more information (<http://dhhs.ne.gov/ITSecurity>)  Due to PHI, DHHS will not give access or demonstrate the current system. Our current data systems include System Automation’s License 2000 and the federal government’s Aspen Central Office. |  | X |  |  |
| Response:  **HIPAA**  Many Salesforce customers store protected health information (PHI) on our service.    The U.S. Centers for Medicare & Medicaid Services (CMS) guidelines states that "Information related to personnel, medical, and similar data includes all information covered by the Privacy Act of 1974 (e.g., salary data, social security information, passwords, user identifiers (IDs), Equal Employment Opportunity (EEO), personnel profile (including home address and phone number), medical history employment history (general and security clearance information), and arrest/criminal investigation history as well as personally identifiable information (PII), individually identifiable information (IIF), or personal health information (PHI) covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA)" should be considered Moderate for Confidentiality, Integrity, and Availability.    Salesforce's FedRAMP ATO is based on a Moderate System Security Level. Please note, Salesforce is not considered a "first-tier, downstream or related entity" for the purposes of compliance with CMS flow-down regulations.    Salesforce has also received a Provisional Authorization (PA) from Defense Information Systems Agency (DISA) at Impact Level 4 (IL4) to store, process, or transmit Controlled Unclassified Information (CUI) and/or other mission critical data to include that used in direct support of military or contingency operations. In addition to the DoD Cloud Computing SRG including PHI as a CUI category, the National Archives' CUI Registry (https://www.archives.gov/cui/registry/category-list) includes Health Information as a category under Privacy.  **HITECH Act**  Salesforce's customers are responsible for complying with HIPAA's Privacy Rule and Security and the HITECH Act in their capacity as a covered entity or business associate using the Salesforce services. The services' features permit customers to customize use as per a compliance program for HIPAA (including the HITECH Act) and many customers store protected health information (PHI) on our service. Salesforce can assist customers with their compliance obligations; for example, by discussing entering into business associate agreements (BAA) to address formal legal requirements pertaining to use and disclosure of protected health information (PHI).    Salesforce regularly signs Business Associate Agreements as required by HIPAA, which your licensing attorney can put in place as an addendum to a Master Subscription Agreement (MSA). This document includes details regarding how we comply with requirements under HIPAA and HITECH; including the Privacy Rule, Security Rule, and breach notification requirements.  **Privacy**  At Salesforce, there is no higher priority than the privacy and security of our customers' data. We believe that protecting the privacy of our customers' data is integral to our mission of earning and maintaining the trust of each of our customers. We seek to lead the industry as a trusted repository for customer data through a world-class privacy program and provide a secure infrastructure and flexible tools which help enable our customers to comply with global privacy and data protection regulations.   * Privacy Statement:<http://www.salesforce.com/company/privacy/> * For detail on Salesforce tools that support privacy compliance:<https://compliance.salesforce.com/en> * For information on the Security, Privacy and Architecture of the various Salesforce offerings, please refer to our Trust and Compliance documentation within Help & Training:<https://trust.salesforce.com/en/trust-and-compliance-documentation/>   **Encryption Capabilities**  Salesforce has many customers that are subject to laws pertaining to the processing of personally identifiable information (PII) or personal data. Salesforce offers its customers a broad spectrum of functionalities and customer-controlled security features that its customers may implement in their respective uses of the Salesforce services. Salesforce believes that these provide its customers the flexibility to comply with laws with stringent privacy and security requirements.    Data In Motion  All transmissions between the user and the Salesforce Services are TLS 1.2 encrypted with a 2048-bit Public Key, using AES 256-bit encryption by default.    Data At Rest  Salesforce Classic Encryption includes a feature to encrypt custom text fields (ECF):   * The fields can be masked appropriately for specific data types (i.e., credit card number, Social Security Number, National Insurance Number, Social Insurance Number). * Access to read the masked parts of the fields is limited by the "View Encrypted Data" permission, which is not enabled by default. * Customers can manage their encryption key based on their organization’s security needs and regulatory requirements. See our Help and Training site for details: <https://help.salesforce.com/apex/HTViewHelpDoc?id=security_keys_using_master.htm&language=en> * Encrypted fields use 128-bit encryption and the AES (Advanced Encryption Standard) algorithm * Custom text fields can be up to 175 characters in length     Additional Salesforce Encryption Capabilities  Apex Code extends the powerful and proven success of the Salesforce Platform by introducing the ability to write code that runs on Salesforce servers. This language makes possible the development of a new class of application and features deployed entirely on demand. Using Apex, the State can create user interface classes that utilize the Apex crypto class to encrypt field level data up to AES 256-bit encryption. Please see here for more information: <https://developer.salesforce.com/page/Apex_Crypto_Class>.    **Salesforce Platform Encryption**  Salesforce Classic Encryption is limited to encrypting custom text fields of 175 characters or less, while Salesforce offers Salesforce Platform Encryption as an additional licensing option for encrypting standard and custom fields of various types, attachments, files, and other content using AES 256-bit encryption.    Salesforce Platform Encryption sets up in minutes, with no additional hardware or software, and uses native strong, standards-based encryption. Platform Encryption provides an extra layer to Salesforce's security while enabling customers to enjoy business critical Platform features, such as search, workflow, and validation rules.    The State can use Platform Encryption so that the State can confidently prove compliance with privacy policies, regulatory requirements, and contractual obligations for handling private data.    Platform Encryption offers native platform encryption and key management features. By default, the State's data is encrypted at rest using a hardware security module-based key derivation system. These features allow the State to protect data at a more granular level than Classic Encryption while still giving users the ability to perform necessary tasks. The State can:   * Encrypt files and attachments (including email attachments) * Encrypt certain standard and custom fields * Encrypt Knowledge article fields and attachments * Encrypt certain Chatter data such as feed posts and comments, feed questions and answers, link labels and URLs, and feed polls and poll choices * Encrypt transcribed conversations (e.g. between agents and customers) * Access encrypted data from most elements in flows and processes, except when filtering or sorting records * Use the Shield Key Management System (KMS) to generate your org-specific tenant secret and data encryption key     Platform Encryption helps address some concerns about protecting confidential information. It prevents sensitive data from being stored in clear, decipherable form and allows you to manage your tenant secrets, which are used to derive the keys that protect your data. Salesforce is committed to high security standards and offers multiple data encryption options. Customers who want to adopt or extend their use of Salesforce can consider using Platform Encryption to comply with various standards. Additional details on Salesforce Platform Encryption are provided in these white papers: <https://a.sfdcstatic.com/content/dam/www/ocms/assets/pdf/platform/whitepaper-platform-shield.pdf> and <https://org62.my.salesforce.com/sfc/p/000000000062/a/0M000000Htiv/0pEjEbyFd3.Yp1XI_zC1I6xuel9EsD0f.VKrwVFu64k>. Please also refer to Platform Encryption Best Practices outlined at: <https://help.salesforce.com/articleView?id=security_pe_best_practices.htm&language=en_US&type=0>.    In addition to the default Shield KMS service, multiple options are available for generating and managing your tenant secrets and data encryption keys outside of Salesforce, for added control and flexibility. With the Bring Your Own Key (BYOK) service, you have two options to manage your encryption key lifecycle: 1) use the infrastructure of your choice to generate a tenant secret and upload to the Shield KMS or 2) use the infrastructure of your choice to create a data encryption key instead of a tenant secret and upload to the Shield KMS. Additionally, with the Cache-Only Key Service you can store your key material outside of Salesforce and fetch your key on demand from a key service that you control. Additional details on the BYOK service are provided at <https://help.salesforce.com/articleView?id=security_pe_byok_setup.htm&type=5>. Additional details on the Cache-Only Key service are provided at <https://help.salesforce.com/articleView?id=security_pe_byok_cache.htm&type=0>.  **National Framework and State DHHS Security Policy Compliance**  Salesforce meets privacy and security requirements for the Office of the National Coordinator's Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health information ([https://www.healthit.gov/sites/default/files/nationwide-ps- framework-5.pdf](https://www.healthit.gov/sites/default/files/nationwide-ps-)) and Nebraska DHHS Information Systems and Technology Security Policies and Standards (<http://dhhs.ne.gov/ITSecurity>  [Information Technology (IT) Security Policies and Standards](http://dhhs.ne.gov/ITSecurity)).  **Electronic Signatures**  The solution would leverage third party digital signature apps provided through the Salesforce App Exchange platform. Many of the digital signature apps published in the platform are legally binding as per the Nebraska state statute. As part of the discovery process, we would recommend appropriate app that is legally binding within the state of Nebraska. | | | | | |
| SEC-3 | Describe how the system meets the DHHS requirements for unique user ID access. Include:   1. Specification on configuration of the unique user ID. 2. How the unique user ID is assigned and managed. 3. How the unique user ID is used to log system activity. 4. How the system handles the creation of duplicate user ID accounts. | X | X |  |  |
| Response:  **Authentication**  Logon is form-based. When users log into the Salesforce application, they submit a username and password, which are sent to Salesforce via an TLS-encrypted session. Security features are developed by Salesforce and built into the application. Third-party packages are not used for development or implementation of security internal to the application.    In addition, single sign-on and two-factor authentication may be used to authenticate users for both standard users and Community users. Some organizations prefer to use an existing single sign-on capability to simplify and standardize their user authentication. You have two options to implement single sign-on—federated authentication using Security Assertion Markup Language (SAML) or delegated authentication.    Federated authentication using SAML allows you to send authentication and authorization data between affiliated but unrelated Web services. This enables you to sign-on to Salesforce from a client application. Federated authentication using SAML is enabled by default for the State.    Delegated authentication single sign-on enables you to integrate Salesforce with an authentication method that you choose. This enables you to integrate authentication with your LDAP (Lightweight Directory Access Protocol) server, or perform single sign-on by authenticating using a token instead of a password. You manage delegated authentication at the profile level, allowing some users to use delegated authentication, while other users continue to use their Salesforce-managed password. Delegated authentication is set by profile, not organization wide. You must request that this feature be enabled by Salesforce.    Salesforce can be configured to utilize Active Directory directly via Delegated Authentication, or indirectly via Federated Identity using either SAML 1.1, or SAML 2.0. Additionally, your users can be loaded from information drawn from your Active Directory servers and modifications made in Active Directory can be propagated into Salesforce.    Customers can use their own SAML Identity Provider, or license one directly from Salesforce with our Identity Connect product.  **Core Auditing Capabilities**  Within Salesforce, the creator and last updater, as well as timestamps, are recorded for every record. Additionally, the Salesforce Platform and Salesforce Applications have a multitude of history tracking and auditing features that provide valuable information about the use of an organization’s applications and data, which in turn can be a critical tool in diagnosing potential or real security issues. Auditing features include:    Record Modification Fields - All objects include fields to store the name of the user who created the record and who last modified the record. This provides some basic auditing information.    Field History Tracking - Enable auditing for individual fields (up to 20 fields per object), which will automatically track any changes in the values of selected fields. Although auditing is available for all custom objects, only some standard objects allow field-level auditing.    Login History - Review up to 20,000 successful and failed login attempts to the State for the past six months. The State can also track the geographic location of the IP addresses of your logins in your personal settings. You can track the geographic location of the login IP addresses for any of your users in the user’s detail page. To get more detailed geographic information, such as city and postal code, you can download the login history. Due to the nature of geolocation technology, the accuracy of geolocation fields (for example, country, city, postal code) can vary.    Identity Verification History - Review up to 20,000 records of your org users’ identity verification attempts from the past six months. For example, suppose that two-factor authentication is enabled when a user logs in. When the user successfully provides a time-based, one-time password as proof of identity, that information is recorded in Identity Verification History.    Setup Audit Trail - Administrators can view a Setup Audit Trail for the past six months within Salesforce, which logs when modifications are made to the State's configuration.    While the Login History and Setup Audit Trail are available for six months within Salesforce, they can be downloaded and stored locally to meet longer audit log retention requirements. Additionally, historic event logs which provide more information can be provided for a fee. For more information, please see<https://help.salesforce.com/articleView?id=000336835&language=en_US&type=1&mode=1>.  **Password Policies Overview**  By default, initial Salesforce user passwords are sent to the email ID on record for that user as stored in the Salesforce application. These passwords are only valid for the initial login. There are several settings you can configure to ensure that your user's passwords are strong:   * Password policies: set various password and login policies, such as specifying an amount of time before all users' passwords expire, the level of complexity required for passwords, and more. * User password expiration: expire the passwords for all the users in the State * User password resets: reset the password for specified users * Login attempts and lockout periods: if a user is locked out of Salesforce due to too many failed login attempts, you can unlock them.     Default Password Settings  A password cannot contain your Username and cannot match your first or last name.  For all editions, a new organization has the following default password settings:   * A password must contain at least eight characters. * A password must contain at least one alphabetic character and one number. * The answer to the question posed if you forget your password cannot contain your password. * The last three passwords are remembered and cannot be reused when you are changing your password.   For more detail on password policies, please access this Help and Training article: <https://help.salesforce.com/apex/HTViewHelpDoc?id=security_overview_passwords.htm&language=en>. | | | | | |
| SEC-4 | Describe how the system meets the DHHS standard for administering passwords:   1. Initial Password assignment. 2. Strong Password Requirements. 3. Password reset process. 4. Password expiration policy. 5. Password controls for automatic lockout access to any user or user group after an administrator-defined number of unsuccessful log-on attempts. | X | X |  |  |
| Response:  **Password Policies Overview**  By default, initial Salesforce user passwords are sent to the email ID on record for that user as stored in the Salesforce application. These passwords are only valid for the initial login. There are several settings you can configure to ensure that your user's passwords are strong:   * Password policies: set various password and login policies, such as specifying an amount of time before all users' passwords expire, the level of complexity required for passwords, and more. * User password expiration: expire the passwords for all the users in the State * User password resets: reset the password for specified users * Login attempts and lockout periods: if a user is locked out of Salesforce due to too many failed login attempts, you can unlock them.     Default Password Settings  A password cannot contain your Username and cannot match your first or last name.  For all editions, a new organization has the following default password settings:   * A password must contain at least eight characters. * A password must contain at least one alphabetic character and one number. * The answer to the question posed if you forget your password cannot contain your password. * The last three passwords are remembered and cannot be reused when you are changing your password.   For more detail on password policies, please access this Help and Training article: <https://help.salesforce.com/apex/HTViewHelpDoc?id=security_overview_passwords.htm&language=en>. | | | | | |
| SEC-5 | Describe how the system meets the requirements for unique system administration access. Include:   1. Specification on configuration of the unique system administration ID, (approximately 30 with ability to access and manage the applications across all license types). 2. How the unique system administration ID is assigned and managed. 3. How the unique system administration ID is used to log system activity. | X | X |  |  |
| Response:  **Administration**  Salesforce has a Setup environment that allows a customer’s Administrator to configure the application based on their specific requirements through a declarative framework (point and click).    The organization administrator (appointed by the State and not by Salesforce) has access to the admin interfaces in order to...   * configure organization default settings (Time Zones, Currency) * set login constraints (SSO, 2 Factor Authentication, IP range) * role-based access control and role-hierarchies * add new users, reset passwords * define customer objects, custom fields, set default pick-list values, custom reports * manage delegated administration * other functions (session timeout, password policies)   The organization administrator logs onto the application like other users within the organization; however, they have admin privileges granted to them which provide them with this additional access.    Administrators can also access a subset of functions using a mobile device via the Salesforce Application. Once downloaded the admin can manage users, reset passwords, applications, profiles and permission sets from their mobile device.    **Core Auditing Capabilities**  Within Salesforce, the creator and last updater, as well as timestamps, are recorded for every record. Additionally, the Salesforce Platform and Salesforce Applications have a multitude of history tracking and auditing features that provide valuable information about the use of an organization’s applications and data, which in turn can be a critical tool in diagnosing potential or real security issues. Auditing features include:    Record Modification Fields - All objects include fields to store the name of the user who created the record and who last modified the record. This provides some basic auditing information.    Field History Tracking - Enable auditing for individual fields (up to 20 fields per object), which will automatically track any changes in the values of selected fields. Although auditing is available for all custom objects, only some standard objects allow field-level auditing.    Login History - Review up to 20,000 successful and failed login attempts to the State for the past six months. The State can also track the geographic location of the IP addresses of your logins in your personal settings. You can track the geographic location of the login IP addresses for any of your users in the user’s detail page. To get more detailed geographic information, such as city and postal code, you can download the login history. Due to the nature of geolocation technology, the accuracy of geolocation fields (for example, country, city, postal code) can vary.    Identity Verification History - Review up to 20,000 records of your org users’ identity verification attempts from the past six months. For example, suppose that two-factor authentication is enabled when a user logs in. When the user successfully provides a time-based, one-time password as proof of identity, that information is recorded in Identity Verification History.    Setup Audit Trail - Administrators can view a Setup Audit Trail for the past six months within Salesforce, which logs when modifications are made to the State's configuration.    While the Login History and Setup Audit Trail are available for six months within Salesforce, they can be downloaded and stored locally to meet longer audit log retention requirements. Additionally, historic event logs which provide more information can be provided for a fee. For more information, please see<https://help.salesforce.com/articleView?id=000336835&language=en_US&type=1&mode=1>. | | | | | |
| SEC-6 | Describe how the system meets the requirements for unique database administration access. Include:   1. Specification on configuration of the unique database administration ID. 2. How the unique database administration ID is assigned and managed. 3. How the unique database administration ID is used to log system activity. | X | X |  |  |
| Response:  Salesforce does not require a platform to run on. Salesforce solutions are delivered on-demand over the Internet, so you need not worry about licensing software and setting up and managing hardware platforms, operating systems, or relational database management systems (RDBMSs).  **Administration**  Salesforce has a Setup environment that allows a customer’s Administrator to configure the application based on their specific requirements through a declarative framework (point and click).    The organization administrator (appointed by the State and not by Salesforce) has access to the admin interfaces in order to...   * configure organization default settings (Time Zones, Currency) * set login constraints (SSO, 2 Factor Authentication, IP range) * role-based access control and role-hierarchies * add new users, reset passwords * define customer objects, custom fields, set default pick-list values, custom reports * manage delegated administration * other functions (session timeout, password policies)   The organization administrator logs onto the application like other users within the organization; however, they have admin privileges granted to them which provide them with this additional access.    Administrators can also access a subset of functions using a mobile device via the Salesforce Application. Once downloaded the admin can manage users, reset passwords, applications, profiles and permission sets from their mobile device. | | | | | |
| SEC-7 | Describe how the system supports the use of multi-factor authentication. | X | X |  |  |
| Response:  **Authentication**  Logon is form-based. When users log into the Salesforce application, they submit a username and password, which are sent to Salesforce via an TLS-encrypted session. Security features are developed by Salesforce and built into the application. Third-party packages are not used for development or implementation of security internal to the application.    In addition, single sign-on and two-factor authentication may be used to authenticate users for both standard users and Community users. Some organizations prefer to use an existing single sign-on capability to simplify and standardize their user authentication. You have two options to implement single sign-on—federated authentication using Security Assertion Markup Language (SAML) or delegated authentication.    Federated authentication using SAML allows you to send authentication and authorization data between affiliated but unrelated Web services. This enables you to sign-on to Salesforce from a client application. Federated authentication using SAML is enabled by default for the State.    Delegated authentication single sign-on enables you to integrate Salesforce with an authentication method that you choose. This enables you to integrate authentication with your LDAP (Lightweight Directory Access Protocol) server, or perform single sign-on by authenticating using a token instead of a password. You manage delegated authentication at the profile level, allowing some users to use delegated authentication, while other users continue to use their Salesforce-managed password. Delegated authentication is set by profile, not organization wide. You must request that this feature be enabled by Salesforce.    Salesforce can be configured to utilize Active Directory directly via Delegated Authentication, or indirectly via Federated Identity using either SAML 1.1, or SAML 2.0. Additionally your users can be loaded from information drawn from your Active Directory servers and modifications made in Active Directory can be propagated into Salesforce.  Customers can use their own SAML Identity Provider, or license one directly from Salesforce with our Identity Connect product. | | | | | |
| SEC-8 | Describe any security processes for managing security updates, and integrated components subject to vulnerability, including anti-virus. |  |  |  |  |
| Response:  **Government Trusted Security and Infrastructure**  Salesforce understands that the confidentiality, integrity, and availability of our customers’ information are vital to their business operations and Salesforce's own success. Salesforce uses a multi-layered approach to protect that key information, constantly monitoring and improving our application, systems, and processes to meet the growing demands and challenges of security.    Independent audits confirm that our security goes far beyond what most companies have been able to achieve on their own. Using the latest firewall protection, intrusion detection systems, and TLS encryption, Salesforce gives you the peace of mind only a world-class security infrastructure can provide.    Third-party validation  Security is a multidimensional business imperative that demands consideration at multiple levels, from security for applications to physical facilities and network security. In addition to the latest technologies, world-class security requires ongoing adherence to best-practice policies. To ensure this adherence, we continually seek relevant third-party certification, including ISO 27001, the SysTrust audit (the recognized standard for system security), and SSAE 16 SOC 1 audit (an examination and assessment of internal corporate controls, previously known as SAS 70 Type II). SOC1, SOC2 and SOC3 audits are performed by a third-party auditor annually at a minimum. Additional audits and certifications include CSA ‘Consensus Assessments Initiative’, JIPDC (Japan Privacy Seal), Tuv (Germany Privacy Mark), and TRUSTe.    Protection at the application level  Salesforce protects customer data by ensuring that only authorized users can access it. Administrators assign data security rules that determine which data users can access. Sharing models define organization-wide defaults and data access based on a role hierarchy. All data is encrypted in transfer. All access is governed by strict password security policies. All passwords are stored in SHA 256 one-way hash format. Applications are continually monitored for security violation attempts.    Protection at the facilities level  Salesforce security standards are stringent and designed with demanding customers in mind, including the world’s most security-conscious financial institutions. Authorized personnel must pass through five levels of biometric scanning to reach the Salesforce system cages. All buildings are completely anonymous, with bullet-resistant exterior walls and embassy-grade concrete posts and planters around the perimeter. All exterior entrances feature silent alarm systems that notify law enforcement in the event of suspicion or intrusion. Data is backed up to disk. These backups provide a second level of physical protection and disks never leave the data center.    Protection at the network level  Multilevel security products from leading security vendors and proven security practices ensure network security. To prevent malicious attacks through unmonitored ports, external firewalls allow only http and https traffic on ports 80 and 443, along with ICMP traffic. Switches ensure that the network complies with the RFC 1918 standard, and address translation technologies further enhance network security. IDS sensors protect all network segments. Internal software systems are protected by two-factor authentication, along with the extensive use of technology that controls points of entry. All networks are certified through third-party vulnerability assessment programs.    Trust.salesforce.com is the Salesforce community’s home for real-time information on system performance and security. On this site you'll find:   * Up-to-the minute information on planned maintenance * Phishing, malicious software, and social engineering threats * Best security practices for the State * Information on how we safeguard your data     These papers further explain the technology that makes the Salesforce Platform fast, scalable, and secure for any type of application:  <https://developer.salesforce.com/page/Multi_Tenant_Architecture>  <https://trust.salesforce.com/en/trust-and-compliance-documentation/>  **Anti-Virus**  Salesforce currently runs anti-virus software on the production systems, which are Linux based. Other controls are also used to address malware such as hardening the Operating System of servers, firewall configuration to ensure only required ports are open and all others denied, and implementing intrusion detection systems. Access to these systems is restricted to authorized personnel and all these systems, as well as the host platforms, are monitored in real-time through a security monitoring system. | | | | | |
