**The tables below list EUTF’s technical requirements for the Benefits Administration System.** Requirements have been broken into two types: mandatory and optional.Mandatory requirements are further broken out based on the degree of flexibility available in delivering the requirement.Offerors must confirm that they meet all mandatory technical requirements as identified below. An offeror's failure to meet these requirements will cause their proposal to be considered non-responsive and rejected.

The tables in the following sections reference different flexibility levels. The table below describes EUTF’s definitions of these priorities and the specific implementation rules. The Offeror must include in their fixed-price bid all functionality included in the Mandatory Requirements.

|  |  |  |
| --- | --- | --- |
| **Flexibility Rating** | **Definition** | **Comments** |
| **Rating 1** | **Mandatory** – No flexibility in how requirement is met | EUTF must have this requirement and it must be implemented to adhere to business rules and/or legislation. The solution must meet the requirement and conform to EUTF’s business process. The vendor must include in their fixed-price bid all functionality identified as Rating 1. |
| **Rating 2** | **Mandatory** – Flexible in how requirement is met | EUTF must have this requirement but is flexible in the way it is designed and implemented. EUTF will adjust its business process to meet the solution. The vendor must include in their bid all functionality identified as Rating 2. |
| **Rating 3** | **Optional** – Desired if requirement can be met without additional cost | EUTF would like this requirement fulfilled, but understands it might be outside the scope of the vendor’s BAS solution. |

Optional requirements are listed after all mandatory requirements. OFFEROR must confirm if they can or cannot meet each requirement within their fixed price proposal. If the requirement can be met at additional cost, OFFEROR should select “Additional” and include details in the Summary tab of Appendix D, *Cost Proposal Workbook*.

**For the mandatory requirements, indicate the Degree of Customization Required in the applicable field:**

1. **Configuration**. Existing system functionality will be configured to deliver the requirement. This includes setting of parameter values, updates to factor and value tables, updating rules engines, and selection from any available configuration options within the existing software release. Configuration changes would not be expected to have any impact on future software updates.
2. **Minor Customization**. To meet the requirement, existing functionality will be modified to incorporate unique EUTF customizations not within the existing software release. This includes customization within well-defined exit/entry points within the system, interface file format definitions, custom formulas, custom SQL or SQR code for queries or reports, and addition/modification of data fields. Minor Customizations would not be expected to have an impact on future software updates.
3. **Major Customization**. Existing functionality to meet the requirement does not currently exist within an existing module, feature, or system component. This includes EUTF-specific extensions/enhancements/customizations to existing functionality, EUTF-specific APIs, protocols, or standards, and back-porting features from another version of the system. These are customizations that would not normally be reviewed or tested by the Contractor as part of their general System release testing and validation. Special care would be required to ensure compatibility with future software updates.
4. **Other** (describe in comments). Existing functionality to meet the requirement does not currently exist and would require either a new functionality be added to the System, e.g. a new module, feature, or system component, the use of third-party technology specifically to meet EUTF’s requirement, or the requirement will be met outside of the System either manually or with a standalone tool.

# MANDATORY REQUIREMENTS

**Complete this section by checking either “Yes” or “No” below.** Offerors who select “No” will be deemed non-responsive and rejected.

| **Do you agree your firm can meet all Mandatory Technical Requirements listed below (Ratings 1 and 2)?** | **Meets All Requirements?** |
| --- | --- |
| Yes No |

## T-01\_Application Architecture

| **ReqID** | **Sub-process** | **Requirement Details** | **Flexibility Rating** | **Degree of Customization** | **Comments** |
| --- | --- | --- | --- | --- | --- |
| T01.01 | Architecture | The proposed BAS architecture must be web-based. | 2 |  |  |
| T01.02 | Architecture | The System must operate in a virtualized environment. | 2 |  |  |
| T01.04 | Data | Data must be viewable and extractable based upon EUTF specified "as is" dates. At a minimum the System must be capable of producing a "snapshot" as of the end of each plan year. Note: EUTF plans have different plan years. | 2 |  |  |
| T01.05 | Data | The System must support the categorization of information per EUTF categorization of information policies. | 2 |  |  |
| T01.06 | Data | The System must provide the capability to move all historical, expired and/or unnecessary data to offline storage according to a set of business rules and schedule to be defined by EUTF. | 2 |  |  |
| T01.07 | Database | The database must be based on a Relational Database Management System (RDBMS). | 2 |  |  |
| T01.08 | Database | The database must be designed to allow for detailed Health Insurance and other supplemental benefits information to be stored and accessible by the System. This data will be provided by EUTF's third-party administrators. | 2 |  |  |
| T01.09 | Design | Validations in the System must be both at the field level and at the database level. | 2 |  |  |
| T01.10 | Design | Dates must be consistently formatted throughout the System. Dates in the System must allow for unambiguous selection of values that are completely visible in lists. | 2 |  |  |
| T01.11 | Design | Drop-down selection lists must have a logical ordering that makes the selection quick and easy. For example, dates must be listed in “date” order, not “alphabetical” order, where applicable. | 2 |  |  |
| T01.12 | Design | The System must provide the ability to modify help text. | 2 |  |  |
| T01.13 | Integration | The System must provide real-time integration (Application Program Interfaces - APIs), such as web services, in order to facilitate the integration with other internal and external Systems. | 2 |  |  |
| T01.14 | Integration | The System must support file exchange via Extensible Markup Language (XML), Comma Separated Value (CSV) files, fixed format, and JavaScript Object Notation (JSON) file formats. EUTF will be able to specify which language or file format should be used for each data exchange. | 2 |  |  |
| T01.15 | Portal | The System must provide access to participants using web browsers and must be Web Content Accessibility Guidelines (WCAG) 2.1 compliant. | 2 |  |  |
| T01.16 | Portal | Self Service Portal access via mobile devices must also be supported. The Self Service Portal must be mobile-friendly and employ the principals of Responsive Web Design (RWD). | 2 |  |  |
| T01.17 | Search | The System must have the ability to perform searches by key data elements. The System must have centralized searching capability including the ability to search by name, ID, SSN, employer, status, and other relevant criteria, as defined by EUTF. Any combination of criteria must be selectable and used to perform the search from a single screen. | 2 |  |  |
| T01.18 | Standards | Every browser-based component of the solution must be Section 508 compliant. | 2 |  |  |
| T01.19 | Standards | The System must support the latest stable release and supported versions of Microsoft Windows. | 2 |  |  |
| T01.20 | UI | The System must have the ability to modify menu descriptions, fields, labels, and text. | 2 |  |  |
| T01.21 | UI | The System must support up to three browsers as specified by EUTF (IE, Edge, Chrome, Safari, and Firefox). For each browser, the System must support all major versions released within 24 months of go-live and the most recent two major versions as a minimum. | 2 |  |  |

## T-02\_Auditing/Logging

| **ReqID** | **Sub-process** | **Requirement Details** | **Flexibility Rating** | **Degree of Customization** | **Comments** |
| --- | --- | --- | --- | --- | --- |
| T02.01 | Logs | The System must produce System logs. These System logs will differentiate between a) Error logs, b) Audit logs, and c) Activity Logs. Entries must be differentiated among one of these three categories. | 2 |  |  |
| T02.02 | Logs | The System must produce detailed and summary reports of all System logs. | 2 |  |  |
| T02.03 | Logs | System logs must be available to EUTF in a plain text format. | 2 |  |  |
| T02.05 | Logs | System log entries must contain the following information; a) a unique event ID and type, b) date and time stamp of the event, c) error message, d) success or failure of the event, e) IP address for the client, f) USER ID triggering the event, g) resources accessed, h) application interface used, and i) co-relation with audit trail entries. | 2 |  |  |
| T02.06 | Logs | System log file retention on the local servers must be configurable. | 2 |  |  |
| T02.07 | Logs | The System must provide System logs containing System information, process information, and user information. | 2 |  |  |
| T02.08 | Logs | The System must date/time stamp all System logs entries. | 2 |  |  |
| T02.09 | Logs | The System logs must record all access by users, especially privileged accounts (System administrators and power users). | 2 |  |  |
| T02.10 | Logs | The System logs must record all failed login attempts and lockouts. | 2 |  |  |
| T02.11 | Logs | The System logs must record all access to Personally Identifiable Information (PII). | 2 |  |  |
| T02.12 | Logs | The System logs must record all account logins and logouts. | 2 |  |  |
| T02.13 | Logs | The System logs must record all account logouts due to inactivity. | 2 |  |  |
| T02.14 | Logs | The System logs must identify users who attempt to access resources they are not authorized to access. | 2 |  |  |
| T02.15 | Logs | The System must use System logs for logging only and not for determining logic for product functionality. | 2 |  |  |
| T02.16 | Logs | The System must provide System logs that record what fields were modified, the old value, the new value, and User Ids or by which process the fields were modified. | 2 |  |  |
| T02.17 | Logs | The System must not base calculations and/or application logic on System log file entries. | 2 |  |  |
| T02.18 | Logs | The System must provide data auditing and standard administrative reports that allow EUTF staff to review System logs through report formats that are easy to use and read. The System must provide reports that must allow an administrator to troubleshoot errors or to trace back an activity within the System log entries. | 2 |  |  |
| T02.19 | Logs | The System must provide System logs that are secured (read-only) in such a manner that no System user (of any security level) can alter the records. Note: System Administrators may have the ability to access the tables to perform System maintenance. | 2 |  |  |
| T02.20 | Logs | The System must indicate in the System logs when a database was restored, backed-up, or refreshed. | 2 |  |  |
| T02.21 | Logs | System activity logging levels must be configurable to adjust the level of detail retained in the System logs. | 2 |  |  |
| T02.22 | Logs | The System must employ data compression or other efficiency methods on System logs in order to keep storage overhead to a minimum. | 2 |  |  |
| T02.23 | Logs | The System must maintain timestamp, user ID, process ID, and effective dates for all parameters. | 2 |  |  |
| T02.27 | Logs | The System must generate System log entries with meaningful descriptions; i.e., log file entries must have meaningful descriptions and must have explanations of specific error codes. | 2 |  |  |
| T02.28 | Logs | The System logs must record all additions and deletions of user accounts | 2 |  |  |
| T02.29 | Logs | The System logs must record all changes in security attributes (access-levels, logon interval, terminal logon restrictions and connection interface) | 2 |  |  |
| T02.30 | Logs | The System logs must record all user account suspensions and reactivations | 2 |  |  |
| T02.31 | Logs | The System logs must record all administrative password resets | 2 |  |  |
| T02.32 | Logs | The System logs must record all account lockout events (invalid password, inactive session, access from unallowed interfaces, logon attempts out of valid intervals and maximum concurrent session limit violations) | 2 |  |  |
| T02.33 | Logs | The System logs must record all password changes | 2 |  |  |
| T02.34 | Logs | The System logs must record all changes to application configuration settings | 2 |  |  |
| T02.35 | Logs | The System logs must record all changes to cryptographic keys | 2 |  |  |
| T02.36 | Logs | The System logs must record all start-ups/stops of application processes | 2 |  |  |
| T02.37 | Logs | The System logs must record all abnormal application exits | 2 |  |  |
| T02.38 | Logs | The System logs must record all failed database connection attempts | 2 |  |  |
| T02.39 | Logs | The System logs must record all attempts to modify critical registry keys | 2 |  |  |
| T02.40 | Logs | The System logs must record all logon/log-off for maintenance | 2 |  |  |
| T02.41 | Logs | The System logs must record all failed integrity checks for application data, executables and audit logs | 2 |  |  |
| T02.42 | Logs | The authentication credentials for the System logs must not be recorded in any System log. | 2 |  |  |
| T02.43 | Logs | The System must provide the ability for System logs to be retained for any period of time, as determined by EUTF. | 2 |  |  |
| T02.44 | Logs | The System must provide the ability for System logs to be archived periodically in accordance with EUTF archiving requirements. | 2 |  |  |