| SEC-9 | Describe how the system provides the ability to maintain a directory of all personnel who currently use or access the system. | X | X |  |  |
| Response:  **User Profiles**  All users and application-level security are defined and maintained by the organization administrator, and not by Salesforce. The organization administrator is appointed by the customer. An organization's sharing model sets the default access that users have to each other's data.    There are four sharing models: Private, Public Read Only, Public Read/Write, and Public Read/Write/Transfer. There are also several sharing model elements: Profiles, Roles, Hierarchy, Record Types, Page Layouts, and Field-Level security. Details about sharing models and sharing model elements are provided below:    Private  Only the record owner, and users above that role in the hierarchy, can view, edit, and report on those records.    Public Read Only  All users can view and report on records but not edit them. Only the owner, and users above that role in the hierarchy, can edit those records.    Public Read/Write  All users can view, edit, and report on all records.    Public Read/Write/Transfer  All users can view, edit, transfer, and report on all records. Only available for cases or leads.    Profiles  A profile contains the settings and permissions that control what users with that profile can do within Salesforce. Profiles control:   * Standard and custom apps the user can view (depending on user license) * Service providers the user can access * Tabs the user can view (depending on user license and other factors, such as access to Salesforce CRM Content) * Administrative and general permissions the user has for managing the organization and apps within it * Object permissions the user is granted to create, read, edit, and delete records * Page layouts a user sees * Field-level security access that the user has to view and edit specific fields * Record types are available to the user * Desktop client’s users can access and related options * Hours during which and IP addresses from which the user can log in * Apex classes a user can execute * Visualforce pages a user can access     User Roles  Every user must be assigned to a role, or their data will not display in reports and other displays based on roles. All users that require visibility to the entire organization should be assigned the highest level in the hierarchy. It is not necessary to create individual roles for each title at the organization, rather a hierarchy of roles should be defined to control access of information entered by users in lower level roles. When a user's role is changed, any relevant sharing rules are reevaluated to add or remove access as necessary.    Record Types  If the customer's organization uses record types, edit the record type to modify which pick list values are visible for the record type. A default pick list values can be set based upon the record type for various divisions.    Field-Level Security  Field-level security settings let administrators restrict user's access to view and edit specific fields on detail and edit pages and in related lists, list views, reports, Offline Edition, search results, email and mail merge templates, Custom Links, and when synchronizing data.    The fields that users see in detail and edit pages are a combination of page layouts and field-level security settings. The most restrictive field access settings of the two always apply. For example, if a field is required in the page layout and read-only in the field-level security settings, the field-level security overrides the page layout and the field will be read-only for the user.    Permission Sets  A permission set is a collection of settings and permissions that give users access to various tools and functions. The settings and permissions in permission sets are also found in profiles, but permission sets extend users’ functional access without changing their profiles.    Users can have only one profile but, depending on the Salesforce edition, they can have multiple permission sets. You can assign permission sets to various types of users, regardless of their profiles. The State can create permission sets to grant access among logical groupings of users, regardless of their primary job function.    See more information at: <https://help.salesforce.com/articleView?id=perm_sets_overview.htm&type=5>.  **Core Auditing Capabilities**  Within Salesforce, the creator and last updater, as well as timestamps, are recorded for every record. Additionally, the Salesforce Platform and Salesforce Applications have a multitude of history tracking and auditing features that provide valuable information about the use of an organization’s applications and data, which in turn can be a critical tool in diagnosing potential or real security issues. Auditing features include:    Record Modification Fields - All objects include fields to store the name of the user who created the record and who last modified the record. This provides some basic auditing information.    Field History Tracking - Enable auditing for individual fields (up to 20 fields per object), which will automatically track any changes in the values of selected fields. Although auditing is available for all custom objects, only some standard objects allow field-level auditing.    Login History - Review up to 20,000 successful and failed login attempts to the State for the past six months. The State can also track the geographic location of the IP addresses of your logins in your personal settings. You can track the geographic location of the login IP addresses for any of your users in the user’s detail page. To get more detailed geographic information, such as city and postal code, you can download the login history. Due to the nature of geolocation technology, the accuracy of geolocation fields (for example, country, city, postal code) can vary.    Identity Verification History - Review up to 20,000 records of your org users’ identity verification attempts from the past six months. For example, suppose that two-factor authentication is enabled when a user logs in. When the user successfully provides a time-based, one-time password as proof of identity, that information is recorded in Identity Verification History.    Setup Audit Trail - Administrators can view a Setup Audit Trail for the past six months within Salesforce, which logs when modifications are made to the State's configuration.    While the Login History and Setup Audit Trail are available for six months within Salesforce, they can be downloaded and stored locally to meet longer audit log retention requirements. Additionally, historic event logs which provide more information can be provided for a fee. For more information, please see<https://help.salesforce.com/articleView?id=000336835&language=en_US&type=1&mode=1>. | | | | | |
| SEC-10 | The State of Nebraska requires authentication and authorization of users through an enterprise directory known as the Nebraska Directory Services (NDS) to access web-based applications. Describe how the system will integrate NDS authentication.  Refer to the Nebraska Information Technology Commission Security Architecture – Authentication and Authorization – Identity and Access Management Standard for State Government Agencies (8-303) for specific requirements:  <https://nitc.nebraska.gov/standards/8-303.pdf> |  | x |  |  |
| Response:  **Authentication**  MST will Logon is form-based. When users log into the Salesforce application, they submit a username and password, which are sent to Salesforce via an TLS-encrypted session. Security features are developed by Salesforce and built into the application. Third-party packages are not used for development or implementation of security internal to the application.  In addition, single sign-on and two-factor authentication may be used to authenticate users for both standard users and Community users. Some organizations prefer to use an existing single sign-on capability to simplify and standardize their user authentication. You have two options to implement single sign-on—federated authentication using Security Assertion Markup Language (SAML) or delegated authentication.  Federated authentication using SAML allows you to send authentication and authorization data between affiliated but unrelated Web services. This enables you to sign-on to Salesforce from a client application. Federated authentication using SAML is enabled by default for the State.  Delegated authentication single sign-on enables you to integrate Salesforce with an authentication method that you choose. This enables you to integrate authentication with your LDAP (Lightweight Directory Access Protocol) server or perform single sign-on by authenticating using a token instead of a password. You manage delegated authentication at the profile level, allowing some users to use delegated authentication, while other users continue to use their Salesforce-managed password. Delegated authentication is set by profile, not organization wide. You must request that this feature be enabled by Salesforce.  Salesforce can be configured to utilize Active Directory directly via Delegated Authentication, or indirectly via Federated Identity using either SAML 1.1, or SAML 2.0. Additionally, your users can be loaded from information drawn from your Active Directory servers and modifications made in Active Directory can be propagated into Salesforce.  Customers can use their own SAML Identity Provider, or license one directly from Salesforce with our Identity Connect product. | | | | | |
| SEC-11 | Describe how the system provides rule-based security and allows restricted access to system features, function, screens, fields, database, etc. Role authentication may occur at the directory level, application level, or database level (depending on database system). Describe the security administration functions integrated into the system that manage role-based access to system functions, features, and data. Include a description of:   1. How and where the system stores security attributes or roles (e.g., LDAP attributes, database tables, files). 2. The interface between the LDAP and the application, if roles are assigned in an LDAP directory. 3. How roles are created and security is applied to the role based on how and where security attributes are stored (if multiple options describe each). 4. How groups are defined and how roles and security are applied to each group. 5. How access limits are applied to screens and data on screens by role or group. 6. How users are created and assigned to one or more roles or groups. 7. How role and group creation and assignment activity is logged. | X | X |  |  |
| Response:  **Authentication**  Logon is form-based. When users log into the Salesforce application, they submit a username and password, which are sent to Salesforce via an TLS-encrypted session. Security features are developed by Salesforce and built into the application. Third-party packages are not used for development or implementation of security internal to the application.    In addition, single sign-on and two-factor authentication may be used to authenticate users for both standard users and Community users. Some organizations prefer to use an existing single sign-on capability to simplify and standardize their user authentication. You have two options to implement single sign-on—federated authentication using Security Assertion Markup Language (SAML) or delegated authentication.    Federated authentication using SAML allows you to send authentication and authorization data between affiliated but unrelated Web services. This enables you to sign-on to Salesforce from a client application. Federated authentication using SAML is enabled by default for the State.    Delegated authentication single sign-on enables you to integrate Salesforce with an authentication method that you choose. This enables you to integrate authentication with your LDAP (Lightweight Directory Access Protocol) server or perform single sign-on by authenticating using a token instead of a password. You manage delegated authentication at the profile level, allowing some users to use delegated authentication, while other users continue to use their Salesforce-managed password. Delegated authentication is set by profile, not organization wide. You must request that this feature be enabled by Salesforce.    Salesforce can be configured to utilize Active Directory directly via Delegated Authentication, or indirectly via Federated Identity using either SAML 1.1, or SAML 2.0. Additionally, your users can be loaded from information drawn from your Active Directory servers and modifications made in Active Directory can be propagated into Salesforce.    Customers can use their own SAML Identity Provider, or license one directly from Salesforce with our Identity Connect product.  **User Profiles**  All users and application-level security are defined and maintained by the organization administrator, and not by Salesforce. The organization administrator is appointed by the customer. An organization's sharing model sets the default access that users have to each other's data.    There are four sharing models: Private, Public Read Only, Public Read/Write, and Public Read/Write/Transfer. There are also several sharing model elements: Profiles, Roles, Hierarchy, Record Types, Page Layouts, and Field-Level security. Details about sharing models and sharing model elements are provided below:    Private  Only the record owner, and users above that role in the hierarchy, can view, edit, and report on those records.    Public Read Only  All users can view and report on records but not edit them. Only the owner, and users above that role in the hierarchy, can edit those records.    Public Read/Write  All users can view, edit, and report on all records.    Public Read/Write/Transfer  All users can view, edit, transfer, and report on all records. Only available for cases or leads.    Profiles  A profile contains the settings and permissions that control what users with that profile can do within Salesforce. Profiles control:   * Standard and custom apps the user can view (depending on user license) * Service providers the user can access * Tabs the user can view (depending on user license and other factors, such as access to Salesforce CRM Content) * Administrative and general permissions the user has for managing the organization and apps within it * Object permissions the user is granted to create, read, edit, and delete records * Page layouts a user sees * Field-level security access that the user has to view and edit specific fields * Record types are available to the user * Desktop clients users can access and related options * Hours during which and IP addresses from which the user can log in * Apex classes a user can execute * Visualforce pages a user can access     User Roles  Every user must be assigned to a role, or their data will not display in reports and other displays based on roles. All users that require visibility to the entire organization should be assigned the highest level in the hierarchy. It is not necessary to create individual roles for each title at the organization, rather a hierarchy of roles should be defined to control access of information entered by users in lower level roles. When a user's role is changed, any relevant sharing rules are reevaluated to add or remove access as necessary.    Record Types  If the customer's organization uses record types, edit the record type to modify which pick list values are visible for the record type. A default pick list values can be set based upon the record type for various divisions.    Field-Level Security  Field-level security settings let administrators restrict user's access to view and edit specific fields on detail and edit pages and in related lists, list views, reports, Offline Edition, search results, email and mail merge templates, Custom Links, and when synchronizing data.    The fields that users see in detail and edit pages are a combination of page layouts and field-level security settings. The most restrictive field access settings of the two always apply. For example, if a field is required in the page layout and read-only in the field-level security settings, the field-level security overrides the page layout and the field will be read-only for the user.    Permission Sets  A permission set is a collection of settings and permissions that give users access to various tools and functions. The settings and permissions in permission sets are also found in profiles, but permission sets extend users’ functional access without changing their profiles.    Users can have only one profile but, depending on the Salesforce edition, they can have multiple permission sets. You can assign permission sets to various types of users, regardless of their profiles. The State can create permission sets to grant access among logical groupings of users, regardless of their primary job function.    See more information at: <https://help.salesforce.com/articleView?id=perm_sets_overview.htm&type=5>.  **Core Auditing Capabilities**  Within Salesforce, the creator and last updater, as well as timestamps, are recorded for every record. Additionally, the Salesforce Platform and Salesforce Applications have a multitude of history tracking and auditing features that provide valuable information about the use of an organization’s applications and data, which in turn can be a critical tool in diagnosing potential or real security issues. Auditing features include:    Record Modification Fields - All objects include fields to store the name of the user who created the record and who last modified the record. This provides some basic auditing information.    Field History Tracking - Enable auditing for individual fields (up to 20 fields per object), which will automatically track any changes in the values of selected fields. Although auditing is available for all custom objects, only some standard objects allow field-level auditing.  Login History - Review up to 20,000 successful and failed login attempts to the State for the past six months. The State can also track the geographic location of the IP addresses of your logins in your personal settings. You can track the geographic location of the login IP addresses for any of your users in the user’s detail page. To get more detailed geographic information, such as city and postal code, you can download the login history. Due to the nature of geolocation technology, the accuracy of geolocation fields (for example, country, city, postal code) can vary.  Identity Verification History - Review up to 20,000 records of your org users’ identity verification attempts from the past six months. For example, suppose that two-factor authentication is enabled when a user logs in. When the user successfully provides a time-based, one-time password as proof of identity, that information is recorded in Identity Verification History.  Setup Audit Trail - Administrators can view a Setup Audit Trail for the past six months within Salesforce, which logs when modifications are made to the State's configuration.  While the Login History and Setup Audit Trail are available for six months within Salesforce, they can be downloaded and stored locally to meet longer audit log retention requirements. Additionally, historic event logs which provide more information can be provided for a fee. For more information, please see<https://help.salesforce.com/articleView?id=000336835&language=en_US&type=1&mode=1>. | | | | | |
| SEC-12 | The system must automatically disconnect based upon inactivity, as required by DHHS Security Policies and Standards.  Describe how the feature is administered and what effect disconnect has on any activity or transaction in process at the time of disconnection.  Refer to DHHS Securing Hardware and Software Standard (DHHS-IT-2018-001A) for specific requirements: <http://dhhs.ne.gov/ITSecurity> | X | X |  |  |
| Response:  Configurable by the Administrator. Sessions may be configured to timeout after 15 minutes up to 24 hours of inactivity, at which time the user is automatically logged out. | | | | | |
| SEC-13 | The system must protect confidential and highly restricted data from unauthorized access during transmission. Describe transmission safeguards that are integrated into the proposed system to protect data during transmission, including any encryption technology.  Refer to DHHS Information Technology (IT) Security Policy (DHHS-IT-2018-001) for specific requirements: <http://dhhs.ne.gov/ITSecurity> | X | X |  |  |
| Response:  **Encryption Capabilities**  Salesforce has many customers that are subject to laws pertaining to the processing of personally identifiable information (PII) or personal data. Salesforce offers its customers a broad spectrum of functionalities and customer-controlled security features that its customers may implement in their respective uses of the Salesforce services. Salesforce believes that these provide its customers the flexibility to comply with laws with stringent privacy and security requirements.  Data In Motion  All transmissions between the user and the Salesforce Services are TLS 1.2 encrypted with a 2048-bit Public Key, using AES 256-bit encryption by default.  Data At Rest  Salesforce Classic Encryption includes a feature to encrypt custom text fields (ECF):   * The fields can be masked appropriately for specific data types (i.e., credit card number, Social Security Number, National Insurance Number, Social Insurance Number). * Access to read the masked parts of the fields is limited by the "View Encrypted Data" permission, which is not enabled by default. * Customers can manage their encryption key based on their organization’s security needs and regulatory requirements. See our Help and Training site for details: <https://help.salesforce.com/apex/HTViewHelpDoc?id=security_keys_using_master.htm&language=en> * Encrypted fields use 128-bit encryption and the AES (Advanced Encryption Standard) algorithm * Custom text fields can be up to 175 characters in length   Additional Salesforce Encryption Capabilities  Apex Code extends the powerful and proven success of the Salesforce Platform by introducing the ability to write code that runs on Salesforce servers. This language makes possible the development of a new class of application and features deployed entirely on demand. Using Apex, the State can create user interface classes that utilize the Apex crypto class to encrypt field level data up to AES 256-bit encryption. Please see here for more information: <https://developer.salesforce.com/page/Apex_Crypto_Class>.  **Salesforce Platform Encryption**  Salesforce Classic Encryption is limited to encrypting custom text fields of 175 characters or less, while Salesforce offers Salesforce Platform Encryption as an additional licensing option for encrypting standard and custom fields of various types, attachments, files, and other content using AES 256-bit encryption.  Salesforce Platform Encryption sets up in minutes, with no additional hardware or software, and uses native strong, standards-based encryption. Platform Encryption provides an extra layer to Salesforce's security while enabling customers to enjoy business critical Platform features, such as search, workflow, and validation rules.  The State can use Platform Encryption so that the State can confidently prove compliance with privacy policies, regulatory requirements, and contractual obligations for handling private data.  Platform Encryption offers native platform encryption and key management features. By default, the State's data is encrypted at rest using a hardware security module-based key derivation system. These features allow the State to protect data at a more granular level than Classic Encryption while still giving users the ability to perform necessary tasks. The State can:   * Encrypt files and attachments (including email attachments) * Encrypt certain standard and custom fields * Encrypt Knowledge article fields and attachments * Encrypt certain Chatter data such as feed posts and comments, feed questions and answers, link labels and URLs, and feed polls and poll choices * Encrypt transcribed conversations (e.g. between agents and customers) * Access encrypted data from most elements in flows and processes, except when filtering or sorting records * Use the Shield Key Management System (KMS) to generate your org-specific tenant secret and data encryption key   Platform Encryption helps address some concerns about protecting confidential information. It prevents sensitive data from being stored in clear, decipherable form and allows you to manage your tenant secrets, which are used to derive the keys that protect your data. Salesforce is committed to high security standards and offers multiple data encryption options. Customers who want to adopt or extend their use of Salesforce can consider using Platform Encryption to comply with various standards. Additional details on Salesforce Platform Encryption are provided in these white papers: <https://a.sfdcstatic.com/content/dam/www/ocms/assets/pdf/platform/whitepaper-platform-shield.pdf> and <https://org62.my.salesforce.com/sfc/p/000000000062/a/0M000000Htiv/0pEjEbyFd3.Yp1XI_zC1I6xuel9EsD0f.VKrwVFu64k>. Please also refer to Platform Encryption Best Practices outlined at: <https://help.salesforce.com/articleView?id=security_pe_best_practices.htm&language=en_US&type=0>.  In addition to the default Shield KMS service, multiple options are available for generating and managing your tenant secrets and data encryption keys outside of Salesforce, for added control and flexibility. With the Bring Your Own Key (BYOK) service, you have two options to manage your encryption key lifecycle: 1) use the infrastructure of your choice to generate a tenant secret and upload to the Shield KMS or 2) use the infrastructure of your choice to create a data encryption key instead of a tenant secret and upload to the Shield KMS. Additionally, with the Cache-Only Key Service you can store your key material outside of Salesforce and fetch your key on demand from a key service that you control. Additional details on the BYOK service are provided at <https://help.salesforce.com/articleView?id=security_pe_byok_setup.htm&type=5>. Additional details on the Cache-Only Key service are provided at <https://help.salesforce.com/articleView?id=security_pe_byok_cache.htm&type=0>. | | | | | |
| SEC-14 | The system must provide auditing functions for all data fields, including but not limited to:   1. The user ID of the person who made the change. 2. The date and time of the change. 3. The physical, software/hardware and/or network location of the person while making the change. 4. The information that was changed. 5. The outcome of the event. 6. The data before and after it was changed, and which screens were accessed and used.   Refer to DHHS Information Technology (IT) Audit Standard (DHHS-IT-2018-001F DHHS IT Audit Standard) for specific audit requirements: <http://dhhs.ne.gov/ITSecurity> | X | X |  |  |
| Response:  **Core Auditing Capabilities**  Within Salesforce, the creator and last updater, as well as timestamps, are recorded for every record. Additionally, the Salesforce Platform and Salesforce Applications have a multitude of history tracking and auditing features that provide valuable information about the use of an organization’s applications and data, which in turn can be a critical tool in diagnosing potential or real security issues. Auditing features include:    Record Modification Fields - All objects include fields to store the name of the user who created the record and who last modified the record. This provides some basic auditing information.    Field History Tracking - Enable auditing for individual fields (up to 20 fields per object), which will automatically track any changes in the values of selected fields. Although auditing is available for all custom objects, only some standard objects allow field-level auditing.    Login History - Review up to 20,000 successful and failed login attempts to the State for the past six months. The State can also track the geographic location of the IP addresses of your logins in your personal settings. You can track the geographic location of the login IP addresses for any of your users in the user’s detail page. To get more detailed geographic information, such as city and postal code, you can download the login history. Due to the nature of geolocation technology, the accuracy of geolocation fields (for example, country, city, postal code) can vary.    Identity Verification History - Review up to 20,000 records of your org users’ identity verification attempts from the past six months. For example, suppose that two-factor authentication is enabled when a user logs in. When the user successfully provides a time-based, one-time password as proof of identity, that information is recorded in Identity Verification History.    Setup Audit Trail - Administrators can view a Setup Audit Trail for the past six months within Salesforce, which logs when modifications are made to the State's configuration.    While the Login History and Setup Audit Trail are available for six months within Salesforce, they can be downloaded and stored locally to meet longer audit log retention requirements. Additionally, historic event logs which provide more information can be provided for a fee. For more information, please see<https://help.salesforce.com/articleView?id=000336835&language=en_US&type=1&mode=1>. | | | | | |