## T-03\_Configuration

| **ReqID** | **Sub-process** | **Requirement Details** | **Flexibility Rating** | **Degree of Customization** | **Comments** |
| --- | --- | --- | --- | --- | --- |
| T03.01 | Design | The System must provide for the key parameters to be driven by effective dates and specific ranges of time. These time-sensitive variances must be used within apply to all functionality, as well. For example, the date-driven variances must allow a calculation or value to be correct for the date range to which it applies. | 2 |  |  |
| T03.02 | Design | The System must provide the capability to add a new plan to the System and to modify an existing plan, from the System. | 2 |  |  |
| T03.03 | Design | The System must allow administrators to clone exiting plans to set up new plans. Rules for the new plan can then be added, deleted, or modified as required. | 2 |  |  |
| T03.04 | Design | The System must provide the capability to maintain pre-defined values, such as employer codes. The System should be table driven to the maximum extent possible. The tables are to be maintained by a single common application. | 2 |  |  |
| T03.05 | Rules | The System must provide EUTF-maintained, effective-date-driven values used in rules with configurable parameters. The System must include tools that are intuitive and easy to use for EUTF to modify these values and rules. Such rules cannot be dependent on hard-coded values. | 2 |  |  |
| T03.06 | Rules | The System must be configurable to handle plan changes, adjustment types, rate changes, rule changes, etc. | 2 |  |  |

## T-04\_Imaging/Workflow

| **ReqID** | **Sub-process** | **Requirement Details** | **Flexibility Rating** | **Degree of Customization** | **Comments** |
| --- | --- | --- | --- | --- | --- |
| T04.01 | Features | The System must provide for customizable dashboards for specific user roles to monitor work and work-in-progress. | 2 |  |  |
| T04.02 | Features | The System must provide an ability to use electronic rubberstamps. | 2 |  |  |
| T04.03 | Features | The System must provide the ability to add unlimited annotations to documents. | 2 |  |  |
| T04.04 | Features | The System must ensure all image format text-based documents are converted to OCR and are Encrypted | 2 |  |  |
| T04.05 | Features | The System must ensure all image format text-based documents are converted to OCR compatible format | 2 |  |  |
| T04.06 | Features | The system must provide the capability to identify documents that have an encoded document identifier such as a barcode printed on the document. | 2 |  |  |
| T04.07 | Features | The system must provide the capability to read and interpret a barcode located anywhere on a document. | 2 |  |  |
| T04.08 | Features | The system must provide the capability to read and interpret a barcode forward and/or backward. | 2 |  |  |
| T04.09 | Features | The system must provide the capability to read and interpret barcodes of varying sizes on documents. | 2 |  |  |
| T04.10 | Features | The system must provide the capability to interpret a barcode on documents and automatically index the document based on the values encoded in the barcode. | 2 |  |  |
| T04.11 | Features | The system must provide the capability for the user to view documents in the incoming folders prior to indexing and filing, although the documents may not yet be accessible from the BAS environment. | 2 |  |  |
| T04.12 | Features | The system must provide the capability to retrieve documents from the repository using document attributes and/or combinations of attributes as search criteria. | 2 |  |  |
| T04.13 | Features | The system must provide the capability for users to search on annotations, comments and redactions that are associated with a document, folder, or group of documents. | 2 |  |  |
| T04.14 | Features | The system must provide the capability for users to browse the stored documents based on their user access permissions. | 2 |  |  |
| T04.15 | Features | The system must provide the capability to search using any combination of record and/or folder metadata elements utilizing full text search. | 2 |  |  |
| T04.16 | Features | The system must provide the capability to specify partial matches and will allow designation of "wild card" fields or characters | 2 |  |  |
| T04.17 | Features | The system must open documents in the repository as view-only as the default. | 2 |  |  |
| T04.18 | Features | The system must provide the capability for the user to edit documents in the repository. | 2 |  |  |
| T04.19 | Features | The system must provide the capability for the user to save an edited document as a new version of the document. | 2 |  |  |
| T04.20 | Features | The system must allow for documents to be marked as “viewable” by the member or employer in the self-service applications. | 2 |  |  |
| T04.21 | Integration | The System must include an integrated electronic workflow System for EUTF defined business processes. | 2 |  |  |
| T04.22 | Integration | The System must provide the capability to define configurable rules for routing documents scanned into Enterprise Content Management (ECM) to appropriate users by document type. | 2 |  |  |
| T04.23 | Integration | The System must include scanning/imaging/ICR(OCR) capabilities that interact with the workflow System to trigger workflows and utilize proposed Imaging System repository of images. | 2 |  |  |
| T04.24 | Integration | The System must provide a means to trigger and process work outside of the proposed workflow System. | 2 |  |  |
| T04.25 | Integration | The System must seamlessly integrate with the existing ECM solution (Kofax) or an ECM solution proposed by the Offer and approved by EUTF. The System must offer single sign-on. | 2 |  |  |
| T04.26 | Integration | The System must provide the ability to pull up participant's documents from within the participant's record. | 2 |  |  |
| T04.27 | Integration | The System must provide the ability to have the fax, scan, or participant's web submission of a document trigger a workflow in the System. | 2 |  |  |
| T04.28 | Integration | The System must provide the ability to image documents and information from whatever source they initiate. For example, when a faxed document comes in, it should go directly to Imaging, based on parameters, so that it does not have to be printed and then imaged. | 2 |  |  |
| T04.29 | Integration | The System must provide the ability to provide an interface between the Self-Service Portal and Imaging to allow documents submitted by a user to be validated and then stored within the ECM solution. | 2 |  |  |
| T04.30 | Integration | The System must provide the ability for EUTF to control which documents stored in Imaging are to be displayed to a user through the Self-Service Portal. | 2 |  |  |
| T04.31 | Integration | The System must provide the ability to push System-generated letters or reports into ECM solution for storage. | 2 |  |  |
| T04.32 | Integration | The System must provide the ability to store a permanent record of System-generated communications and documents including index values and metadata in the ECM solution. | 2 |  |  |
| T04.33 | Integration | The System must provide the capability to have a workflow process triggered by scanning a document. | 2 |  |  |
| T04.34 | Integration | The System must provide the ability to initiate workflow processes both automatically (via the imaging of documents) and manually based on the receipt of a phone-call, walk-in, fax, e-mail, etc. They System must provide the ability to configure for any chosen document type. | 2 |  |  |
| T04.35 | Sizing | For purposes of completing Attachment 2, Offer Form OF-2, assume the following quality and complexity of workflows; 1) 10 High Complexity workflows and 2) 20 Medium Complexity workflows. | 2 |  |  |
| T04.36 | Workflow | The System must provide for a workflow activity log of all activity of tasks through the workflow, to include at a minimum: task id, task name, user assigned, date assigned, and date completed. The workflow activity log must be accessible through the System to let users view the history and review the activities on any given workflow. | 2 |  |  |
| T04.37 | Workflow | The workflow activity log must record which documents are used or processed at each workflow step. | 2 |  |  |
| T04.38 | Workflow | The workflow activity log must track the length of time tasks have been in the work queues. | 2 |  |  |
| T04.39 | Workflow | The System must provide deadline monitoring capabilities to trigger the start of a workflow task or the next step in a workflow. | 2 |  |  |
| T04.40 | Workflow | The System must provide the capability to define configurable rules to prioritize workflow tasks based on the type of document and/or other attributes of the task. | 2 |  |  |
| T04.41 | Workflow | The System must provide the capability to establish thresholds for review or approval. For example, approving refunds over a given level may require special approvals whereas amounts less than the threshold would not. | 2 |  |  |
| T04.42 | Workflow | The workflow queues must be unlimited in size. | 2 |  |  |
| T04.43 | Workflow | The System must provide the capability to configure workflow step status attributes (e.g. review, pending, complete, approve etc.). | 2 |  |  |
| T04.44 | Workflow | The System must provide the capability to start a workflow process manually. | 2 |  |  |
| T04.45 | Workflow | The System must provide the capability for a supervisor to reassign a workflow task. | 2 |  |  |
| T04.46 | Workflow | The System must provide the capability to manage workflow tasks using a combination of passive and active workflow models. Staff would select work from a common pool for some tasks (passive workflow), while with other tasks, staff would be assigned work directly (active workflow). | 2 |  |  |
| T04.47 | Workflow | The System must provide the capability to establish a timeline for each workflow including tasks such as when items are due, when reminders need to be sent, the frequency and number of additional reminders, and when internal escalations are required. | 2 |  |  |
| T04.48 | Workflow | The System must provide the capability to alert or notify EUTF users (through email, dashboard, or other means) of upcoming due dates and past due dates for both internal tasks and tasks to be completed by external parties. | 2 |  |  |
| T04.49 | Workflow | The System must provide the ability for users to link electronic documents (images, spreadsheets, etc.) to any workflow or contact record. | 2 |  |  |
| T04.50 | Workflow | The System must provide the ability to display the status (not-started, in-process, pending, completed, etc.) of all workflow processes. | 2 |  |  |
| T04.54 | Workflow | The System must provide the capability to send e-mail notifications to recipients other than System users, as well as recipients outside of EUTF. | 2 |  |  |
| T04.55 | Workflow | The System must provide the capability for communication to be triggered by business events, user requests, or scheduled times. | 2 |  |  |
| T04.56 | Workflow | The System must provide the capability to set up and maintain workflows and their associated sub-tasks based on the business processes defined by EUTF. | 2 |  |  |