| SEC-15 | The system must provide auditing functions for confidential and highly restricted data that is accessed and viewed, regardless of whether the data was changed. Describe the auditing functions which must include but not be limited to:   1. The user ID of the person who viewed the data. 2. The date and time of the viewed data. 3. The physical, software/hardware and/or network location of the person viewing the data. 4. The information that was viewed.   Refer to DHHS Information Technology (IT) Audit Standard (DHHS-IT-2018-001F DHHS IT Audit Standard) for specific audit requirements: <http://dhhs.ne.gov/ITSecurity> |  | x |  |  |
| Response:  This functionality will be available as part of the Event Monitoring Package from Shield. The API Event Stream Event in Event Monitoring can detect when a user queries sensitive data, such as patient records and stream this data to an event subscriber. This Event data is available only in Real-Time Event Monitoring with Salesforce Shield.  **Core Auditing Capabilities**  Within Salesforce, the creator and last updater, as well as timestamps, are recorded for every record. Additionally, the Salesforce Platform and Salesforce Applications have a multitude of history tracking and auditing features that provide valuable information about the use of an organization’s applications and data, which in turn can be a critical tool in diagnosing potential or real security issues. Auditing features include:  Record Modification Fields - All objects include fields to store the name of the user who created the record and who last modified the record. This provides some basic auditing information.  Field History Tracking - Enable auditing for individual fields (up to 20 fields per object), which will automatically track any changes in the values of selected fields. Although auditing is available for all custom objects, only some standard objects allow field-level auditing.  Login History - Review up to 20,000 successful and failed login attempts to the State for the past six months. The State can also track the geographic location of the IP addresses of your logins in your personal settings. You can track the geographic location of the login IP addresses for any of your users in the user’s detail page. To get more detailed geographic information, such as city and postal code, you can download the login history. Due to the nature of geolocation technology, the accuracy of geolocation fields (for example, country, city, postal code) can vary.    Identity Verification History - Review up to 20,000 records of your org users’ identity verification attempts from the past six months. For example, suppose that two-factor authentication is enabled when a user logs in. When the user successfully provides a time-based, one-time password as proof of identity, that information is recorded in Identity Verification History.    Setup Audit Trail - Administrators can view a Setup Audit Trail for the past six months within Salesforce, which logs when modifications are made to the State's configuration.  While the Login History and Setup Audit Trail are available for six months within Salesforce, they can be downloaded and stored locally to meet longer audit log retention requirements. Additionally, historic event logs which provide more information can be provided for a fee. For more information, please see<https://help.salesforce.com/articleView?id=000336835&language=en_US&type=1&mode=1>. | | | | | |
| SEC-16 | If the system has the ability to override edits, describe how the system audits all overridden edits and identifies information including, but not limited to, the login ID, date, and time. | X | X |  |  |
| Response:  **Core Auditing Capabilities**  Within Salesforce, the creator and last updater, as well as timestamps, are recorded for every record. Additionally, the Salesforce Platform and Salesforce Applications have a multitude of history tracking and auditing features that provide valuable information about the use of an organization’s applications and data, which in turn can be a critical tool in diagnosing potential or real security issues. Auditing features include:  Record Modification Fields - All objects include fields to store the name of the user who created the record and who last modified the record. This provides some basic auditing information.  Field History Tracking - Enable auditing for individual fields (up to 20 fields per object), which will automatically track any changes in the values of selected fields. Although auditing is available for all custom objects, only some standard objects allow field-level auditing.  Login History - Review up to 20,000 successful and failed login attempts to the State for the past six months. The State can also track the geographic location of the IP addresses of your logins in your personal settings. You can track the geographic location of the login IP addresses for any of your users in the user’s detail page. To get more detailed geographic information, such as city and postal code, you can download the login history. Due to the nature of geolocation technology, the accuracy of geolocation fields (for example, country, city, postal code) can vary.  Identity Verification History - Review up to 20,000 records of your org users’ identity verification attempts from the past six months. For example, suppose that two-factor authentication is enabled when a user logs in. When the user successfully provides a time-based, one-time password as proof of identity, that information is recorded in Identity Verification History  Setup Audit Trail - Administrators can view a Setup Audit Trail for the past six months within Salesforce, which logs when modifications are made to the State's configuration.  While the Login History and Setup Audit Trail are available for six months within Salesforce, they can be downloaded and stored locally to meet longer audit log retention requirements. Additionally, historic event logs which provide more information can be provided for a fee. For more information, please see<https://help.salesforce.com/articleView?id=000336835&language=en_US&type=1&mode=1>. | | | | | |
| SEC-17 | Describe how the system produces daily audit trail reports and allows inquiries, showing updates applied to the data. | X | X |  |  |
| Response:  **Core Auditing Capabilities**  Within Salesforce, the creator and last updater, as well as timestamps, are recorded for every record. Additionally, the Salesforce Platform and Salesforce Applications have a multitude of history tracking and auditing features that provide valuable information about the use of an organization’s applications and data, which in turn can be a critical tool in diagnosing potential or real security issues. Auditing features include:  Record Modification Fields - All objects include fields to store the name of the user who created the record and who last modified the record. This provides some basic auditing information.    Field History Tracking - Enable auditing for individual fields (up to 20 fields per object), which will automatically track any changes in the values of selected fields. Although auditing is available for all custom objects, only some standard objects allow field-level auditing.    Login History - Review up to 20,000 successful and failed login attempts to the State for the past six months. The State can also track the geographic location of the IP addresses of your logins in your personal settings. You can track the geographic location of the login IP addresses for any of your users in the user’s detail page. To get more detailed geographic information, such as city and postal code, you can download the login history. Due to the nature of geolocation technology, the accuracy of geolocation fields (for example, country, city, postal code) can vary.    Identity Verification History - Review up to 20,000 records of your org users’ identity verification attempts from the past six months. For example, suppose that two-factor authentication is enabled when a user logs in. When the user successfully provides a time-based, one-time password as proof of identity, that information is recorded in Identity Verification History.    Setup Audit Trail - Administrators can view a Setup Audit Trail for the past six months within Salesforce, which logs when modifications are made to the State's configuration.  While the Login History and Setup Audit Trail are available for six months within Salesforce, they can be downloaded and stored locally to meet longer audit log retention requirements. Additionally, historic event logs which provide more information can be provided for a fee. For more information, please see<https://help.salesforce.com/articleView?id=000336835&language=en_US&type=1&mode=1>. | | | | | |
| SEC-18 | Describe how the system provides an auto archive/purge of the log files to prevent uncontrolled growth of the log and historical records storage using administrator-set parameters. |  | x |  |  |
| Response:  **Retention**  Active customer data stays on disk until the customer deletes or changes it. Customer-deleted data is temporarily available (15 days) to customers online from the Recycle Bin. The retention policy for backup media is 90 days (30 days for sandboxes). Deleted / modified data cannot be recovered after 90 days (30 days for sandboxes).    Salesforce customers are responsible for complying with their company's data retention requirements in their use of the Salesforce Services. If a Salesforce customer must preserve data and the retention procedures above are insufficient, they may schedule a weekly export of data or copy to a sandbox account. Exports of Customer Data are available in comma separated value (.csv) format by request via Salesforce's Customer Support department. In addition, many exports can be manually pulled by the designated org administrators.  **Core Auditing Capabilities**  Within Salesforce, the creator and last updater, as well as timestamps, are recorded for every record. Additionally, the Salesforce Platform and Salesforce Applications have a multitude of history tracking and auditing features that provide valuable information about the use of an organization’s applications and data, which in turn can be a critical tool in diagnosing potential or real security issues. Auditing features include:  Record Modification Fields - All objects include fields to store the name of the user who created the record and who last modified the record. This provides some basic auditing information.    Field History Tracking - Enable auditing for individual fields (up to 20 fields per object), which will automatically track any changes in the values of selected fields. Although auditing is available for all custom objects, only some standard objects allow field-level auditing.  Login History - Review up to 20,000 successful and failed login attempts to the State for the past six months. The State can also track the geographic location of the IP addresses of your logins in your personal settings. You can track the geographic location of the login IP addresses for any of your users in the user’s detail page. To get more detailed geographic information, such as city and postal code, you can download the login history. Due to the nature of geolocation technology, the accuracy of geolocation fields (for example, country, city, postal code) can vary.  Identity Verification History - Review up to 20,000 records of your org users’ identity verification attempts from the past six months. For example, suppose that two-factor authentication is enabled when a user logs in. When the user successfully provides a time-based, one-time password as proof of identity, that information is recorded in Identity Verification History.  Setup Audit Trail - Administrators can view a Setup Audit Trail for the past six months within Salesforce, which logs when modifications are made to the State's configuration.  While the Login History and Setup Audit Trail are available for six months within Salesforce, they can be downloaded and stored locally to meet longer audit log retention requirements. Additionally, historic event logs which provide more information can be provided for a fee. For more information, please see<https://help.salesforce.com/articleView?id=000336835&language=en_US&type=1&mode=1>. | | | | | |
| SEC-19 | Describe how the system supports encryption of data at rest or an equivalent alternative protection mechanism. Describe the proposed encryption of data. If data is not encrypted, describe in detail compensating controls. | X | X |  |  |
| Response:  **Encryption Capabilities**  Salesforce has many customers that are subject to laws pertaining to the processing of personally identifiable information (PII) or personal data. Salesforce offers its customers a broad spectrum of functionalities and customer-controlled security features that its customers may implement in their respective uses of the Salesforce services. Salesforce believes that these provide its customers the flexibility to comply with laws with stringent privacy and security requirements.  Data In Motion  All transmissions between the user and the Salesforce Services are TLS 1.2 encrypted with a 2048-bit Public Key, using AES 256-bit encryption by default.  Data At Rest  Salesforce Classic Encryption includes a feature to encrypt custom text fields (ECF):   * The fields can be masked appropriately for specific data types (i.e., credit card number, Social Security Number, National Insurance Number, Social Insurance Number). * Access to read the masked parts of the fields is limited by the "View Encrypted Data" permission, which is not enabled by default. * Customers can manage their encryption key based on their organization’s security needs and regulatory requirements. See our Help and Training site for details: <https://help.salesforce.com/apex/HTViewHelpDoc?id=security_keys_using_master.htm&language=en> * Encrypted fields use 128-bit encryption and the AES (Advanced Encryption Standard) algorithm * Custom text fields can be up to 175 characters in length   Additional Salesforce Encryption Capabilities  Apex Code extends the powerful and proven success of the Salesforce Platform by introducing the ability to write code that runs on Salesforce servers. This language makes possible the development of a new class of application and features deployed entirely on demand. Using Apex, the State can create user interface classes that utilize the Apex crypto class to encrypt field level data up to AES 256-bit encryption. Please see here for more information: <https://developer.salesforce.com/page/Apex_Crypto_Class>.  **Salesforce Platform Encryption**  Salesforce Classic Encryption is limited to encrypting custom text fields of 175 characters or less, while Salesforce offers Salesforce Platform Encryption as an additional licensing option for encrypting standard and custom fields of various types, attachments, files, and other content using AES 256-bit encryption.    Salesforce Platform Encryption sets up in minutes, with no additional hardware or software, and uses native strong, standards-based encryption. Platform Encryption provides an extra layer to Salesforce's security while enabling customers to enjoy business critical Platform features, such as search, workflow, and validation rules.    The State can use Platform Encryption so that the State can confidently prove compliance with privacy policies, regulatory requirements, and contractual obligations for handling private data.  Platform Encryption offers native platform encryption and key management features. By default, the State's data is encrypted at rest using a hardware security module-based key derivation system. These features allow the State to protect data at a more granular level than Classic Encryption while still giving users the ability to perform necessary tasks. The State can:   * Encrypt files and attachments (including email attachments) * Encrypt certain standard and custom fields * Encrypt Knowledge article fields and attachments * Encrypt certain Chatter data such as feed posts and comments, feed questions and answers, link labels and URLs, and feed polls and poll choices * Encrypt transcribed conversations (e.g. between agents and customers) * Access encrypted data from most elements in flows and processes, except when filtering or sorting records * Use the Shield Key Management System (KMS) to generate your org-specific tenant secret and data encryption key   Platform Encryption helps address some concerns about protecting confidential information. It prevents sensitive data from being stored in clear, decipherable form and allows you to manage your tenant secrets, which are used to derive the keys that protect your data. Salesforce is committed to high security standards and offers multiple data encryption options. Customers who want to adopt or extend their use of Salesforce can consider using Platform Encryption to comply with various standards. Additional details on Salesforce Platform Encryption are provided in these white papers: <https://a.sfdcstatic.com/content/dam/www/ocms/assets/pdf/platform/whitepaper-platform-shield.pdf> and <https://org62.my.salesforce.com/sfc/p/000000000062/a/0M000000Htiv/0pEjEbyFd3.Yp1XI_zC1I6xuel9EsD0f.VKrwVFu64k>. Please also refer to Platform Encryption Best Practices outlined at: <https://help.salesforce.com/articleView?id=security_pe_best_practices.htm&language=en_US&type=0>.    In addition to the default Shield KMS service, multiple options are available for generating and managing your tenant secrets and data encryption keys outside of Salesforce, for added control and flexibility. With the Bring Your Own Key (BYOK) service, you have two options to manage your encryption key lifecycle: 1) use the infrastructure of your choice to generate a tenant secret and upload to the Shield KMS or 2) use the infrastructure of your choice to create a data encryption key instead of a tenant secret and upload to the Shield KMS. Additionally, with the Cache-Only Key Service you can store your key material outside of Salesforce and fetch your key on demand from a key service that you control. Additional details on the BYOK service are provided at <https://help.salesforce.com/articleView?id=security_pe_byok_setup.htm&type=5>. Additional details on the Cache-Only Key service are provided at <https://help.salesforce.com/articleView?id=security_pe_byok_cache.htm&type=0>. | | | | | |
| SEC-20 | Describe how the system adheres to the principle of "Fail Safe" to ensure that a system in a failed state does not reveal any sensitive information or leave any access controls open for attacks. | X | X |  |  |
| Response:  Redundant boundary protection devices are employed within the production network to allow for failover capabilities in the event that a device becomes inoperable. If a boundary protection device fails, devices fail securely (closed). Salesforce follows OWASP principles around information leakage and improper error handling.  All aspects of the Salesforce system are configured in an N+1 redundant configuration, where N is the number of components of a given type needed for the service to operate, and +1 is the redundancy. In many cases, Salesforce has more than one piece of redundant equipment for a given function. The infrastructure utilizes carrier-class components designed to support millions of users. Extensive use of high availability servers and network technologies, and a carrier-neutral network strategy, help to minimize the risk of single points of failure, and provide a highly resilient environment with maximum uptime and performance. | | | | | |
| SEC-21 | Describe how the system is configurable to prevent corruption or loss of data already entered into the system in the event of failure. | X | X |  |  |
| Response:  **Backup & Disaster Recovery**  Customer data, up to the last committed transaction, is replicated to disk in near-real time at the designated disaster recovery data center, backed up at the Active data center, and then cloned at a Ready data center. Disaster recovery tests verify our projected recovery times and the integrity of the customer data.  Backups are performed daily at each data center facility without stopping access to the application. Backup cloning is transmitted over an encrypted network (our MPLS network across all data centers). Backups never leave our secure data center facilities, unless they are to be retired and destroyed through a secure destruction process.  The backup retention policy is 90 days (30 days for sandboxes). Deleted / modified data cannot be recovered after 90 days (30 days for sandboxes). If customers want a longer retention, they can use the weekly export feature available in the system.  **RTO/RPO**  Our Recovery Time Objective (RTO) is 12 hours and Recovery Point Objective (RPO) is 4 hours.    Salesforce's disaster recovery plans currently have the following target recovery objectives: (a) restoration of the Service within 12 hours after Salesforce's declaration of a disaster; and (b) maximum Customer Data loss of 4 hours; excluding, however, a disaster or multiple disasters causing the compromise of both multiple Salesforce data centers at the same time, and excluding development and test bed environments, such as the Sandbox service. | | | | | |
| SEC-22 | Describe how the system, upon access, displays a message banner indicating that this application is only to be accessed by those individuals who are authorized to use the system. | X | X |  |  |
| Response:  **User Profile**  This is configurable by the State’s Administrator.  All users and application-level security are defined and maintained by the organization administrator, and not by Salesforce. The organization administrator is appointed by the customer. An organization's sharing model sets the default access that users have to each other's data.    There are four sharing models: Private, Public Read Only, Public Read/Write, and Public Read/Write/Transfer. There are also several sharing model elements: Profiles, Roles, Hierarchy, Record Types, Page Layouts, and Field-Level security. Details about sharing models and sharing model elements are provided below:    Private  Only the record owner, and users above that role in the hierarchy, can view, edit, and report on those records.    Public Read Only  All users can view and report on records but not edit them. Only the owner, and users above that role in the hierarchy, can edit those records.    Public Read/Write  All users can view, edit, and report on all records.    Public Read/Write/Transfer  All users can view, edit, transfer, and report on all records. Only available for cases or leads.    Profiles  A profile contains the settings and permissions that control what users with that profile can do within Salesforce. Profiles control:   * Standard and custom apps the user can view (depending on user license) * Service providers the user can access * Tabs the user can view (depending on user license and other factors, such as access to Salesforce CRM Content) * Administrative and general permissions the user has for managing the organization and apps within it * Object permissions the user is granted to create, read, edit, and delete records * Page layouts a user sees * Field-level security access that the user has to view and edit specific fields * Record types are available to the user * Desktop clients users can access and related options * Hours during which and IP addresses from which the user can log in * Apex classes a user can execute * Visualforce pages a user can access     User Roles  Every user must be assigned to a role, or their data will not display in reports and other displays based on roles. All users that require visibility to the entire organization should be assigned the highest level in the hierarchy. It is not necessary to create individual roles for each title at the organization, rather a hierarchy of roles should be defined to control access of information entered by users in lower level roles. When a user's role is changed, any relevant sharing rules are reevaluated to add or remove access as necessary.    Record Types  If the customer's organization uses record types, edit the record type to modify which pick list values are visible for the record type. A default pick list values can be set based upon the record type for various divisions.    Field-Level Security  Field-level security settings let administrators restrict user's access to view and edit specific fields on detail and edit pages and in related lists, list views, reports, Offline Edition, search results, email and mail merge templates, Custom Links, and when synchronizing data.    The fields that users see in detail and edit pages are a combination of page layouts and field-level security settings. The most restrictive field access settings of the two always apply. For example, if a field is required in the page layout and read-only in the field-level security settings, the field-level security overrides the page layout and the field will be read-only for the user.    Permission Sets  A permission set is a collection of settings and permissions that give users access to various tools and functions. The settings and permissions in permission sets are also found in profiles, but permission sets extend users’ functional access without changing their profiles.    Users can have only one profile but, depending on the Salesforce edition, they can have multiple permission sets. You can assign permission sets to various types of users, regardless of their profiles. The State can create permission sets to grant access among logical groupings of users, regardless of their primary job function.  See more information at: <https://help.salesforce.com/articleView?id=perm_sets_overview.htm&type=5>. | | | | | |
| SEC-23 | Describe how the system, prior to access of any confidential or highly restricted data, displays a configurable warning or login banner (e.g. "The system must only be accessed by authorized users"). In the event that the system does not support pre-login capabilities, describe how the system displays the banner immediately following authorization. | X | x |  |  |
| Response: Login flows allow admins to build post-authentication processes to match their business practices, associate the flow with a user profile, and send the user through that flow when logging in. Salesforce directs users to the login flow after they authenticate but before they access your org or community. After users complete the login flow, they’re logged in to your Salesforce org or community. The login process can also log out users immediately if necessary.  What can you do with a login flow?   * Enhance or customize the login experience. For example, add a logo or login message. * Collect and update user data. For example, request an email address, phone number, or mailing address. * Interact with users and ask them to perform an action. For example, complete a survey or accept terms of service. * Connect to an external identity service or geo-fencing service and collect or verify user information. * Enforce strong authentication. For example, implement a two-factor authentication method using hardware, SMS, biometric, or another authentication technique. * Run a confirmation process. For example, have a user define a secret question, and validate the answer during login. * Create more granular policies. For example, set up a policy that sends a notification every time a user logs in during non-standard working hours.   The first step is to create a flow using either Flow Builder or Visualforce. Flow Builder is a point-and-click tool that you can use to design a simple flow that users execute when logging in. Use Visualforce to have complete control over how the login page looks and behaves.  Next, you designate the flow as a login flow and associate it with specific profiles in your org. You can create multiple login flows and associate each one with a different user profile. Users assigned to one profile, like sales reps, experience a particular login process as they log in. Users assigned to a different profile like service reps, experience a different login process.  After you associate a login flow with a profile, it is applied each time a user with that profile logs in to Salesforce, communities, the Salesforce app, and even Salesforce client applications that use OAuth. You can apply login flows to Salesforce orgs and communities, including external identity communities.  Login flows support all Salesforce authentication methods: standard username and password, delegated authentication, SAML single sign-on, and social sign-on through a third-party authentication provider. For example, users logging in with a LinkedIn account can go through a login flow specific for LinkedIn users | | | | | |
| Response:  Many Salesforce customers store protected health information (PHI) on our service.    The U.S. Centers for Medicare & Medicaid Services (CMS) guidelines (<http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/System-Security-Levels-by-Information-Type.pdf)> states that "Information related to personnel, medical, and similar data includes all information covered by the Privacy Act of 1974 (e.g., salary data, social security information, passwords, user identifiers (IDs), Equal Employment Opportunity (EEO), personnel profile (including home address and phone number), medical history, employment history (general and security clearance information), and arrest/criminal investigation history as well as personally identifiable information (PII), individually identifiable information (IIF), or personal health information (PHI) covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA)" should be considered Moderate for Confidentiality, Integrity, and Availability.    Salesforce's FedRAMP ATO is based on a Moderate System Security Level. Please note, Salesforce is not considered a "first-tier, downstream or related entity" for the purposes of compliance with CMS flow-down regulations.    Salesforce has also received a Provisional Authorization (PA) from Defense Information Systems Agency (DISA) at Impact Level 4 (IL4) to store, process, or transmit Controlled Unclassified Information (CUI) and/or other mission critical data to include that used in direct support of military or contingency operations. In addition to the DoD Cloud Computing SRG including PHI as a CUI category, the National Archives' CUI Registry (https://www.archives.gov/cui/registry/category-list) includes Health Information as a category under Privacy.  **User Profile**  This is configurable by the State’s Administrator.  All users and application-level security are defined and maintained by the organization administrator, and not by Salesforce. The organization administrator is appointed by the customer. An organization's sharing model sets the default access that users have to each other's data.  There are four sharing models: Private, Public Read Only, Public Read/Write, and Public Read/Write/Transfer. There are also several sharing model elements: Profiles, Roles, Hierarchy, Record Types, Page Layouts, and Field-Level security. Details about sharing models and sharing model elements are provided below:  Private  Only the record owner, and users above that role in the hierarchy, can view, edit, and report on those records.  Public Read Only  All users can view and report on records but not edit them. Only the owner, and users above that role in the hierarchy, can edit those records.  Public Read/Write  All users can view, edit, and report on all records.  Public Read/Write/Transfer  All users can view, edit, transfer, and report on all records. Only available for cases or leads.  Profiles  A profile contains the settings and permissions that control what users with that profile can do within Salesforce. Profiles control:   * Standard and custom apps the user can view (depending on user license) * Service providers the user can access * Tabs the user can view (depending on user license and other factors, such as access to Salesforce CRM Content) * Administrative and general permissions the user has for managing the organization and apps within it * Object permissions the user is granted to create, read, edit, and delete records * Page layouts a user sees * Field-level security access that the user has to view and edit specific fields * Record types are available to the user * Desktop clients users can access and related options * Hours during which and IP addresses from which the user can log in * Apex classes a user can execute * Visualforce pages a user can access   User Roles  Every user must be assigned to a role, or their data will not display in reports and other displays based on roles. All users that require visibility to the entire organization should be assigned the highest level in the hierarchy. It is not necessary to create individual roles for each title at the organization, rather a hierarchy of roles should be defined to control access of information entered by users in lower level roles. When a user's role is changed, any relevant sharing rules are reevaluated to add or remove access as necessary.  Record Types  If the customer's organization uses record types, edit the record type to modify which pick list values are visible for the record type. A default pick list values can be set based upon the record type for various divisions.  Field-Level Security  Field-level security settings let administrators restrict user's access to view and edit specific fields on detail and edit pages and in related lists, list views, reports, Offline Edition, search results, email and mail merge templates, Custom Links, and when synchronizing data.    The fields that users see in detail and edit pages are a combination of page layouts and field-level security settings. The most restrictive field access settings of the two always apply. For example, if a field is required in the page layout and read-only in the field-level security settings, the field-level security overrides the page layout and the field will be read-only for the user.  Permission Sets  A permission set is a collection of settings and permissions that give users access to various tools and functions. The settings and permissions in permission sets are also found in profiles, but permission sets extend users’ functional access without changing their profiles.  Users can have only one profile but, depending on the Salesforce edition, they can have multiple permission sets. You can assign permission sets to various types of users, regardless of their profiles. The State can create permission sets to grant access among logical groupings of users, regardless of their primary job function.  See more information at: <https://help.salesforce.com/articleView?id=perm_sets_overview.htm&type=5>. | | | | | |
| SEC-25 | The system or Contractor must alert DHHS of potential violations of security and privacy safeguards. Incidents that involve or could potentially involve confidential or highly restricted data must be reported immediately as defined in DHHS Policy DHHS-2018-IT-001E DHHS IT Incident Management Standard. | x | X |  |  |
| Response:  If negotiated into a final contract, and for the Salesforce Government Cloud only, Salesforce will promptly notify the State in the event Salesforce becomes aware of a confirmed unauthorized disclosure of Customer Data in the Salesforce Services caused by Salesforce or its contractors. Notification may include phone contact by Salesforce support, email to the State's administrator and Security Contact (if submitted by the State), and public posting on trust.salesforce.com. If the customer maintains an email address for a Security Contact in the Service then Salesforce will notify such Security Contact within 24 hours of becoming aware of such an unauthorized disclosure. Customer is responsible for maintaining the accuracy and currency of the Security Contact information.  Salesforce maintains an Incident Response Plan and has an established Security Incident Response Process. During a security incident, the process guides Salesforce personnel in management, communication, and resolution activities. Government customers can report security incidents related to their Salesforce products and offerings via [security\_gov@salesforce.com](mailto:security_gov@salesforce.com). Salesforce will respond in accordance with the incident response process described above.  Our incident response plan/process was created in accordance with FedRAMP moderate control requirements which include incident response requirements derived from NIST SP 800-53, NIST SP 800-61, and the FedRAMP Incident Communications Procedure. | | | | | |
| SEC-26 | Describe how the system provides the capability to monitor events on the information system, detects attacks, and provides identification of unauthorized use of the system. | x | X |  |  |
| Response:  **Government Trusted Security and Infrastructure**  Salesforce understands that the confidentiality, integrity, and availability of our customers’ information are vital to their business operations and Salesforce's own success. Salesforce uses a multi-layered approach to protect that key information, constantly monitoring and improving our application, systems, and processes to meet the growing demands and challenges of security.    Independent audits confirm that our security goes far beyond what most companies have been able to achieve on their own. Using the latest firewall protection, intrusion detection systems, and TLS encryption, Salesforce gives you the peace of mind only a world-class security infrastructure can provide.    Third-party validation  Security is a multidimensional business imperative that demands consideration at multiple levels, from security for applications to physical facilities and network security. In addition to the latest technologies, world-class security requires ongoing adherence to best-practice policies. To ensure this adherence, we continually seek relevant third-party certification, including ISO 27001, the SysTrust audit (the recognized standard for system security), and SSAE 16 SOC 1 audit (an examination and assessment of internal corporate controls, previously known as SAS 70 Type II). SOC1, SOC2 and SOC3 audits are performed by a third-party auditor annually at a minimum. Additional audits and certifications include CSA ‘Consensus Assessments Initiative’, JIPDC (Japan Privacy Seal), Tuv (Germany Privacy Mark), and TRUSTe.    Protection at the application level  Salesforce protects customer data by ensuring that only authorized users can access it. Administrators assign data security rules that determine which data users can access. Sharing models define organization-wide defaults and data access based on a role hierarchy. All data is encrypted in transfer. All access is governed by strict password security policies. All passwords are stored in SHA 256 one-way hash format. Applications are continually monitored for security violation attempts.    Protection at the facilities level  Salesforce security standards are stringent and designed with demanding customers in mind, including the world’s most security-conscious financial institutions. Authorized personnel must pass through five levels of biometric scanning to reach the Salesforce system cages. All buildings are completely anonymous, with bullet-resistant exterior walls and embassy-grade concrete posts and planters around the perimeter. All exterior entrances feature silent alarm systems that notify law enforcement in the event of suspicion or intrusion. Data is backed up to disk. These backups provide a second level of physical protection and disks never leave the data center.    Protection at the network level  Multilevel security products from leading security vendors and proven security practices ensure network security. To prevent malicious attacks through unmonitored ports, external firewalls allow only http and https traffic on ports 80 and 443, along with ICMP traffic. Switches ensure that the network complies with the RFC 1918 standard, and address translation technologies further enhance network security. IDS sensors protect all network segments. Internal software systems are protected by two-factor authentication, along with the extensive use of technology that controls points of entry. All networks are certified through third-party vulnerability assessment programs.    Trust.salesforce.com is the Salesforce community’s home for real-time information on system performance and security. On this site you'll find:   * Up-to-the minute information on planned maintenance * Phishing, malicious software, and social engineering threats * Best security practices for the State * Information on how we safeguard your data     These papers further explain the technology that makes the Salesforce Platform fast, scalable, and secure for any type of application:  <https://developer.salesforce.com/page/Multi_Tenant_Architecture>  <https://trust.salesforce.com/en/trust-and-compliance-documentation/> | | | | | |
| SEC-27 | The system must provide a process for archiving or destroying data and sanitizing storage media in conformance with DHHS and Division data governance policies and subject to applicable HIPAA, and federal (e.g., Federal Information Processing Standards (FIPS), National Institutes of Standards and Technology (NIST), and State laws. | X | x |  |  |
| Response:  **HIPAA**  Many Salesforce customers store protected health information (PHI) on our service.  The U.S. Centers for Medicare & Medicaid Services (CMS) guidelines (<http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/System-Security-Levels-by-Information-Type.pdf>) states that "Information related to personnel, medical, and similar data includes all information covered by the Privacy Act of 1974 (e.g., salary data, social security information, passwords, user identifiers (IDs), Equal Employment Opportunity (EEO), personnel profile (including home address and phone number), medical history, employment history (general and security clearance information), and arrest/criminal investigation history as well as personally identifiable information (PII), individually identifiable information (IIF), or personal health information (PHI) covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA)" should be considered Moderate for Confidentiality, Integrity, and Availability.  Salesforce's FedRAMP ATO is based on a Moderate System Security Level. Please note, Salesforce is not considered a "first-tier, downstream or related entity" for the purposes of compliance with CMS flow-down regulations.  Salesforce has also received a Provisional Authorization (PA) from Defense Information Systems Agency (DISA) at Impact Level 4 (IL4) to store, process, or transmit Controlled Unclassified Information (CUI) and/or other mission critical data to include that used in direct support of military or contingency operations. In addition to the DoD Cloud Computing SRG including PHI as a CUI category, the National Archives' CUI Registry (https://www.archives.gov/cui/registry/category-list) includes Health Information as a category under Privacy.  **Federal Information Processing Standards (FIPS)**  On the Salesforce Government Cloud, Salesforce has implemented encryption to protect customer information at rest and in transit in accordance with Federal Risk and Authorization Management Program (FedRAMP) moderate impact level requirements. The Salesforce Government Cloud includes such encryption of Customer Data (i.e., electronic data and information submitted by or for the Customer to the Services) by default, both in transit between Salesforce's customers' network(s) and the Salesforce Government Cloud FedRAMP authorized boundary, and in transit between the Salesforce Government Cloud data centers. Salesforce also provides customers with the ability to utilize encryption for Customer Data at rest on the Salesforce Government Cloud via Salesforce Classic Encryption or Salesforce Shield Platform Encryption (additional subscription service). These implementations leverage cryptographic modules that have been specifically validated by Cryptographic Module Validation Program (CMVP) for conformance to the Federal Information Processing Standard (FIPS) Publication 140-2. Those modules are required to operate in FIPS 140 approved mode with approved cryptographic algorithms and key lengths.  **National Institutes of Standards and Technology (NIST)**  **Government Cloud**  Salesforce was the first Cloud Service Provider granted a FedRAMP Authority to Operate (ATO) for both Software as a Service (SaaS) and Platform as a Service (PaaS), consistent with the FedRAMP moderate baseline controls.    On May 23, 2014 Salesforce was granted a FedRAMP ATO at the moderate impact level issued by the Department of Health and Human Services (HHS) for the Salesforce Government Cloud. Testing for the ATO was performed by a third party assessment organization (3PAO).    The Salesforce Government Cloud information system and authorization boundary, is comprised of the Salesforce Platform\*, Sales, Service, Communities, Analytics, Salesforce Mobile, and Industry Solutions, as well as the backend infrastructure (e.g., servers, network devices, databases, storage arrays) that support the operations of these products, referred to as the General Support System (GSS).    To obtain compliance with FedRAMP, Salesforce conducted security assessment and authorization activities in accordance with FedRAMP guidance, NIST SP 800-37, and HHS requirements. As part of this process Salesforce documented a System Security Plan (SSP) for the Salesforce Government Cloud service offering. The SSP is developed in accordance with NIST SP 800-18. The SSP identifies control implementations for the GSS and in-scope customer facing products (e.g., Lightning Platform, applicable Salesforce Services) according to the FedRAMP moderate baseline and HHS security control parameters. A security assessment of the information system was conducted by a 3PAO in accordance with FedRAMP Moderate requirements. The security assessment testing determined the adequacy of the management, operational, and technical security controls used to protect the confidentiality, integrity, and availability of Salesforce's Government Cloud service offering and the Customer Data it stores, transmits and processes.    To maintain compliance with FedRAMP, Salesforce conducts continuous monitoring, which includes ongoing technical vulnerability detection, remediation of open compliance related findings, and at least annual independent assessment of security controls by a 3PAO. As part of the current FedRAMP annual assessment, Salesforce is aligned with NIST SP 800-53 Revision 4.    Federal customers have the ability to access Salesforce's FedRAMP ATO package through the OMB MAX information portal upon filling out the Package Access Request form on the FedRAMP PMO website:<https://marketplace.fedramp.gov/#/product/salesforce-government-cloud?sort=productName>.  Additionally, under the Salesforce Government Cloud Compliance Information Non-Disclosure Agreement, other applicable customers approved for the Government Cloud can be provided the Salesforce Government Cloud FedRAMP ATO package outside of OMB MAX.  For more information on the Salesforce Government Cloud please see the [Salesforce Government Cloud whitepaper](https://org62.my.salesforce.com/sfc/p/#000000000062/a/0M000000Q8ar/moggeD49GPYM4jsNqrIjHnLlcqW7Zc7VwHfyKfuEmbs).    \*Only the Salesforce Platform is included within the FedRAMP Authorization Boundary for the Salesforce Government Cloud.    For more information on the Salesforce Government cloud please see the Salesforce Government Cloud white paper: <https://org62.my.salesforce.com/sfc/p/000000000062/a/0M000000Q8ar/moggeD49GPYM4jsNqrIjHnLlcqW7Zc7VwHfyKfuEmbs>.  **Media Sanitization**  Salesforce has an established process for sanitizing media consistent with industry guidelines and NIST SP 800-88 Guidelines for Media Sanitization. Salesforce performs a 7-pass wipe. Destruction of processing equipment is defined in Salesforce’s Media Handling Standard and Process documents which cover the following points:   * Media is sanitized using Salesforce approved equipment, techniques and procedures, and data is removed from the device or media using approved sanitization procedures. * Media sanitization is tracked, documented, and verified, and periodic tests of sanitizing equipment and procedures are performed. * Media is sanitized or destroyed before disposing or releasing for reuse outside of Salesforce to prevent access to any information contained on the device or media by unauthorized individuals. * Success or failure of sanitization procedures is validated after execution. * Devices or media are physically destroyed if they cannot be sanitized, or if sanitization is unsuccessful. * Any decommissioned media that ever-contained Customer Data is physically destroyed to meet or exceed the requirements set forth in the NIST SP 800-88 Revision 1. * Applicable hardcopy materials are disposed of via secure shredding.   **Termination**  In the event of termination of the Salesforce service, requests by the State made within 30 days after the effective date of termination or expiration of the Subscription Agreement, Salesforce will make your data available to you for export or download. Once the export has been completed, an email will be sent to you containing a link where you can download a .zip file that contains multiple .csv (spreadsheets) files, each representing your Salesforce objects. Your data on disk is flagged within the database and set to inactive status or what can be referred to as a "soft delete." This data is no longer available or accessible to the application but is backed up in the full database backup process. The data remains in this state for 180 days; this is done in the event that the customer decides to resume services or needs the data for a legal reason. At 180 days, the data is marked for deletion ("hard delete") and will be deleted after 30 more days. Once this "hard delete" is executed the customer data is physically deleted and non-recoverable from the database. Following the purge, the data will remain on backup for an additional 90 days prior to being overwritten and unrecoverable. This process is standard for all Salesforce Customers.  Upon customer request, Salesforce will provide written confirmation of the deletion of customer data. However, Salesforce will not be able to provide the State with a Certificate of Destruction signed by a senior officer. | | | | | |
| SEC-28 | Describe how the system provides the capability to identify and report on unauthorized attempts to access information in the system, based on user-defined criteria. |  | x |  |  |
| Response: | | | | | |
| **Multi-Tenant Architecture**  The multitenant architecture and secure logical controls address separation of customer data. There are no dedicated servers used for individual customers. The Salesforce Services infrastructure is divided into a modular architecture based on “Instance”. Each Instance is capable of supporting several thousand customers in a secure and efficient manner. Services are grouped within each Instance; with app, search, and database elements contained. There are appropriate controls in place to ensure that any given customer’s org (application) is not compromised. The service has been designed to accomplish this and is robustly tested on an ongoing basis by both Salesforce and its customers.    Salesforce also provides contractual assurance to its customers that the data hosted in the Salesforce Services will be kept confidential and not accessed except under narrow circumstances (such as a support issue) and only for a set amount of time chosen by the customer. In such circumstances, we will access your org only with prior approval and subject to a Non-Disclosure Agreement (NDA).    To protect against access through the application, Salesforce employees don't have access at the application level for any customers, unless the customer grants access through the “login as” feature.    Access to the production environment infrastructure is restricted to a very limited number of full-time Salesforce employees required to manage the service. Salesforce's Technical Operations team and Release Managers have logical access to servers. These employees must authenticate to the production environment via a secure server (Secure Global Desktop) using 2 points of RSA two-factor authentication. This tool provides pixel data only to these administrators. Systems access is role-based and controlled and logged. DBAs do not have login access to customer's instances (org) and do not see customer data in an assembled manner. They manage the system in aggregate-performance tuning, allocating space, building indices, etc. The Oracle tables and rows in our infrastructure do not reflect the view of a single customer instance (org) since we are multi-tenant and the data is spread across multiple disk arrays.    Database administrator account activity is logged. These logs are sent to the security information and event management (SIEM) system. These database activities logs are reviewed for appropriateness by the Computer Security Incident Response Team (CSIRT) team on a regular basis. This log data is also available as a forensic audit trail to support CSIRT during incident investigations.    A customer's instance (org) of Salesforce is an aggregate of the raw data. The data model is very complicated, normalized, and the rows are identified by base62 encoded keys (primary and foreign). Re-establishing data ownership and a business context for the data would be very difficult to do at the database level. In order to reassemble any given customer's application (org), someone would need access to our source code in order to reassemble the raw data in a manner that could be interpreted and understood, and would need the entire set of tapes or disks/arrays supporting a given Instance, as the data for any one customer is spread across several tapes/disks. Data center engineers with physical access to the servers do not have logical access to the production environment and administrators with logical access to the systems do not have physical access to the data centers.  **Login Restrictions**  To help protect the State’s data against unauthorized access, the State can restrict users' ability to log in to the Salesforce application by customizing user profiles and the customer's list of trusted IP addresses/ranges. The administrator can also restrict the hours during which users can log in. If IP address restrictions are defined for a user's profile and a login originates from an unknown IP address, Salesforce does not allow the login. These restrictions help protect customer's data from unauthorized access and phishing attacks.  **User Profiles**  This is configurable by the State’s Administrator.  All users and application-level security are defined and maintained by the organization administrator, and not by Salesforce. The organization administrator is appointed by the customer. An organization's sharing model sets the default access that users have to each other's data.    There are four sharing models: Private, Public Read Only, Public Read/Write, and Public Read/Write/Transfer. There are also several sharing model elements: Profiles, Roles, Hierarchy, Record Types, Page Layouts, and Field-Level security. Details about sharing models and sharing model elements are provided below:    Private  Only the record owner, and users above that role in the hierarchy, can view, edit, and report on those records.    Public Read Only  All users can view and report on records but not edit them. Only the owner, and users above that role in the hierarchy, can edit those records.    Public Read/Write  All users can view, edit, and report on all records.    Public Read/Write/Transfer  All users can view, edit, transfer, and report on all records. Only available for cases or leads.    Profiles  A profile contains the settings and permissions that control what users with that profile can do within Salesforce. Profiles control:   * Standard and custom apps the user can view (depending on user license) * Service providers the user can access * Tabs the user can view (depending on user license and other factors, such as access to Salesforce CRM Content) * Administrative and general permissions the user has for managing the organization and apps within it * Object permissions the user is granted to create, read, edit, and delete records * Page layouts a user sees * Field-level security access that the user has to view and edit specific fields * Record types are available to the user * Desktop clients users can access and related options * Hours during which and IP addresses from which the user can log in * Apex classes a user can execute * Visualforce pages a user can access     User Roles  Every user must be assigned to a role, or their data will not display in reports and other displays based on roles. All users that require visibility to the entire organization should be assigned the highest level in the hierarchy. It is not necessary to create individual roles for each title at the organization, rather a hierarchy of roles should be defined to control access of information entered by users in lower level roles. When a user's role is changed, any relevant sharing rules are reevaluated to add or remove access as necessary.    Record Types  If the customer's organization uses record types, edit the record type to modify which pick list values are visible for the record type. A default pick list values can be set based upon the record type for various divisions.    Field-Level Security  Field-level security settings let administrators restrict user's access to view and edit specific fields on detail and edit pages and in related lists, list views, reports, Offline Edition, search results, email and mail merge templates, Custom Links, and when synchronizing data.    The fields that users see in detail and edit pages are a combination of page layouts and field-level security settings. The most restrictive field access settings of the two always apply. For example, if a field is required in the page layout and read-only in the field-level security settings, the field-level security overrides the page layout and the field will be read-only for the user.    Permission Sets  A permission set is a collection of settings and permissions that give users access to various tools and functions. The settings and permissions in permission sets are also found in profiles, but permission sets extend users’ functional access without changing their profiles.    Users can have only one profile but, depending on the Salesforce edition, they can have multiple permission sets. You can assign permission sets to various types of users, regardless of their profiles. The State can create permission sets to grant access among logical groupings of users, regardless of their primary job function.    See more information at: <https://help.salesforce.com/articleView?id=perm_sets_overview.htm&type=5>.  **Core Auditing Capabilities and Event Monitoring**  Within Salesforce, the creator and last updater, as well as timestamps, are recorded for every record. Additionally, the Salesforce Platform and Salesforce Applications have a multitude of history tracking and auditing features that provide valuable information about the use of an organization’s applications and data, which in turn can be a critical tool in diagnosing potential or real security issues. Auditing features include:    Record Modification Fields - All objects include fields to store the name of the user who created the record and who last modified the record. This provides some basic auditing information.    