## T-05\_Infrastructure

| **ReqID** | **Sub-process** | **Requirement Details** | **Flexibility Rating** | **Degree of Customization** | **Comments** |
| --- | --- | --- | --- | --- | --- |
| T05.01 | Data protection | The Offeror must implement and maintain appropriate administrative, technical, and organizational security measures to safeguard against unauthorized access, disclosure, or theft of all data within its control. Such security measures will be in accordance with recognized industry practice and not less stringent than the measures the Offeror applies to its own data of similar kind. | 2 |  |  |
| T05.02 | Data protection | At no time must any data or processes, which either belong to or are intended for the use of EUTF or its officers, agents, or employees, be copied, disclosed, or retained by the Offeror or any party related to the Offeror for subsequent use in any transaction that does not include EUTF. | 2 |  |  |
| T05.03 | Data protection | The Offeror must maintain and implement procedures to logically separate EUTF data from the Offeror’s data and the data belonging to the Offeror’s other customers. | 2 |  |  |
| T05.04 | Data protection | The Offeror must not store EUTF Data on any portable computing device including, but not limited to, personal data assistant (PDA), cell phone, smartphone, laptop (each a “Portable Computing Device”), unless EUTF Data stored on such Portable Computing Device is encrypted. | 2 |  |  |
| T05.05 | Data protection | The Offeror must not store EUTF Data on any removable media, such as compact disc, flash drive, tape (each a “Removable Media”), unless EUTF Data stored on such Removable Media is encrypted. | 2 |  |  |
| T05.06 | Data protection | The Offeror must ensure hard drive encryption consistent with validated cryptography standards as referenced in FIPS 140-2, Security Requirements for Cryptographic Modules for all Confidential Data, Restricted Data, and Personal Data, unless the Offeror presents a justifiable position approved by EUTF that data must be stored on an Offeror portable device in order to accomplish work as defined in the scope of work. | 2 |  |  |
| T05.07 | Data protection | EUTF must have the ability to import or export data in piecemeal or in entirety at its discretion without interference from the Offeror. This includes the ability for EUTF to import or export data to/from other service providers. | 2 |  |  |
| T05.08 | Data protection | The Offeror must contact EUTF upon receipt of any electronic discovery, litigation holds, discovery searches, or expert testimonies related to EUTF’s data under this contract, or which in any way might reasonably require access to the data of EUTF. The Offeror will not respond to subpoenas, service of process, or other legal requests related to EUTF without first notifying EUTF, unless prohibited by law from providing such notice. | 2 |  |  |
| T05.09 | Data protection | In the event of an early termination of the contract, the Offeror must allow for EUTF to retrieve its digital content and provide for the subsequent secure disposal of EUTF digital content. | 2 |  |  |
| T05.10 | Data protection | During any period of suspension, the Offeror must not take any action to intentionally erase any EUTF digital content. | 2 |  |  |
| T05.11 | Data protection | In the event of early termination of any services or agreement in entirety, the Offeror must not take any action to intentionally or unintentionally, erase any EUTF data until all data has been transferred to a new environment of EUTF’s choice. After the transition, the Offeror will have no obligation to maintain or provide any EUTF data and will thereafter, unless legally prohibited, delete all EUTF Data in its systems or otherwise in its possession or under its control. In the event of termination for cause, the Offeror will impose no fees for access and retrieval of digital content to EUTF. | 2 |  |  |
| T05.12 | Disaster Recovery | The System must provide full backups that must have the ability to be encrypted. The System must securely protect the backup data so that it cannot be accidentally or inappropriately accessed. | 2 |  |  |
| T05.13 | Disaster Recovery | The Offeror's Cloud Services must use, subject to EUTF's approval, multiple geographically distinct regions for disaster recovery and business continuity. | 2 |  |  |
| T05.14 | Disaster Recovery | The Offeror's Cloud Services must use, subject to EUTF's approval, multiple data sites and/or availability zones for System fault tolerance. | 2 |  |  |
| T05.15 | Disaster Recovery | The System must provide for a Recovery Time Objective of no greater than 24 hours | 2 |  |  |
| T05.16 | Disaster Recovery | The System must provide a Recovery Point Objective (Maximum time period of lost transactions, data changes, or work-in-process) of no greater than 8 hours | 2 |  |  |
| T05.17 | Environment | The System must provide multi-tiered, redundant environments that are physically or logically isolated and distinct from each other. | 2 |  |  |
| T05.18 | Environment | The Offeror must implement separate application and database environments in order to fulfill all of the requirements of this RFP. The Offeror must be responsible for replicating the application and data base in all environments (Production, Production (DR Instance), UAT, Test, and Development) including any additional configuration activities that may be necessary. | 2 |  |  |
| T05.19 | Environment | The Offeror must implement separate Application and database environments in order to fulfill all of the requirements of this RFP. The Offeror must be responsible for replicating the application and data base in all environments (Pre-Production, UAT and Training) including any additional configuration activities that may be necessary. | 2 |  |  |
| T05.20 | Environment | The System must allow developers to work independently from the rest of their project team, enabling them to make and validate changes without having to worry about adversely affecting the rest of their project team. These environments must need to have their own databases to enable regression testing, | 2 |  |  |
| T05.21 | Environment | The Pre-Production environment must completely match the production environment and also be physically separate from all other server components in EUTF's infrastructure. This environment must be used for load testing of major releases of and for implementation of emergency production fixes (which must subsequently be migrated into production and then merged with the other environments). | 2 |  |  |
| T05.22 | Environment | The Offeror must propose a methodology and tools for maintaining the multiple environments (including data refresh and migration capabilities) on an ongoing basis after project completion. All environments should be sized according to their usage. | 2 |  |  |
| T05.23 | Environment | The Offeror must not use production data in a test or development environment. | 2 |  |  |
| T05.24 | Interoperability | The System must work with EUTF’s infrastructure. | 2 |  |  |
| T05.25 | Logs | The Offeror must provide access to system logs which include usage statistics, user access data, user access IP address, user access history, and security information. | 2 |  |  |
| T05.26 | Policy | The Offeror must not undertake Network security auditing, testing and scanning of the System without prior approval by EUTF. | 2 |  |  |
| T05.27 | Policy | The Offeror must not conduct, nor allow to be conducted, a network attack or penetration test of the System by any internal or external party without the explicit approval of EUTF. | 2 |  |  |
| T05.28 | Policy | EUTF will be allowed to scan for vulnerabilities against systems in which EUTF has the primary responsibility for system and data confidentiality, integrity, and availability. | 2 |  |  |
| T05.29 | Policy | The Offeror will allow EUTF, or its representative, to conduct forensic investigations for both criminal and non-criminal purposes. The Offeror must ensure that there is no interference with the investigation and will ensure the integrity of the data is maintained throughout the investigation. | 2 |  |  |
| T05.30 | Policy | Upon EUTF’s request, the Offeror must promptly provide EUTF with such assistance and information as is required by EUTF in order to comply with any legal obligations to preserve or collect EUTF data or information concerning EUTF’s use of the Offeror's Cloud Services or to respond to or otherwise address any inquiry, access request, complaint, enforcement notice, claim, or similar action raised in relation to or made by any or all subjects of EUTF data. | 2 |  |  |