Field History Tracking - Enable auditing for individual fields (up to 20 fields per object), which will automatically track any changes in the values of selected fields. Although auditing is available for all custom objects, only some standard objects allow field-level auditing.    Login History - Review up to 20,000 successful and failed login attempts to the State for the past six months. The State can also track the geographic location of the IP addresses of your logins in your personal settings. You can track the geographic location of the login IP addresses for any of your users in the user’s detail page. To get more detailed geographic information, such as city and postal code, you can download the login history. Due to the nature of geolocation technology, the accuracy of geolocation fields (for example, country, city, postal code) can vary.    Identity Verification History - Review up to 20,000 records of your org users’ identity verification attempts from the past six months. For example, suppose that two-factor authentication is enabled when a user logs in. When the user successfully provides a time-based, one-time password as proof of identity, that information is recorded in Identity Verification History.    Setup Audit Trail - Administrators can view a Setup Audit Trail for the past six months within Salesforce, which logs when modifications are made to the State's configuration.    While the Login History and Setup Audit Trail are available for six months within Salesforce, they can be downloaded and stored locally to meet longer audit log retention requirements. Additionally, historic event logs which provide more information can be provided for a fee. For more information, please see<https://help.salesforce.com/articleView?id=000336835&language=en_US&type=1&mode=1>.  **Event Monitoring**  In addition to Salesforce’s core auditing capabilities, Salesforce offers Event Monitoring as an additional license option. The State can use event monitoring to discover how often and at what times your users are logging into and out of the State. This includes insight into what Salesforce applications are being adopted by users, who is logging in and from where, what pages users are viewing, what knowledge articles users are viewing, what reports users are running and exporting, which search terms users are using and what individual users click, and other aspects of application usage. This capability helps you discriminate between valid and invalid login requests and also track user login patterns for future reference. For example, depending on your org settings, admins can log into Salesforce as another user. You can use Login As event type data to review those actions to identify any security breaches or vulnerabilities, and also to inform your users what occurred. Not only can the State better understand how your apps are being utilized, you can also monitor if users download large amounts of data that might put the State at risk. In addition, the State can also determine if an employee is unnecessarily downloading sensitive customer information, pinpointing the exact time and location of that event. Event Monitoring is delivered as an API-first feature and there are Salesforce partners with visualization tools available.    Use the SOAP API and REST API resources to retrieve event log files that contain information useful for assessing organizational usage trends and user behavior. Because event log files are accessed through the Salesforce Platform SOAP API and REST API, you can integrate log data with your own back-end storage and data marts so that you can correlate data from multiple organizations and across disparate systems easily. When using event monitoring, keep the following in mind:   * Log data can be deleted by your Salesforce administrator. You cannot insert or update log data. * Use the Event Type field to determine which files were generated for the State. * An event generates log data in real time. However, log files are generated the day after an event takes place, during non-peak hours. Therefore, daily log file data is unavailable for at least one day after an event. For hourly log files, depending on event delivery and final processing time, an event is expected to take three to six hours from the time of the event to be available in the log file. However, it can take longer. * Log files, represented by the Event Type field, are only generated if there is at least one event of that type for the day or hour. If no events took place, the file isn't generated. * Log files are available based on Created Date for the last 30 days when organizations purchase User Event Monitoring * All event monitoring logs are exposed to the API through the Event Logfile object. However, there is no access through the user interface, except through the Event Monitoring Analytics app. * Hourly event log files are provided for you to review events in your orgs on an accelerated basis. However, it is possible that you don’t get all event log data in hourly event log files, especially during site switches, instance refreshes, or unplanned system outages. For complete data, use the daily log files.     Event monitoring can be used with 49 different event types. For more information please see:<https://developer.salesforce.com/docs/atlas.en-us.api.meta/api/sforce_api_objects_eventlogfile_supportedeventtypes.htm>.    Event Monitoring Transaction Security  Transaction Security policies give the State the ability to take real-time security actions based on event triggers. With Transaction Security, you can monitor events according to the policies that you establish. When a policy is triggered, you can receive a notification and/or take an action.    For example, suppose that you activate a policy to limit the number of concurrent sessions per user to three. A user with three login sessions tries to create a fourth session. The State can require a user to end one of their existing sessions before proceeding with the new session. At the same time, you are notified that the policy was triggered. For more information, please see:<https://help.salesforce.com/articleView?id=security_transactions.htm>.    Real-Time Event Monitoring  With the Real-Time Event Monitoring feature, you can stream and store event data and create transaction security policies for several new events in Salesforce, all in real time. When you enable Real-Time Event Monitoring, you automatically get Enhanced Transaction Security—Salesforce’s latest and greatest feature for creating transaction security policies. Use Event Manager to view and monitor events in your org. For more information, please see: <https://help.salesforce.com/articleView?id=real_time_event_monitoring_overview.htm>.    Event Monitoring Analytics App  The State can use the built-in Event Monitoring Analytics App to explore your monitoring data in Salesforce. The Event Monitoring Analytics App integrates with Event Monitoring and Setup Audit Trail data to give you insights into your user and org behavior. App creation is easy and with its pre built dashboards and datasets, you can start exploring right away. This app helps you drill into your org’s data and swiftly identify suspicious behavior, slow page performance, and poor user adoption. Get valuable information instantly from your Salesforce event logs, such as the number of people and IP addresses accessing your org, which Visualforce requests are timing out, and which users make changes in Setup. The State can detect performance problems early, such as queries taking too much time, by getting notifications when a KPI value exceeds your established threshold. Hourly event log file integration with the Event Monitoring Analytics app is unavailable. Data is refreshed once a day in the app. For more information, please see: <https://help.salesforce.com/articleView?id=bi_app_admin_wave.htm>. | | | | | |
| SEC-29 | Describe how the system has defined and deployed strong controls (including access and query rights) to prevent any data misuse, such as fraud, marketing or other purposes. |  | x |  |  |
| Response:  **Government Trusted Security and Infrastructure**  Salesforce understands that the confidentiality, integrity, and availability of our customers’ information are vital to their business operations and Salesforce's own success. Salesforce uses a multi-layered approach to protect that key information, constantly monitoring and improving our application, systems, and processes to meet the growing demands and challenges of security.    Independent audits confirm that our security goes far beyond what most companies have been able to achieve on their own. Using the latest firewall protection, intrusion detection systems, and TLS encryption, Salesforce gives you the peace of mind only a world-class security infrastructure can provide.    Third-party validation  Security is a multidimensional business imperative that demands consideration at multiple levels, from security for applications to physical facilities and network security. In addition to the latest technologies, world-class security requires ongoing adherence to best-practice policies. To ensure this adherence, we continually seek relevant third-party certification, including ISO 27001, the SysTrust audit (the recognized standard for system security), and SSAE 16 SOC 1 audit (an examination and assessment of internal corporate controls, previously known as SAS 70 Type II). SOC1, SOC2 and SOC3 audits are performed by a third-party auditor annually at a minimum. Additional audits and certifications include CSA ‘Consensus Assessments Initiative’, JIPDC (Japan Privacy Seal), Tuv (Germany Privacy Mark), and TRUSTe.    Protection at the application level  Salesforce protects customer data by ensuring that only authorized users can access it. Administrators assign data security rules that determine which data users can access. Sharing models define organization-wide defaults and data access based on a role hierarchy. All data is encrypted in transfer. All access is governed by strict password security policies. All passwords are stored in SHA 256 one-way hash format. Applications are continually monitored for security violation attempts.    Protection at the facilities level  Salesforce security standards are stringent and designed with demanding customers in mind, including the world’s most security-conscious financial institutions. Authorized personnel must pass through five levels of biometric scanning to reach the Salesforce system cages. All buildings are completely anonymous, with bullet-resistant exterior walls and embassy-grade concrete posts and planters around the perimeter. All exterior entrances feature silent alarm systems that notify law enforcement in the event of suspicion or intrusion. Data is backed up to disk. These backups provide a second level of physical protection and disks never leave the data center.    Protection at the network level  Multilevel security products from leading security vendors and proven security practices ensure network security. To prevent malicious attacks through unmonitored ports, external firewalls allow only http and https traffic on ports 80 and 443, along with ICMP traffic. Switches ensure that the network complies with the RFC 1918 standard, and address translation technologies further enhance network security. IDS sensors protect all network segments. Internal software systems are protected by two-factor authentication, along with the extensive use of technology that controls points of entry. All networks are certified through third-party vulnerability assessment programs.    Trust.salesforce.com is the Salesforce community’s home for real-time information on system performance and security. On this site you'll find:   * Up-to-the minute information on planned maintenance * Phishing, malicious software, and social engineering threats * Best security practices for the State * Information on how we safeguard your data     These papers further explain the technology that makes the Salesforce Platform fast, scalable, and secure for any type of application:  <https://developer.salesforce.com/page/Multi_Tenant_Architecture>  <https://trust.salesforce.com/en/trust-and-compliance-documentation/>  **User Profiles**  This is configurable by the State’s Administrator.  All users and application-level security are defined and maintained by the organization administrator, and not by Salesforce. The organization administrator is appointed by the customer. An organization's sharing model sets the default access that users have to each other's data.    There are four sharing models: Private, Public Read Only, Public Read/Write, and Public Read/Write/Transfer. There are also several sharing model elements: Profiles, Roles, Hierarchy, Record Types, Page Layouts, and Field-Level security. Details about sharing models and sharing model elements are provided below:    Private  Only the record owner, and users above that role in the hierarchy, can view, edit, and report on those records.    Public Read Only  All users can view and report on records but not edit them. Only the owner, and users above that role in the hierarchy, can edit those records.    Public Read/Write  All users can view, edit, and report on all records.    Public Read/Write/Transfer  All users can view, edit, transfer, and report on all records. Only available for cases or leads.    Profiles  A profile contains the settings and permissions that control what users with that profile can do within Salesforce. Profiles control:   * Standard and custom apps the user can view (depending on user license) * Service providers the user can access * Tabs the user can view (depending on user license and other factors, such as access to Salesforce CRM Content) * Administrative and general permissions the user has for managing the organization and apps within it * Object permissions the user is granted to create, read, edit, and delete records * Page layouts a user sees * Field-level security access that the user has to view and edit specific fields * Record types are available to the user * Desktop clients users can access and related options * Hours during which and IP addresses from which the user can log in * Apex classes a user can execute * Visualforce pages a user can access     User Roles  Every user must be assigned to a role, or their data will not display in reports and other displays based on roles. All users that require visibility to the entire organization should be assigned the highest level in the hierarchy. It is not necessary to create individual roles for each title at the organization, rather a hierarchy of roles should be defined to control access of information entered by users in lower level roles. When a user's role is changed, any relevant sharing rules are reevaluated to add or remove access as necessary.    Record Types  If the customer's organization uses record types, edit the record type to modify which pick list values are visible for the record type. A default pick list values can be set based upon the record type for various divisions.    Field-Level Security  Field-level security settings let administrators restrict user's access to view and edit specific fields on detail and edit pages and in related lists, list views, reports, Offline Edition, search results, email and mail merge templates, Custom Links, and when synchronizing data.    The fields that users see in detail and edit pages are a combination of page layouts and field-level security settings. The most restrictive field access settings of the two always apply. For example, if a field is required in the page layout and read-only in the field-level security settings, the field-level security overrides the page layout and the field will be read-only for the user.    Permission Sets  A permission set is a collection of settings and permissions that give users access to various tools and functions. The settings and permissions in permission sets are also found in profiles, but permission sets extend users’ functional access without changing their profiles.    Users can have only one profile but, depending on the Salesforce edition, they can have multiple permission sets. You can assign permission sets to various types of users, regardless of their profiles. The State can create permission sets to grant access among logical groupings of users, regardless of their primary job function.    See more information at: <https://help.salesforce.com/articleView?id=perm_sets_overview.htm&type=5>. | | | | | |
| SEC-30 | The system must be able to export audit logs that can be used with a third party Log Management & Analysis tool. Describe how the system exports logs in such a manner as to allow correlation based on time (e.g. Universal Time Coordinate (UTC) synchronization. |  | x |  |  |
| Response:  **Core Auditing Capabilities**  Within Salesforce, the creator and last updater, as well as timestamps, are recorded for every record. Additionally, the Salesforce Platform and Salesforce Applications have a multitude of history tracking and auditing features that provide valuable information about the use of an organization’s applications and data, which in turn can be a critical tool in diagnosing potential or real security issues. Auditing features include:    Record Modification Fields - All objects include fields to store the name of the user who created the record and who last modified the record. This provides some basic auditing information.    Field History Tracking - Enable auditing for individual fields (up to 20 fields per object), which will automatically track any changes in the values of selected fields. Although auditing is available for all custom objects, only some standard objects allow field-level auditing.    Login History - Review up to 20,000 successful and failed login attempts to the State for the past six months. The State can also track the geographic location of the IP addresses of your logins in your personal settings. You can track the geographic location of the login IP addresses for any of your users in the user’s detail page. To get more detailed geographic information, such as city and postal code, you can download the login history. Due to the nature of geolocation technology, the accuracy of geolocation fields (for example, country, city, postal code) can vary.    Identity Verification History - Review up to 20,000 records of your org users’ identity verification attempts from the past six months. For example, suppose that two-factor authentication is enabled when a user logs in. When the user successfully provides a time-based, one-time password as proof of identity, that information is recorded in Identity Verification History.    Setup Audit Trail - Administrators can view a Setup Audit Trail for the past six months within Salesforce, which logs when modifications are made to the State's configuration.    While the Login History and Setup Audit Trail are available for six months within Salesforce, they can be downloaded and stored locally to meet longer audit log retention requirements. Additionally, historic event logs which provide more information can be provided for a fee. For more information, please see<https://help.salesforce.com/articleView?id=000336835&language=en_US&type=1&mode=1>.  **Event Monitoring**  In addition to Salesforce’s core auditing capabilities, Salesforce offers Event Monitoring as an additional license option. The State can use event monitoring to discover how often and at what times your users are logging into and out of the State. This includes insight into what Salesforce applications are being adopted by users, who is logging in and from where, what pages users are viewing, what knowledge articles users are viewing, what reports users are running and exporting, which search terms users are using and what individual users click, and other aspects of application usage. This capability helps you discriminate between valid and invalid login requests and also track user login patterns for future reference. For example, depending on your org settings, admins can log into Salesforce as another user. You can use Login As event type data to review those actions to identify any security breaches or vulnerabilities, and also to inform your users what occurred. Not only can the State better understand how your apps are being utilized, you can also monitor if users download large amounts of data that might put the State at risk. In addition, the State can also determine if an employee is unnecessarily downloading sensitive customer information, pinpointing the exact time and location of that event. Event Monitoring is delivered as an API-first feature and there are Salesforce partners with visualization tools available.    Use the SOAP API and REST API resources to retrieve event log files that contain information useful for assessing organizational usage trends and user behavior. Because event log files are accessed through the Salesforce Platform SOAP API and REST API, you can integrate log data with your own back-end storage and data marts so that you can correlate data from multiple organizations and across disparate systems easily. When using event monitoring, keep the following in mind:   * Log data can be deleted by your Salesforce administrator. You can’t insert or update log data. * Use the Event Type field to determine which files were generated for the State. * An event generates log data in real time. However, log files are generated the day after an event takes place, during non-peak hours. Therefore, daily log file data is unavailable for at least one day after an event. For hourly log files, depending on event delivery and final processing time, an event is expected to take three to six hours from the time of the event to be available in the log file. However, it can take longer. * Log files, represented by the Event Type field, are only generated if there is at least one event of that type for the day or hour. If no events took place, the file isn't generated. * Log files are available based on Created Date for the last 30 days when organizations purchase User Event Monitoring * All event monitoring logs are exposed to the API through the Event Logfile object. However, there is no access through the user interface, except through the Event Monitoring Analytics app. * Hourly event log files are provided for you to review events in your orgs on an accelerated basis. However, it is possible that you don’t get all event log data in hourly event log files, especially during site switches, instance refreshes, or unplanned system outages. For complete data, use the daily log files.     Event monitoring can be used with 49 different event types. For more information please see:<https://developer.salesforce.com/docs/atlas.en-us.api.meta/api/sforce_api_objects_eventlogfile_supportedeventtypes.htm>.    Event Monitoring Transaction Security  Transaction Security policies give the State the ability to take real-time security actions based on event triggers. With Transaction Security, you can monitor events according to the policies that you establish. When a policy is triggered, you can receive a notification and/or take an action.    For example, suppose that you activate a policy to limit the number of concurrent sessions per user to three. A user with three login sessions tries to create a fourth session. The State can require a user to end one of their existing sessions before proceeding with the new session. At the same time, you are notified that the policy was triggered. For more information, please see:<https://help.salesforce.com/articleView?id=security_transactions.htm>.    Real-Time Event Monitoring  With the Real-Time Event Monitoring feature, you can stream and store event data and create transaction security policies for several new events in Salesforce, all in real time. When you enable Real-Time Event Monitoring, you automatically get Enhanced Transaction Security—Salesforce’s latest and greatest feature for creating transaction security policies. Use Event Manager to view and monitor events in your org. For more information, please see: <https://help.salesforce.com/articleView?id=real_time_event_monitoring_overview.htm>.    Event Monitoring Analytics App  The State can use the built-in Event Monitoring Analytics App to explore your monitoring data in Salesforce. The Event Monitoring Analytics App integrates with Event Monitoring and Setup Audit Trail data to give you insights into your user and org behavior. App creation is easy and with its pre built dashboards and datasets, you can start exploring right away. This app helps you drill into your org’s data and swiftly identify suspicious behavior, slow page performance, and poor user adoption. Get valuable information instantly from your Salesforce event logs, such as the number of people and IP addresses accessing your org, which Visualforce requests are timing out, and which users make changes in Setup. The State can detect performance problems early, such as queries taking too much time, by getting notifications when a KPI value exceeds your established threshold. Hourly event log file integration with the Event Monitoring Analytics app is unavailable. Data is refreshed once a day in the app. For more information, please see: <https://help.salesforce.com/articleView?id=bi_app_admin_wave.htm>. | | | | | |
| SEC-31 | Describe how the system supports removal of a user's privileges without deleting the user from the system to ensure a history of user's identity and actions. | x |  |  |  |
| Response:  User provisioning and management is performed through the Salesforce Administrative Setup environment. Users, their profiles, permissions and passwords may be managed, edited, activated and deactivated as needed by those with appropriate permissions. An administrator with appropriate privileges can manage session timeout, password policies, IP range login restrictions, delegated authentication/SSO, and requirements as part of this process.  **User Profiles** This is configurable by the State’s Administrator.  All users and application-level security are defined and maintained by the organization administrator, and not by Salesforce. The organization administrator is appointed by the customer. An organization's sharing model sets the default access that users have to each other's data.    There are four sharing models: Private, Public Read Only, Public Read/Write, and Public Read/Write/Transfer. There are also several sharing model elements: Profiles, Roles, Hierarchy, Record Types, Page Layouts, and Field-Level security. Details about sharing models and sharing model elements are provided below:    Private  Only the record owner, and users above that role in the hierarchy, can view, edit, and report on those records.    Public Read Only  All users can view and report on records but not edit them. Only the owner, and users above that role in the hierarchy, can edit those records.    Public Read/Write  All users can view, edit, and report on all records.    Public Read/Write/Transfer  All users can view, edit, transfer, and report on all records. Only available for cases or leads.    Profiles  A profile contains the settings and permissions that control what users with that profile can do within Salesforce. Profiles control:   * Standard and custom apps the user can view (depending on user license) * Service providers the user can access * Tabs the user can view (depending on user license and other factors, such as access to Salesforce CRM Content) * Administrative and general permissions the user has for managing the organization and apps within it * Object permissions the user is granted to create, read, edit, and delete records * Page layouts a user sees * Field-level security access that the user has to view and edit specific fields * Record types are available to the user * Desktop clients users can access and related options * Hours during which and IP addresses from which the user can log in * Apex classes a user can execute * Visualforce pages a user can access     User Roles  Every user must be assigned to a role, or their data will not display in reports and other displays based on roles. All users that require visibility to the entire organization should be assigned the highest level in the hierarchy. It is not necessary to create individual roles for each title at the organization, rather a hierarchy of roles should be defined to control access of information entered by users in lower level roles. When a user's role is changed, any relevant sharing rules are reevaluated to add or remove access as necessary.    Record Types  If the customer's organization uses record types, edit the record type to modify which pick list values are visible for the record type. A default pick list values can be set based upon the record type for various divisions.    Field-Level Security  Field-level security settings let administrators restrict user's access to view and edit specific fields on detail and edit pages and in related lists, list views, reports, Offline Edition, search results, email and mail merge templates, Custom Links, and when synchronizing data.    The fields that users see in detail and edit pages are a combination of page layouts and field-level security settings. The most restrictive field access settings of the two always apply. For example, if a field is required in the page layout and read-only in the field-level security settings, the field-level security overrides the page layout and the field will be read-only for the user.    Permission Sets  A permission set is a collection of settings and permissions that give users access to various tools and functions. The settings and permissions in permission sets are also found in profiles, but permission sets extend users’ functional access without changing their profiles.    Users can have only one profile but, depending on the Salesforce edition, they can have multiple permission sets. You can assign permission sets to various types of users, regardless of their profiles. The State can create permission sets to grant access among logical groupings of users, regardless of their primary job function.    See more information at: <https://help.salesforce.com/articleView?id=perm_sets_overview.htm&type=5>. | | | | | |

***Data Conversion Requirements***

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Req #** | **Requirement** | (1) Comply | (a) Core | (b) Custom | (c) 3rd Party |
| DAC-1 | Describe the process for converting all historical data from the Department’s existing systems, spreadsheets, and other supporting applications that are required for ongoing operations of the system and the historical reporting needs of the department.  There are approximately 94 microfilm rolls with up to1500 pages of records on each roll, for up to 141,000 microfilm records that must be digitally converted. Additionally, approximately 25,000 pages of Board meeting minutes and associated files that should be digitized.  System Automation’s License 2000 (Oracle) currently contains approximately 655 tables and 50 million records.  DHHS also has approximately twelve (12) Access/Excel databases. Some information in these databases does not tie to license information in L2K.  DHHS also uses the federal government’s Aspen Central Office to import licensure data on a daily basis. | X |  | X | X |
| Response:  Considering the magnitude of data conversion requested it is important to get ensure a thorough knowledge of the date and a proper state for data to be translated effectively. The data conversion workstream will have sub-workstreams dedicated on identifying, inventorying, defining, categorizing, and prioritizing data for review, validation, cleansing and transfer. .Where there is substantial overhead to improve a state of date data will be further prioritized and a strategy to advance the state of that data to an acceptable health.  The | | | | | |
| DAC-2 | Describe the data conversion plan which includes data element mapping crosswalks, data cleansing, data synchronization for initial and interim conversion activities leading up to the final data conversion, and frequency of interim conversion events and final conversion execution. Contractor will be responsible for all data standardization and cleansing.  It is acceptable to migrate data and go live with license applications in incremental steps.  For individual licensees, SSN is included in L2K. There is also an identifier called “Person ID” in L2K.  For establishments in L2K, there are unique license numbers by license type, and unique applicant numbers.  In ACO, establishments have unique license numbers by license type. |  |  |  |  |
| Response:  The data conversion process will involve the following steps  Planning: As a first step in the process, our project manager will work with the business to identify the plan for data migration. This plan will identify all the systems from where data needs to be migrated, identify the data Subject Matter Expert for each system, the format the data resides in or delivered, data security concerns for handling the data, identify the cleanliness of the data, identify the tools that will be used for the migration, estimate the time required for the migration, identify the responsible party and timelines for completing the mapping, identify the environments where testing will be performed and the resources responsible for the testing, when will the system go live, and the acceptable downtime to complete the migration.  Once the plan is formalized, the next step is to start the mapping process and work with the business to identify the required data cleansing process. It is important to identify the unique identifier are in place for all the data to be migrated.  After the mapping, the developer will prepare the target environment with the necessary object, begin to implement the mapping process between source and destination in the selected tool. The tool will be selected based on the volume of data to be migrated and the complexity of the source data.  The next step is to perform quality assurance to ensure that all the data has been migrated with the right format and relationships are correctly reflected as per expectation. Salesforce reports will be created for each object to validate the count of the records and provide an overall snapshot of the migration. | | | | | |

***Production, Test and Training Requirements***

DHHS requires three separate environments (Production, Test, and Training) in order to operate and maintain the new software on an ongoing basis:

**Test Environment** – A test environment is required that mirrors the live production environment, including hardware and software. This test environment will be used to test application changes before deployed to production. This step is an important part of quality assurance, where all changes are tested to minimize the risk of adverse reactions in the production environment. While it is necessary to mirror all of the functions of the production environment, it is not necessary to maintain the same load capacity.

**Training Environment** – A training environment is also required that allows DHHS to provide hands-on training to users. This environment would allow DHHS to maintain unique data for use in training and conduct training without interference with the test or production environments. This environment will have occasional use.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Req #** | | **Requirement** | (1) Comply | (a) Core | (b) Custom | (c) 3rd Party |
| PTT-1 | | Describe how the system supports several environments, i.e., production environment, test environment, and training environment. | X | X |  |  |
| Response:  **Sandboxes**  Sandboxes give the State the ability to create multiple copies of your Salesforce organization in separate environments for a variety of purposes, such as development, testing, and training, without compromising the data and applications in your Salesforce production organization.  Administrators can set up users with the “Manage Sandbox” permission, which allows users to create, refresh, activate, and delete sandboxes. With the “Manage Sandbox” permission, users can manage sandboxes without compromising the State's control over data security, access management, and more. | | | | | | |
| PTT-2 | | Describe how the system supports non-production environments such as testing and training environments. Training environment must contain de-identified data and not include confidential or highly restricted data. | X | X |  |  |
| Response:  As illustrated in PTT-1 there are various sandboxes with features that enable testing, building, training and other activities that are not in production. Salesforce App Exchange platform provides solutions to help customers to scramble production data when it is copied during a sandbox refresh. As part of our discovery process we will work to understand the organization needs and recommend a tool that best meets the requirements. | | | | | | |
| PTT-3 | | Describe how the system provides the ability to refresh any testing or training environment at the request of DHHS. Describe the refresh process and whether the refresh process can be completed using DHHS resources, or whether the process requires professional services from the Contractor. | X | X |  |  |
| Response:  Refreshing a sandbox updates the sandbox’s metadata from its source org. If the sandbox is a clone or if it uses a sandbox template, the refresh process updates the org’s data in addition to its metadata. Sandbox refreshes can be performed by the system admin and do not require professional services from the contractor. Following is the process for refreshing the sandboxes:   1. From Setup, enter Sandboxes in the Quick Find box, then select Sandboxes. 2. A list of your sandboxes displays. Sandboxes that you can refresh have a Refresh link next to their name. 3. Next to the name, click Refresh. 4. Review the Name, Description, and Create From values, and edit these values if needed. 5. Select the type of sandbox environment you want. 6. A table shows the number and type of sandbox licenses available in your org. You can select a different sandbox type to refresh. 7. If the sandbox you’re refreshing is a clone, this option isn’t available. A cloned sandbox refreshes from its source org and retains the source org’s sandbox license type. If a sandbox’s source org has been deleted, the clone refreshes from your production org. 8. Select the data you want to copy. 9. For a Partial Copy sandbox, click Next, and then select a template to specify the data for your sandbox. If you have not created a template for this Partial Copy sandbox, see [Create or Edit Sandbox Templates](https://help.salesforce.com/articleView?id=data_sandbox_templates.htm&type=5). 10. For a Full sandbox, click Next, and then decide how much object data to include. 11. To include template-based data in a Full sandbox, select an existing sandbox template. For more information, see [Create or Edit Sandbox Templates](https://help.salesforce.com/articleView?id=data_sandbox_templates.htm&type=5). 12. To include all object data in a Full sandbox, choose whether and how much field tracking history to include, and whether to copy Chatter data. You can copy from 0 to 180 days of history, in 30-day increments. The default is 0 days. Chatter data includes feeds, messages, and discovery topics. Decreasing the amount of data you copy can speed sandbox copy time. 13. If you want to activate your sandbox immediately after you refresh it, select Auto Activate. In this case, you don’t receive an activation email. 14. Click Create. Salesforce will start copying the data | | | | | | |
| PTT-4 | | Describe the test procedures for any changes to the system. Describe user test planning including unit testing, end-to-end testing, stress testing, and readiness testing prior to “go live” date. | X | X |  |  |
| Response:  Testing is a critical component to the success of the project and will be done early, often, throughout and after the release dates to ensure only the requirements approved enter production. Thorough testing functionality, performance, limits and business processes are in scope for this engagement and MST requests the business to be heavily involved in writing business test scenarios and testing the product along the way of it being built.   Summary of Testing Methods  The following are the specific testing methods in scope for the project and are completed from the unit testing and task level all the way to full-regression pre- and post-production:   Quality Assurance testing   * Regression Testing * User Acceptance Testing * Integration Testing * Performance Testing * End to End testing    Regression Testing   A regression test suite will be built over the period of overall testing which will be utilized for End to End Functional Testing. The list of regression use cases will be provided at each regression interval.  Regression testing is conducted at minimum every sprint to cover scenarios developed in previous sprint to ensure system integrity. All test results will be documented and provided to the team for review.  Performance Testing  While Salesforce provides various governor limits to help enhance performance in multi-tenant architecture, MST works with customers through the implementation to identify performance thresholds and designs the system to ensure support. MST will execute performance testing and provide detailed statistics on major application processing times which can include performance of portal form submission process, portal data verification/lookup process. Performance validation will be conducted in UAT environment with all migrated data.  User Acceptance Testing   A dedicated environment is created for user acceptance testing which will have the ability to store all migrated data. This enables a ‘production’ like environment that users can test within.  Migrated data will be utilized during the User Acceptance testing to provide for real life scenarios.  The MST team will provide necessary test data, test plans and guidance as required to the Business Analyst and UAT Subject Matter Experts (SMEs). The UAT test plan will be prepared and shared based on the user stories and functionalities developed based on the feedback from end users.  These exercises comprise the defect resolution management aspect of the implementation.   Once UAT testing team logs and issue in the tracker, MST team reviews the feedback and triages the issues with team. Once triaged, the issue is logged in JIRA and fixed by the team. Then the MST team retests them once they are fixed before sending it back to the UAT team. The UAT fixes are validated with Business Analyst and SMEs from client team before considering them as done. | | | | | | |
| PTT-5 | Describe how the system allows changes to be tested before implementation in the production database. Examples include changing licensure requirements, license type name changes, and scripts to replace data. | | X | X |  |  |
| Response:  Salesforce provides for robust environment setups scenarios as described in the above requirements. Through the sandbox environments a pre-production and configuration and testing sandbox can be setup to ensure the testing of licensure requirements and name changes and versioning. Furthermore, Salesforce offers robust data management tools to allow for intake and export of data. More on testing described below in the summary of testing methods.  Summary of Testing Methods  The following are the specific testing methods in scope for the project and are completed from the unit testing and task level all the way to full-regression pre- and post-production:     * Quality Assurance testing * Regression Testing * User Acceptance Testing * Integration Testing * Performance Testing * End to End testing     Regression Testing   A regression test suite will be built over the period of overall testing which will be utilized for End to End Functional Testing. The list of regression use cases will be provided at each regression interval.  Regression testing is conducted at minimum every sprint to cover scenarios developed in previous sprint to ensure system integrity. All test results will be documented and provided to the team for review.  Performance Testing  While Salesforce provides various governor limits to help enhance performance in multi-tenant architecture, MST works with customers through the implementation to identify performance thresholds and designs the system to ensure support. MST will execute performance testing and provide detailed statistics on major application processing times which can include performance of portal form submission process, portal data verification/lookup process. Performance validation will be conducted in UAT environment with all migrated data.  User Acceptance Testing   A dedicated environment is created for user acceptance testing which will have the ability to store all migrated data. This enables a ‘production’ like environment that users can test within.  Migrated data will be utilized during the User Acceptance testing to provide for real life scenarios.  The MST team will provide necessary test data, test plans and guidance as required to the Business Analyst and UAT Subject Matter Experts (SMEs). The UAT test plan will be prepared and shared based on the user stories and functionalities developed based on the feedback from end users.  These exercises comprise the defect resolution management aspect of the implementation.   Once UAT testing team logs and issue in the tracker, MST team reviews the feedback and triages the issues with team. Once triaged, the issue is logged in JIRA and fixed by the team. Then the MST team retests them once they are fixed before sending it back to the UAT team. The UAT fixes are validated with Business Analyst and SMEs from client team before considering them as done. | | | | | | |