## T-06\_Installation & Config

| **ReqID** | **Sub-process** | **Requirement Details** | **Flexibility Rating** | **Degree of Customization** | **Comments** |
| --- | --- | --- | --- | --- | --- |
| T06.01 | Documentation | The Offeror must affix a EUTF Asset Management tag to all hardware delivered to EUTF and adhere to all processes regarding EUTF asset tracking. | 2 |  |  |
| T06.02 | Documentation | The Offeror must propose and establish a Project Documentation Repository, subject to EUTF’s approval, as a common repository for Project documentation and to facilitate communication to Project participants as to Project status, activities, Work Products, Milestones, accomplishments, etc. | 2 |  |  |
| T06.03 | Documentation | The Offeror must develop an IT Operations Manual, which features clear organization of content, easy to understand language, useful graphic presentations, and a thorough index and glossary. The IT Operations Manual will provide EUTF staff the knowledge to efficiently operate and update the System independent of Offeror assistance. The IT Operations Manual will address the view of the System required by technical users. It will provide an understanding of the Application, database design and file structures, relationships between programs, security, troubleshooting, special constraints, procedures for data recovery, and other operational guidelines. | 2 |  |  |
| T06.04 | Documentation | The Offeror must develop a Business User Manual that features clear organization of content, easy to understand language, useful graphic presentations, and a thorough index and glossary. The Business User Manual will be used by the EUTF Acceptance Test team to mirror the production environment and verify manual content. | 2 |  |  |
| T06.05 | Documentation | In conjunction with the Business User Manual, a Quick Reference Business User Document must be produced by the Offeror that will be an immediate aid to the user and quickly describe operations. | 2 |  |  |
| T06.06 | Documentation | The Offeror must will develop a Business Procedure Manual which features clear organization of content, easy to understand language, useful graphic presentations, and a thorough index and glossary. The Business Procedure Manual will document instructions for manual operations and tasks that are performed in direct conjunction with the automated system. It will address each task performed in a step by step procedure that identifies the action (task to be performed) and the individual with responsibility to complete the action. | 2 |  |  |