***Interfaces/Imports/Exports Requirements***

The system is required to be able to interface with other computer systems as necessary.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Req #** | **Requirement** | (1) Comply | (a) Core | (b) Custom | (c) 3rd Party |
| INT-1 | Describe the automated approach to managing interfaces. HL7 standards are available at [www.hl7.org](https://www.hl7.org/) | x |  | x |  |
| Response:  **Salesforce Integration**  Connecting Salesforce to an existing enterprise application is a common and frequently performed task. Integration options range from native Web Services support (APIs, outbound workflow, etc.) to import/export utilities to middleware integration via packaged connectors to toolkits for Java, .NET, and other open platforms. Our solution provides the ability to call out to virtually all common APIs, to enable synchronization, push / pull, and mashups with external apps/systems. Salesforce itself is based on web-service based APIs that in turn simplify access to Salesforce data from external systems. API-based integration is heavily leveraged by our customers.    The APIs are provided with the Salesforce Platform to build integration interfaces with third party applications or by our integration partners to use in their connectors. Any 3rd party application that accesses your Salesforce instance via the APIs, will be subject to the same security protections that are used in your Salesforce user interface. Therefore, the third-party application will need to use a "granted" user in order to access the Salesforce data. These are open APIs (based on industry-standards such as REST and SOAP) that you can use to integrate Salesforce endpoints with external endpoints such as apps or enterprise integration hubs. As an example, you have the Batch and Bulk APIs used in the Data integration patterns or the SOAP and REST APIs used for UI integration patterns.    Integration Options as various Layers of a Solution  Salesforce lets you choose integration methods at different layers to optimally align with business requirements, security policies, and master data management guidelines. Specifically, the State can choose how best to integrate across Security, User Interface, Business Logic and Data Integration layers. For more details on optimal design patterns for integration, see the Whitepaper “Integration Patterns and Practices” at: <https://resources.docs.salesforce.com/sfdc/pdf/integration_patterns_and_practices.pdf>.    Paths to Integration Success  Salesforce provides paths to integration success—all based on our industry-leading Web services API—and an extensive integration partner ecosystem. Integration with Salesforce means faster, simpler, and less-risky integration that doesn’t break during upgrades and delivers a new level of access and agility to your existing IT investments.     1. Choose your integration middleware - Salesforce is designed to work with all major integration middleware solutions. For a list of certified integration solutions, check out the Integration category in the AppExchange marketplace (https://appexchange.salesforce.com/category/integration). Here you’ll find pre-built connectors and the services of numerous integration technology partners such as IBM CastIron, Informatica Software and Jitterbit. 2. Build it yourself - For building custom integrations plus maximum flexibility and choice, the Salesforce Platform supports all major development environments and tools, including .NET, Java, PHP, Ruby on Rails, and many more. Learn more from our wiki developer network at <https://developer.salesforce.com/>. 3. Find it on the AppExchange - For the easiest and fastest way to add pre-integrated functionality, check the AppExchange directory. You can integrate with 5,000+ components and applications with the click of a mouse. Learn more at https://appexchange.salesforce.com. Here you will find both free and pay-as-you-go licensed add-ons. 4. Connect the clouds - Harness the power of multiple clouds. Learn how to connect Salesforce with the data and content of the most popular cloud services, including Amazon Web Services, Facebook, Google AppEngine, and Twitter. For example, you can enrich your Salesforce Contacts' profiles integrating with the likes of Facebook or Twitter to create a 360-degree single view of your customers.     For more information on integration capabilities, please visit: <https://developer.salesforce.com/page/Integration>.    Developer toolkits  These toolkits provide the ultimate in integration flexibility and choice. The Salesforce Platform supports all major development environments and tools, including Java, .NET, PHP, and Ruby on Rails.  **MuleSoft**  In addition to Salesforce's core integration capabilities, Salesforce also recently acquired MuleSoft, Inc. (“MuleSoft”), the provider of one of the world’s leading platforms for building application networks that connect enterprise apps, data and devices, across any cloud and on-premises. Together, Salesforce and MuleSoft will accelerate our customers’ digital transformations, enabling them to unlock data across legacy systems, cloud apps and devices to make smarter, faster decisions and create highly differentiated, connected customer experiences. The MuleSoft Anypoint Platform is generally available today.    At Salesforce, our mission is to help our customers connect to their customers in a whole new way. We do this by giving them a platform that abstracts away all of their complex enterprise systems and helps them build modern experiences that connect every system, every customer, and every device. A core and strategic piece of this is integration, and the foundation of the Salesforce Integration Cloud is MuleSoft. The MuleSoft Anypoint Platform enables over 1,600 organizations in approximately 60 countries to build application networks and meet the challenges of the digital economy. The MuleSoft Anypoint Platform is a horizontal solution that addresses a broad range of integration and API management use cases. Common use cases include:   * Pull data from external systems into Salesforce. * Expose data from existing systems to mobile apps, partners, and customers via APIs. * Sync data records between cloud applications and on-premise databases.     MuleSoft’s approach enables a new and more efficient IT operating model that leverages consumption-oriented, reusable assets to connect applications, data, and devices. MuleSoft’s Anypoint Platform provides a unified solution to solve integration and API management use cases. The Anypoint Platform uniquely combines integration with full API lifecycle management. The Anypoint Platform resolves many kinds of challenges—from tactical uses to mission-critical pains. It is adaptable and designed to swiftly solve the problems that organizations face today and in the future | | | | | |
| INT-2 | Describe how the system interfaces secure and protect the data and the associated infrastructure from a confidentiality, integrity and availability perspective. | x | x |  |  |
| Response: | | | | | |
| **Government Trusted Security and Infrastructure**  Salesforce understands that the confidentiality, integrity, and availability of our customers’ information are vital to their business operations and Salesforce's own success. Salesforce uses a multi-layered approach to protect that key information, constantly monitoring and improving our application, systems, and processes to meet the growing demands and challenges of security.    Independent audits confirm that our security goes far beyond what most companies have been able to achieve on their own. Using the latest firewall protection, intrusion detection systems, and TLS encryption, Salesforce gives you the peace of mind only a world-class security infrastructure can provide.    Third-party validation  Security is a multidimensional business imperative that demands consideration at multiple levels, from security for applications to physical facilities and network security. In addition to the latest technologies, world-class security requires ongoing adherence to best-practice policies. To ensure this adherence, we continually seek relevant third-party certification, including ISO 27001, the SysTrust audit (the recognized standard for system security), and SSAE 16 SOC 1 audit (an examination and assessment of internal corporate controls, previously known as SAS 70 Type II). SOC1, SOC2 and SOC3 audits are performed by a third-party auditor annually at a minimum. Additional audits and certifications include CSA ‘Consensus Assessments Initiative’, JIPDC (Japan Privacy Seal), Tuv (Germany Privacy Mark), and TRUSTe.    Protection at the application level  Salesforce protects customer data by ensuring that only authorized users can access it. Administrators assign data security rules that determine which data users can access. Sharing models define organization-wide defaults and data access based on a role hierarchy. All data is encrypted in transfer. All access is governed by strict password security policies. All passwords are stored in SHA 256 one-way hash format. Applications are continually monitored for security violation attempts.    Protection at the facilities level  Salesforce security standards are stringent and designed with demanding customers in mind, including the world’s most security-conscious financial institutions. Authorized personnel must pass through five levels of biometric scanning to reach the Salesforce system cages. All buildings are completely anonymous, with bullet-resistant exterior walls and embassy-grade concrete posts and planters around the perimeter. All exterior entrances feature silent alarm systems that notify law enforcement in the event of suspicion or intrusion. Data is backed up to disk. These backups provide a second level of physical protection and disks never leave the data center.    Protection at the network level  Multilevel security products from leading security vendors and proven security practices ensure network security. To prevent malicious attacks through unmonitored ports, external firewalls allow only http and https traffic on ports 80 and 443, along with ICMP traffic. Switches ensure that the network complies with the RFC 1918 standard, and address translation technologies further enhance network security. IDS sensors protect all network segments. Internal software systems are protected by two-factor authentication, along with the extensive use of technology that controls points of entry. All networks are certified through third-party vulnerability assessment programs.    Trust.salesforce.com is the Salesforce community’s home for real-time information on system performance and security. On this site you'll find:   * Up-to-the minute information on planned maintenance * Phishing, malicious software, and social engineering threats * Best security practices for the State * Information on how we safeguard your data   **100% Multi-Tenant, Cloud Application**  Salesforce offers the market leading Platform as a Service (PaaS) and market leading Software as a Service (SaaS) solutions.  Salesforce is a multi-tenant, cloud-based web application. No additional software or infrastructure is required. Salesforce hosts the entire solution, thus freeing up the State to manage its mission, not manage an infrastructure solution. Additionally, Salesforce is browser agnostic and supports all major browsers (Firefox, Chrome, Safari, IE, Edge). No installations on users’ laptops or desktops are required and thus the solution is accessible from anywhere an internet connection and supported browser are available, including mobile devices.  The fully documented list of supported browsers and mobile devices for the full Salesforce site and Salesforce Mobile is available in the following articles in online our Help & Training Portal: https://help.salesforce.com/HTViewHelpDoc?id=getstart\_browser\_overview.htm&language=en\_US and <https://help.salesforce.com/articleView?id=sf1_requirements.htm&type=0&language=en_US&release=206.5>.  **Superior Uptime**  Salesforce has maintained high levels of availability across all Salesforce instances since inception. As the only on-demand vendor to provide daily service-quality data on a public Web site (https://trust.salesforce.com), Salesforce proves that we are the leader in availability. And by making its track record completely transparent, Salesforce proves we are worthy of our customers’ trust. To ensure maximum uptime and continuous availability, Salesforce provides the best redundant data protection and most advanced facilities protection available, along with a complete data recovery plan—all without affecting performance.  Salesforce uses commercially reasonable efforts to make its on-demand services available to its customers 24/7, except for planned downtime, for which Salesforce gives customers prior notice, and force majeure events. Excellent availability statistics are critical to Salesforce's customers’ success and to the success of Salesforce as a company. Live availability status and historical availability is publicly published at https://trust.salesforce.com/en/#systemStatus.  The persistence layer underlying the Salesforce Platform is proven database technology that powers all of Salesforce’s products today, serving more than 150,000 organizations and over 5 billion transactions per day with an average request response time of less than 200 milliseconds, all with an average uptime of 99.9+ percent.  Salesforce does not typically offer Service Level Agreements as part of the base service offering. Our approach is to offer a service with high availability and fast resolution of problems. If a customer requires an SLA it will be negotiated separately. | | | | | |
| INT-3 | Describe how the system has the capability to notify system administrators/ system support staff if an interface is not available for any reason. | X |  |  |  |
| Response:  When the Salesforce system sends a message to the external system and if it is not available, then a error is logged in a custom error log and an automated email notification will be sent to the System Administrator. In addition, Salesforce Services will always be available, at times issues could occur due to one of the following,   1. Credential change that was not communicated to the client 2. IP address restrictions – need to whitelist client IP address   In these situations, we would handle these errors by logging the error in a custom error log table and update System Administrator when such an error occurs through automated email notifications. | | | | | |
| INT-4 | Describe how the system provides necessary application program interfaces and/or web services to allow DHHS to create interfaces to and from the system.  Exact number of imports/exports required. DHHS anticipates disciplinary databanks, compacts, schools, exam companies, and employers may interact with the system. | X |  |  |  |
| Response:  Salesforce provides OAuth open protocol that authorizes a client application to access data from a protected resource through the exchange of tokens. OAuth tokens are essentially permissions given to a client application. The resource server can validate the tokens and allow the client application access to the defined protected resources. In Salesforce, you can use OAuth authorization to approve a client application’s access to your org’s protected resources. | | | | | |
| INT-5 | Describe how the system supports data exchanges between components in real time so that data is always synchronous across the entire system, including any third-party components. | X |  |  |  |
| Response:  Data exchange between different systems and Salesforce is made possible through SOAP/REST services. We would automate the data exchange in form of an outbound request from Salesforce based on User action like clicking a button, this would trigger an outbound callout and for an inbound request from external systems we have an endpoint listener that processes the incoming request and persists the data in Salesforce. | | | | | |
| INT-6 | Describe how the system has the ability to expand data access to additional systems that are consistent with current data standards. | XX |  |  |  |
| Response:  Both external/internal systems can access Salesforce data using SOAP/REST services. To consume the data, third party systems would be provided with Oauth authentications details, this enables the system to request and post data to Salesforce. Access to data for the integration systems are defined using Profiles and for additional needs appropriate Permission Sets would be provided to the individual integration user. | | | | | |
| INT-7 | Describe how the system conducts end-to-end testing with interface partners, both external and internal, to ensure requirements are met. |  |  |  |  |
| Response:  We perform end-to-end testing using manual/automation testing process as per need of the project. Integrating with external systems would involve both inbound/outbound requests, we use open source tools like postman to validate the requests and responses. Proper error handling/validations will be built around the integration module to handle errors and to notify System administrator. | | | | | |

***System Performance Requirements***

This section describes requirements related to the systems' on-line performance, response times, and sizing from a system architecture standpoint.

\*NOTE\*: If your system has specific high availability or redundancy requirements, the requirements must be defined below (see PER-5).