## T-07\_Interfaces/Integration

| **ReqID** | **Sub-process** | **Requirement Details** | **Flexibility Rating** | **Degree of Customization** | **Comments** |
| --- | --- | --- | --- | --- | --- |
| T07.01 | Compliance | The System must comply with HIPAA requirements for enrollment transactions when appropriate. | 2 |  |  |
| T07.02 | Compliance | The System must comply with NACHA requirements for electronic payments when appropriate. | 2 |  |  |
| T07.03 | Compliance | Health insurance data exchanged with health plans and pharmacy benefit managers must comply with HIPAA standards that mandate the use of ANSI X.12 820, 834, and 999 transaction formats at the most recent standard revision levels. | 2 |  |  |
| T07.04 | Compliance | The System must create insurance enrollment change files utilizing HIPAA mandated ANSI-834 and ANSI-820 file formats. | 2 |  |  |
| T07.05 | Compliance | The System must accept files from third-party administrators in HIPAA-mandated ANSI-834, ANSI-820 and ANSI-999 formats. | 2 |  |  |
| T07.06 | Configuration | If a phased deployment is undertaken, all necessary data back bridges, back feeds, and interim interfaces between the EUTF legacy systems and the new System during the Phase deployment of the new System will be the responsibility of the Offeror. | 2 |  |  |
| T07.07 | Configuration | The System must make use of the existing interfaces without modification to either the interface or the interfaced System. The exception is those interfaces which are finalized during a design session, based on mutual agreement by EUTF and Offeror. | 2 |  |  |
| T07.08 | Configuration | The System must include an easily-configurable mechanism for adding new input/output file formats and transmission channels. | 2 |  |  |
| T07.10 | Integration | The System must integrate with a EUTF approved 3rd party address validation provider. | 2 |  |  |
| T07.11 | Integration | The System must integrate with a EUTF approved 3rd party death notification/validation provider. | 2 |  |  |
| T07.12 | Integration | The System must integrate with a service provider as chosen by EUTF to accept online E-Check/credit card payments. | 2 |  |  |
| T07.13 | Integration | The System must integrate with MS Query using ODBC (or a bridgeable configuration such as JDBC, OLE DB, .NET) for data analysis. | 2 |  |  |
| T07.14 | Integration | The System must integrate with the existing e-mail system. | 2 |  |  |
| T07.16 | Integration | The System must, for the Self-Service Portal, provide the capability to re-direct to a EUTF approved 3rd party payment gateway. | 2 |  |  |
| T07.17 | Interfaces | The System must accept and create interface files in proprietary file layouts | 2 |  |  |
| T07.18 | Interfaces | The System must accept and create interface files in txt, CSV and Excel file formats | 2 |  |  |
| T07.19 | Interfaces | The System must accept and create interface files as full files and as changes only files. | 2 |  |  |
| T07.20 | Interfaces | The System must create a file of all tax withholdings to be transmitted to the federal IRS and State DOR. | 2 |  |  |
| T07.21 | Interfaces | The System must create a file containing 1099 data in a proprietary format to be transmitted to the print shop. | 2 |  |  |
| T07.22 | Interfaces | The System must create a file or files in a format to be approved by EUTF in order to back bridge data during any interphase period during the implementation. | 2 |  |  |
| T07.23 | Interfaces | The System must provide for the capability to roll-back or restart from the abort point of partially completed or aborted interface load/extract. | 2 |  |  |
| T07.24 | Performance | The system must provide capability to import and process transmittal files live in production, without affecting access to other system functionality. | 2 |  |  |
| T07.25 | Portal | The System must provide remote access to Imaging for EUTF approved 3rd parties. | 2 |  |  |
| T07.26 | Portal | The system must provide the ability for employers to upload their transmittal files directly to the EUTF system via an Employer Web Portal. | 2 |  |  |
| T07.27 | Portal | The system must provide the ability for employers to manually input transmittal information directly into the EUTF system through an Employer Web Portal. | 2 |  |  |
| T07.29 | Sizing | For purposes of completing Attachment 2, Offer Form OF-2, assume the following quality and complexity of interfaces; 1) 45 High Complexity interfaces and 2) 90 Medium Complexity interfaces. | 2 |  |  |