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Req #** | **Requirement** | (1) Comply | (a) Core | (b) Custom | (c) 3rd Party |
| PER-1 | Describe the system performance functionality and monitoring tools. | x |  | x |  |
| Response:  **Superior Uptime**  Salesforce has maintained high levels of availability across all Salesforce instances since inception. As the only on-demand vendor to provide daily service-quality data on a public Web site (https://trust.salesforce.com), Salesforce proves that we are the leader in availability. And by making its track record completely transparent, Salesforce proves we are worthy of our customers’ trust. To ensure maximum uptime and continuous availability, Salesforce provides the best redundant data protection and most advanced facilities protection available, along with a complete data recovery plan—all without affecting performance.  Salesforce uses commercially reasonable efforts to make its on-demand services available to its customers 24/7, except for planned downtime, for which Salesforce gives customers prior notice, and force majeure events. Excellent availability statistics are critical to Salesforce's customers’ success and to the success of Salesforce as a company. Live availability status and historical availability is publicly published at https://trust.salesforce.com/en/#systemStatus.  The persistence layer underlying the Salesforce Platform is proven database technology that powers all of Salesforce’s products today, serving more than 150,000 organizations and over 5 billion transactions per day with an average request response time of less than 200 milliseconds, all with an average uptime of 99.9+ percent.  Salesforce does not typically offer Service Level Agreements as part of the base service offering. Our approach is to offer a service with high availability and fast resolution of problems. If a customer requires an SLA it will be negotiated separately.  **Overall System Monitoring**  Overall system monitoring is provided by a variety of tools. All monitoring alerts are aggregated and monitored by the Site Reliability (SR) team. Alerts such as configuration changes from network devices, server state changes, and other events can be correlated to indicate root cause. The dynamic model capability also allows the customization of the monitoring tool to mimic Salesforce Service's hardware/software configuration, so that custom symptoms and problems can be rolled up into the correlation engine.  Salesforce has built extensive monitoring and instrumentation into the application itself, so that the application can accurately report its health and performance to the systems engineers, network operations staff, QA personnel, and developers. All network devices, servers, services, and most application processes are monitored from the dedicated monitoring host.  The Site Reliability (SR) team monitors the Production network 24x7 and is on call for issue resolution. Any potential issues identified by the monitoring tools provide visual and/or email alerts to SR and other appropriate technical operations personnel. Alerts trigger analysis and response procedures. Further notification using established procedures may be executed based on the severity of the issue. In the event of an operational issue, Salesforce's goal is to rapidly restore service.  Management and operations of the Production network is a coordinated effort between the technical operations teams. Several system and application performance monitoring tools are used in the environment. Network devices, servers, services, and application processes are monitored with appropriate tools. Data is aggregated into an event monitoring tool which performs alerting and event correlation.  **Trust.salesforce.com**  Trust.salesforce.com is the Salesforce community’s home for real-time information on system performance and security. On this site you'll find:   * Up-to-the minute information on planned maintenance * Phishing, malicious software, and social engineering threats * Best security practices for the State * Information on how we safeguard your data   The Trust site includes an API that the State can use to directly integrate Salesforce availability information into existing monitoring tools or processes. For example, the State can retrieve the status of a given instance, details on any active availability or performance incidents, transaction performance data, and the upcoming planned maintenance schedule.  Details on all available API endpoints can be found here: <https://api.status.salesforce.com/v1/docs/>.  Also see additional information on Trust.salesforce.com at: [https://trust.salesforce.com/en/statususerguide/ and https://status.salesforce.com/status](https://trust.salesforce.com/en/statususerguide/).  **Health Check**  Health Check lets the State understand and proactively remediate your Salesforce org’s security risks and vulnerabilities from a single page.    At a glance, Health Check can see and fix security risks for your org in your Session Settings, Password Policies, and Network Access settings. A health check dashboard shows how well your org measures against the Salesforce-recommended baseline. You can customize the Health Check security baseline to compare your org’s security settings with your industry standards. Alternatively, you can upload up to five custom baselines.    The Salesforce Baseline standard contains recommended values for the Session Settings, Password Policies, and Network Access setting groups. If you change all of a group’s settings to be less restrictive than what’s in the Salesforce Baseline standard, your health check score decreases.    The dashboard shows high and medium risk settings and how they compare against the standard. To remediate a risk, click the edit link next to the setting. All of your settings that meet the standard are listed at the bottom.    For example, suppose that you changed your password minimum length from 8 (the default value) to 5, and changed other Password Policies settings to be less restrictive. These changes make your users’ passwords more vulnerable to guessing and other brute force attacks. As a result, your overall score decreases, and the settings are listed as risks.    For more information please see Security Health Check: <https://help.salesforce.com/HTViewHelpDoc?id=security_health_check.htm> and How Is the Health Check Score Calculated?: <https://help.salesforce.com/HTViewHelpDoc?id=security_health_check_score.htm>.    Salesforce also offers a Health Check API, which consists of two read-only Tooling API objects: SecurityHealthCheck and SecurityHealthCheckRisks. The State can make SOQL queries to retrieve your org’s security settings, risks, Health Check score, and Salesforce baseline settings. You can add this information to your security monitoring systems and dashboards to verify that multiple Salesforce applications have the same security posture.    For security reasons, only users with both the “View Setup and Configuration” and “Modify All Data” user permissions can view and edit information on the Health Check page in Setup. In addition to password policies, session settings, and network access settings, the State can also identify and fix security risks for login access policies and remote site settings. | | | | | |
| PER-2 | Describe the minimum response times for the following functions, even at peak load. For example, expected response time will be within two (2) seconds 95% of the time, and under five (5) seconds for 100% of the time.   1. Record Search Time 2. Record Retrieval Time 3. Transaction Response Time 4. Print Initiation Time 5. Subsequent Page Display Response Time 6. Document Availability   Note: These response times do not include network latency, which will be measured and reported by DHHS. | x |  | x |  |
| Response:  **Application Response Times**  Salesforce routinely processes over 5 billion transactions during normal business days. Of the over 5 billion transactions performed daily on the Salesforce multi-tenant infrastructure, approximately 40% of these transactions are through the API. In general, we average response times around 200 milliseconds. | | | | | |
| PER-3 | Describe how the system captures system downtimes, along with the causes of the downtimes where applicable. Describe the method and timing of communication to DHHS on downtimes. | x |  | x |  |
| Response:  **Monitoring Performance**  Trust.salesforce.com is the Salesforce community’s home for real-time information on system performance and security. On this site you'll find:   * Up-to-the minute information on planned maintenance * Phishing, malicious software, and social engineering threats * Best security practices for the State * Information on how we safeguard your data     The Trust site includes an API that the State can use to directly integrate Salesforce availability information into existing monitoring tools or processes. For example, the State can retrieve the status of a given instance, details on any active availability or performance incidents, transaction performance data, and the upcoming planned maintenance schedule.    Details on all available API endpoints can be found here: <https://api.status.salesforce.com/v1/docs/>.    Also see additional information on Trust.salesforce.com at: [https://trust.salesforce.com/en/statususerguide/ and https://status.salesforce.com/status](https://trust.salesforce.com/en/statususerguide/).  **Maintenance and Upgrades**  When maintenance is scheduled, Salesforce publishes the dates and times of the maintenance windows on trust.salesforce.com which show a forward 12-month view of the maintenance windows Salesforce plans to take. Premier Alerts are sent via email when the maintenance windows are posted to trust.salesforce.com. Approximately one week prior to the scheduled maintenance, Salesforce communicates those dates and times via the in-application pop-up window upon login to Salesforce. In the event of planned maintenance that requires customer action in advance (e.g. updating network settings in preparation for additional login pools), Salesforce endeavors to communicate via email to system administrators of the State months prior to the maintenance.    Please note: If emergency system maintenance is required, customers may be notified less than one (1) week in advance.    There are two types of maintenance at Salesforce: System Maintenance and Release Maintenance.   * System Maintenance is for sustaining the security, availability, and performance of the infrastructure supporting Salesforce services. * Release Maintenance is for upgrading Salesforce services to the latest product version to deliver enhanced features and functionality. There are three different kinds of release maintenance: major releases, patch releases, and emergency releases.     Major Release Maintenance dates and times are posted on trust.salesforce.com approximately one year before the release date. To see the schedule for your instance click on <https://status.salesforce.com/status> and select the relevant instance. On the calendar click the release date to view further information. Major release maintenance occurs three times per year during the windows listed below. The instance will be unavailable for up to five minutes during the release window.    Patch Releases and Emergency Releases are used to deliver scheduled and ad hoc application fixes and are typically seamless to customers. Whenever possible, patches and emergency releases are deployed during off-peak hours and without downtime. Patch releases are scheduled weekly and are usually deployed to instances on Tuesday, Wednesday or Thursday, with release to Asia-Pacific instances the following day. Emergency releases are conducted on an as-needed basis and can occur any day of the week.    Please refer to the following Help & Training article for more information: <https://help.salesforce.com/apex/HTViewSolution?id=000176208&language=en_US>. | | | | | |
| PER-4 | Describe how the system supports concurrent users with minimal impact to response time, with the ability to increase the demand on the system by 50% without modification to the software or degradation in performance. | x |  | x |  |
| Response:  **Scalability**  Salesforce is a pure multi-tenant, cloud-based web application. Multi-tenancy gives applications elasticity. Salesforce applications can automatically scale from one to millions of users. Processing more than 5 billion transactions each day, Salesforce is used for large-scale deployments. Any application that runs on the Salesforce Platform is automatically architected to seamlessly scale from 1 user to millions of users without the customer having to do anything differently.  All applications (including mobile, offline and read-only options) and data running on the Salesforce Platform are deployed to and replicated across multiple data centers in different geographies. Every application, no matter how large or small, gets the full benefits of the backup, failover, disaster recovery, and other infrastructure services required for an organization’s mission-critical applications. | | | | | |
| PER-5 | Describe how the system is available online 24 hours a day and 7 days a week. Describe any known timeframes where the system will be unavailable for use. | X | X |  |  |
| Response:  **Superior Uptime**  Salesforce has maintained high levels of availability across all Salesforce instances since inception. As the only on-demand vendor to provide daily service-quality data on a public Web site (https://trust.salesforce.com), Salesforce proves that we are the leader in availability. And by making its track record completely transparent, Salesforce proves we are worthy of our customers’ trust. To ensure maximum uptime and continuous availability, Salesforce provides the best redundant data protection and most advanced facilities protection available, along with a complete data recovery plan—all without affecting performance.  The persistence layer underlying the Salesforce Platform is proven database technology that powers all of Salesforce’s products today, serving more than 150,000 organizations and over 5 billion transactions per day with an average request response time of less than 200 milliseconds, all with an average uptime of 99.9+ percent.  Salesforce uses commercially reasonable efforts to make its on-demand services available to its customers 24/7, except for planned downtime, for which Salesforce gives customers prior notice, and force majeure events. Excellent availability statistics are critical to Salesforce's customers’ success and to the success of Salesforce as a company. Live availability status and historical availability is publicly published at https://trust.salesforce.com/en/#systemStatus.  Salesforce does not typically offer Service Level Agreements as part of the base service offering. Our approach is to offer a service with high availability and fast resolution of problems. If a customer requires an SLA it will be negotiated separately.  **Upgrades & Maintenance**  All upgrades, patches, and other system maintenance are provided as part of the subscription service with no additional cost to the State. In addition, Salesforce releases 3 complimentary upgrades each year, in Winter, Spring, and Summer versions. All Salesforce users are always on the latest version of our platform because everyone gets instant upgrades (typically on an opt-in basis). Each time Salesforce releases a new version of the application and the platform, the entire community can take advantage of the latest innovations from our product development team. Because of our multi-tenant architecture, Salesforce is able to provide all of our customers with a service based on a single version of our application. We are able to upgrade all of our customers at the same time with each release. As a result, we do not have to maintain multiple versions of our application. Each release will be delivered automatically in a transparent manner, and will not break your configurations.  When maintenance is scheduled, Salesforce publishes the dates and times of the maintenance windows on trust.salesforce.com which show a forward 12-month view of the maintenance windows Salesforce plans to take. Premier Alerts are sent via email when the maintenance windows are posted to trust.salesforce.com. Approximately one week prior to the scheduled maintenance, Salesforce communicates those dates and times via the in-application pop-up window upon login to Salesforce. In the event of planned maintenance that requires customer action in advance (e.g. updating network settings in preparation for additional login pools), Salesforce endeavors to communicate via email to system administrators of the State months prior to the maintenance.  Please note: If emergency system maintenance is required, customers may be notified less than one (1) week in advance.  There are two types of maintenance at Salesforce: System Maintenance and Release Maintenance.   1. System Maintenance is for sustaining the security, availability, and performance of the infrastructure supporting Salesforce services. 2. Release Maintenance is for upgrading Salesforce services to the latest product version to deliver enhanced features and functionality. There are three different kinds of release maintenance: major releases, patch releases, and emergency releases.     Major Release Maintenance dates and times are posted on trust.salesforce.com approximately one year before the release date. To see the schedule for your instance click on <https://status.salesforce.com/status> and select the relevant instance. On the calendar click the release date to view further information. Major release maintenance occurs three times per year during the windows listed below. The instance will be unavailable for up to five minutes during the release window.  Patch Releases and Emergency Releases are used to deliver scheduled and ad hoc application fixes and are typically seamless to customers. Whenever possible, patches and emergency releases are deployed during off-peak hours and without downtime. Patch releases are scheduled weekly and are usually deployed to instances on Tuesday, Wednesday, or Thursday, with release to Asia-Pacific instances the following day. Emergency releases are conducted on an as-needed basis and can occur any day of the week.  Please refer to the following Help & Training article for more information: <https://help.salesforce.com/apex/HTViewSolution?id=000176208&language=en_US>. | | | | | |
| PER-6 | Describe how the system provides application performance monitoring and management capabilities, including any key performance indicators (KPI) or other metrics to measure and report system performance for the proposed system. | X | X |  |  |
| Response:  Trust.salesforce.com is the Salesforce community’s home for real-time information on system performance and security. On this site you'll find:   * Up-to-the minute information on planned maintenance * Phishing, malicious software, and social engineering threats * Best security practices for the State * Information on how we safeguard your data   The Trust site includes an API that the State can use to directly integrate Salesforce availability information into existing monitoring tools or processes. For example, the State can retrieve the status of a given instance, details on any active availability or performance incidents, transaction performance data, and the upcoming planned maintenance schedule.  Details on all available API endpoints can be found here: <https://api.status.salesforce.com/v1/docs/>.  Also see additional information on Trust.salesforce.com at: [https://trust.salesforce.com/en/statususerguide/ and https://status.salesforce.com/status](https://trust.salesforce.com/en/statususerguide/).  **Overall System Monitoring**  Overall system monitoring is provided by a variety of tools. All monitoring alerts are aggregated and monitored by the Site Reliability (SR) team. Alerts such as configuration changes from network devices, server state changes, and other events can be correlated to indicate root cause. The dynamic model capability also allows the customization of the monitoring tool to mimic Salesforce Service's hardware/software configuration, so that custom symptoms and problems can be rolled up into the correlation engine.  Salesforce has built extensive monitoring and instrumentation into the application itself, so that the application can accurately report its health and performance to the systems engineers, network operations staff, QA personnel, and developers. All network devices, servers, services, and most application processes are monitored from the dedicated monitoring host.  The Site Reliability (SR) team monitors the Production network 24x7 and is on call for issue resolution. Any potential issues identified by the monitoring tools provide visual and/or email alerts to SR and other appropriate technical operations personnel. Alerts trigger analysis and response procedures. Further notification using established procedures may be executed based on the severity of the issue. In the event of an operational issue, Salesforce's goal is to rapidly restore service.  Management and operations of the Production network is a coordinated effort between the technical operations teams. Several system and application performance monitoring tools are used in the environment. Network devices, servers, services, and application processes are monitored with appropriate tools. Data is aggregated into an event monitoring tool which performs alerting and event correlation. | | | | | |

***System and User Documentation Requirements***

DHHS requires the Contractor to develop, electronically store and distribute system documentation to include, at a minimum:

1. Reference Materials
2. System Documentation
3. A complete Data Dictionary

The Contractor must provide a complete Data Dictionary. The Data Dictionary is to include definitions of all data elements and tables where they reside.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Req #** | **Requirement** | (1) Comply | (a) Core | (b) Custom | (c) 3rd Party |
| DOC-1 | Describe how the system provides on-line help for all features, functions, and data element fields, as well as descriptions and resolutions for error messages, using help features including indexing, searching, tool tips, and context-sensitive help topics. Provide a sample copy of five (5) screen shots with on-line help. | X | X |  |  |
| Response:  **Salesforce Training & Learning Resources**  Salesforce incorporates the following training and learning resources and best practices as part of the proposed subscription service as well as additional Salesforce instructor-led training that is available for an additional cost. There are also a variety of training resources accessible from within the Salesforce application.    Salesforce Help & Training Portal  Salesforce provides an intuitive help and training portal which brings together a rich set of resources that would give the State a centralized way to help solve problems quickly and easily. Salesforce also provides context-sensitive help icons throughout the application screens to make it easier for users to get unique help without searching. It is notable that we don’t provide large, offline help manuals but rather, all our help is online, so we assure that online help is extremely thorough and effective for usability.  The Help site:   * Is fully customizable - You can personalize Help to meet your specific needs, customizing the gadget layout to show what is important to you * Allows users to get the right answers, fast - Knowledgebase is more intelligent and comprehensive than ever (Auto Suggestion of Search Terms, Expanded Knowledge Repository [Help Docs, Solutions, FAQs, Training, Best Practices], and Refinement by Dimension) * Provides chat - New engagement Channel gives customers the ability to chat with the Salesforce support team in real time * Has easy case management - Opening and reviewing cases is easier than ever * Makes your administrator’s life easier - Administrators gain insight with enhanced reporting on cases and organization information   Salesforce Printable Tip Sheets & User Guides  In addition to online help, Salesforce publishes printable documentation to help you be successful with Salesforce. These documents include tip sheets, user guides, and other resources that describe the features and capabilities of Salesforce. Link here for Getting Started information: <https://pages.mail.salesforce.com/gettingstarted/home/> and here to Salesforce’s online documentation: <https://help.salesforce.com/articleView?id=salesforce_help_map.htm&type=5>.    Trailhead: the Free, Fun Way to Learn Salesforce  Trailhead is accessible through the Search Documentation link in-app or through the Trailhead web page.    Everyone can learn Salesforce. Whether you are an admin, user or developer, there is a learning trail for you. Customers can sign up for a free Developer edition account and take advantage of the fun and free interactive learning curriculum provided at Salesforce Trailhead (<https://trailhead.salesforce.com/en/home>). Users can pick specific trails, modules or projects based on role (admin, user, etc.), experience level (beginner, intermediate, advanced), products (Service Cloud, Salesforce Platform, etc) or topics (App Logic, CRM, Data Management, etc) to learn new skills and absorb the information they need quickly.     * Trails - There are over 170 trails to choose from that provide guided learning paths through modules and projects and help users cover the most ground in the shortest amount of time. They provide users a game plan for exploring new skills. Trails include Admin Beginner, Admin Intermediate, Developer Beginner, Develop Intermediate, CRM Essentials, Analytics, and more. * Modules - There are nearly 655 modules that dive into specific topics. Modules introduce users to specific topics in bite-sized units. Users learn what a feature is, when it's helpful, and how to use it. Users can then test themselves with interactive challenges. * Projects - There are over 109 projects to choose from that provide users hands-on practice applying what they've learned. Projects give users hands-on practice with Salesforce technologies via step-by-step instructions and enable users to gain new skills and confidence working in Salesforce faster than they thought possible. * Super Badges - Take the skills you've developed through Modules and Projects and apply them to real world, hands-on challenges. * Trailhead Live - Live and on-demand videos from experts covering everything from certification preparation to building reports and dashboards, to coding best practices.     Developer Community  The State will also have access to the Developer Community, Salesforce's free developer program for the Salesforce Platform. The Developer Community website is a free community-based online portal for developers, where developers can learn, access key resources, and discuss a diverse set of topics anchored around the Salesforce Platform. These topics include Apex Code, Visualforce, Web service APIs, database topics, packaging and distribution of your applications, and much more.    The Salesforce Developer Community is comprised primarily of a technical body of developers and architects, system administrators and IT management.    The primary goal for the Developer Community is to promote community, learning and conversations. This is done through articles, the blogging community and its blogs, tech notes, sample code, providing a free Developer Edition account, together with discussion boards, RSS feeds, documentation, webinars, on-demand sessions, newsletters, event calendar and wikis.    Salesforce Premier+ Success Plan  With the Premier+ Success support plan, which includes support, training, and administration, the State will have unlimited access to our complete library of more than 100 online courses to build expertise in Salesforce products, drive value, and maximize ROI.    Customer Success Community  Customer Success offers many resources and tools to get started, including the Customer Resource Center ([success.salesforce.com](https://success.salesforce.com/)) with online Help, Learning Center and Communities, where you can tap into training videos, a knowledgebase, or reach out to other customers for best practices.    Ongoing success monitoring is a key part of Customer Success. Salesforce’s cloud computing model enables us to monitor usage data, to determine whether customers are getting the most from their subscription. We share this information with customers through Personal Account Reviews and Success Scorecards, along with actionable recommendations for improvement. Customer Success offers programs to help customers roll out new features or products, with training and adoption toolkits, to ensure our customers’ business benefit is always growing, and that they remain customers for life.    Additional Salesforce Training  Should the State desire instructor-led training in addition to online training and training that is included in the Premier+ Success Plan, for an additional cost, Salesforce offers a number of instructor-led courses tailored for user types. More information is provided at:<https://www.salesforce.com/services/learn/classes/#!page=1>.    Salesforce provides comprehensive training and certification options for every Salesforce user whether Administrator, Developer, Business Analyst, and others. Putting the right training plan in place for all Salesforce users is essential to a successful ongoing deployment. Salesforce Certification provides assurance that the team responsible for your Salesforce deployment is an expert in their field and up to date on the latest capabilities from Salesforce. As your team gets trained, certification is an important milestone to demonstrate readiness. And as you hire and contract with Salesforce Partners, be sure to look for Salesforce Certified Professionals to ensure that you are getting the right level of expertise, whether that is Certified Administrators, Developers, Solution Designers, or Technical Architects.    Training is available as:   * Self-paced, online courses as part of Premier Success Plan subscription * Instructor-led classes delivered by Salesforce Certified Instructors at our facilities and through our Partners worldwide * Private training classes held at your facilities, delivered by Salesforce Certified Instructors     For a complete list of courses, review the course catalog at [www.salesforce.com/training](http://www.salesforce.com/training). Learn more about the benefits of Salesforce Certification at [www.salesforce.com/certification](http://www.salesforce.com/certification).  **Tableau Training & Learning Resources**  Tableau has a variety of opportunities for training.   * A free guided set of training based on role: <https://www.tableau.com/learn/get-started> * A free set of video-based training: <https://www.tableau.com/learn/training/20201> * e-Learning training: <https://www.tableau.com/learn/training/elearning> * Classroom training: <https://www.tableau.com/learn/classroom> | | | | | |
| DOC-2 | Describe how the system provides on-line user reference materials with a printable version available. The documentation must include full mock-ups of all screens/windows and provide narratives of the navigation features for each window/screen. Provide a sample copy of five (5) pages of the user reference materials. | X | X |  |  |
| Response:  In addition to Salesforce training and learning resources, self-learning user manuals can be made available within Salesforce in Word or PDF format. User manuals in the form of Word or PDF documents can be uploaded to Salesforce and can be provided as a help link for System users to refer and print when necessary. | | | | | |
| DOC-3 | Describe how the system will have on-line reporting reference materials with a printable version available that includes descriptions, definitions, and layouts for each standard report. Include definitions of all selection criteria parameters and each report item/data element, all field calculations defined in detail, and field and report titles. Provide a sample copy of five (5) pages of the reporting reference materials. | X | X |  |  |
| Response:  As part of the Salesforce platform, training materials, reporting diagrams and dictionaries can be built into the system to ensure proper reference points for all reports, layouts and other important parameters. | | | | | |
| DOC-4 | Describe how the system provides an entity-relationship model, class diagram, and a table of contents with data dictionary for report creation by the State that is regularly updated and includes table, field, and relationships. | X | X |  |  |
| Response:  Salesforce provides a Schema Builder online tool, a dynamic environment for viewing and modifying all the objects and relationships in your app. This greatly simplifies the task of designing, implementing, and modifying your data model, or schema. Schema Builder is enabled by default.  You can view your existing schema and interactively add new custom objects, custom fields, and relationships, simply by dragging and dropping. Schema Builder automatically implements the changes and saves the layout of your schema any time you move an object. This eliminates the need to click from page to page to find the details of a relationship or to add a new custom field to an object in your schema.  Schema Builder provides details like the field values, required fields, and how objects are related by displaying lookup and master-detail relationships. You can view the fields and relationships for both standard and custom objects.  Schema Builder lets you add the following to your schema:   * Custom objects * Lookup relationships * Master-detail relationships * All custom fields except: Geolocation | | | | | |
| DOC-5 | Describe how the system provides a data dictionary which includes user-defined fields and tables which can be viewed online and kept updated for each modification. | X | X |  |  |
| Response:  Salesforce provides a Schema Builder online tool, a dynamic environment for viewing and modifying all the objects and relationships in your app. This greatly simplifies the task of designing, implementing, and modifying your data model, or schema. Schema Builder is enabled by default.  You can view your existing schema and interactively add new custom objects, custom fields, and relationships, simply by dragging and dropping. Schema Builder automatically implements the changes and saves the layout of your schema any time you move an object. This eliminates the need to click from page to page to find the details of a relationship or to add a new custom field to an object in your schema.  Schema Builder provides details like the field values, required fields, and how objects are related by displaying lookup and master-detail relationships. You can view the fields and relationships for both standard and custom objects.  Schema Builder lets you add the following to your schema:   * Custom objects * Lookup relationships * Master-detail relationships * All custom fields except: Geolocation | | | | | |