## T-08\_Operational Requirements

| **ReqID** | **Sub-process** | **Requirement Details** | **Flexibility Rating** | **Degree of Customization** | **Comments** |
| --- | --- | --- | --- | --- | --- |
| T08.01 | Batch processing | Any required batch jobs must provide for the ability to be scheduled and run to completion without any user intervention. | 2 |  |  |
| T08.02 | Batch processing | The System must provide the ability for scheduling batch jobs using a EUTF approved batch scheduling software. | 2 |  |  |
| T08.03 | Batch processing | The System must be capable of executing some batch processes during normal business operations without affecting operations. | 2 |  |  |
| T08.04 | Batch processing | The System must provide for the ability to limit the running of batch jobs during predetermined hours of the day. | 2 |  |  |
| T08.05 | Batch processing | The System must provide for the capability to roll-back or restart from the abort point of partially completed or aborted batch jobs. | 2 |  |  |
| T08.06 | Batch processing | All batch jobs must have a finite run-time of no more than two (2) hours, except as otherwise approved by EUTF. | 2 |  |  |
| T08.08 | Disaster Recovery | The Offeror must provide content for inclusion in EUTF's comprehensive Disaster Recovery/Business Continuity plan. | 2 |  |  |
| T08.09 | Disaster Recovery | The Offeror must perform an annual recovery test in conjunction with EUTF to ensure the EUTF Disaster Recovery plan is viable (the first such test will take place during the warranty period following System Acceptance). | 2 |  |  |
| T08.11 | Integration | The Offeror must track problems from the time reported or discovered to closure using a tracking tool approved by EUTF and will report their statuses upon request. EUTF currently uses Jira. | 2 |  |  |
| T08.12 | Output management | The System must allow for print jobs to be limited by page size. | 2 |  |  |
| T08.13 | Output management | The System must allow for print output to be viewed online. | 2 |  |  |
| T08.14 | Output management | Output destinations for the print job must be configurable by end users and by EUTF operations staff using Windows Desktop Print Services. | 2 |  |  |
| T08.15 | Output management | The System must allow for Magnetic Ink Character Recognition (MICR) check writing capability. | 2 |  |  |
|  |  |  |  |  |  |
| T08.17 | Performance | Response time requirements (including the Self-Service Portal) must be met independent of how many users are online, how many web-based users are online, and independent of what processes or scripts are being run, such as wage and contribution edits, wage and contribution posting, interest posting, payroll, etc. | 2 |  |  |
| T08.18 | Performance | The System must provide full functionality without concurrent processing impeding any aspect of the enterprise’s operations of the day-to-day business. | 2 |  |  |
| T08.19 | Policy | All system, services, or networks must reflect Hawaii Standard Time. | 2 |  |  |
| T08.20 | Policy | The Offeror must provide a risk assessment prior to implementing all new or significantly changed production software, hardware, or network devices. | 2 |  |  |
| T08.21 | Policy | The Offeror must provide a contingency plan prior to implementing all new or significantly changed production software, hardware, or network devices. | 2 |  |  |
| T08.22 | Sizing | The System design, sizing, configuration, and implementation must support all workloads, including special daily, weekly, quarterly, and annual processing, and be able to support 10% per annum growth with no performance impact for five (5) years post warranty end at no added financial burden to EUTF. | 2 |  |  |
| T08.23 | Sizing | The System must at a minimum be capable of supporting one hundred (100) Line of Business user accounts without adverse impact to system performance. | 2 |  |  |
| T08.24 | Sizing | The System must at a minimum be capable of supporting seven hundred and fifty (750) employer user accounts. | 2 |  |  |
| T08.25 | Sizing | The System must at a minimum be capable of supporting one hundred and fifty thousand (150,000) participant user accounts. | 2 |  |  |
| T08.26 | Sizing | The System must at a minimum be capable of supporting one hundred (100) third-party user accounts. | 2 |  |  |
| T08.27 | Sizing | The System must be capable of supporting a 10% growth per annum in user accounts and concurrent user sessions with no performance impact for five (5) years post warranty end at no added financial burden to EUTF. | 2 |  |  |
| T08.28 | Sizing | The System must at a minimum be capable of supporting one hundred (100) concurrent Line of Business user session. | 2 |  |  |
| T08.29 | Sizing | The System must at a minimum be capable of supporting two hundred (200) concurrent employer user accounts. | 2 |  |  |
| T08.30 | Sizing | The System must at a minimum be capable of supporting one thousand (1,000) concurrent participant user accounts. | 2 |  |  |
| T08.31 | Sizing | The System must at a minimum be capable of supporting forty-five (45) concurrent third-party user accounts. | 2 |  |  |
| T08.32 | Workload scheduling | Batch jobs must be able to be started, restarted, and terminated using an EUTF approved batch scheduling/management tool. | 2 |  |  |
| T08.33 | Workload scheduling | The System must clearly indicate at a System level and to the EUTF batch scheduling software tool the status of all batch jobs. | 2 |  |  |
| T08.34 | Workload scheduling | The System must include tools capable of automatically initiating jobs based on time of day, the day of the week, calendar day, and/or successful completion of preceding events. | 2 |  |  |

## T-09\_Reports

| **ReqID** | **Sub-process** | **Requirement Details** | **Flexibility Rating** | **Degree of Customization** | **Comments** |
| --- | --- | --- | --- | --- | --- |
| T09.01 | Development | The System must provide two basic types of reports: pre-developed (canned) reports and an ad hoc querying/reporting tool for end users. | 2 |  |  |
| T09.02 | Development | The System must support the use of Microsoft Word or other tool as approved by the EUTF for the creation of forms, letters, and e-communications. | 2 |  |  |
| T09.03 | Development | The System must provide the ability for the EUTF to create, save, and re-use queries and reports. | 2 |  |  |
| T09.04 | Development | The System must be able to produce output in PDF format. | 2 |  |  |
| T09.05 | Development | The System must provide the capability to perform ad-hoc reporting and query functionality, including the ability for the EUTF to define roles and security levels for the ad-hoc reporting such that only data the user is allowed to access can be accessed. | 2 |  |  |
| T09.06 | Development | The System must provide the capability to perform ad-hoc reporting and query functionality, including the ability to save queries as personal or public (available to other users within defined roles). | 2 |  |  |
| T09.07 | Development | The System must provide the capability to perform ad-hoc reporting and query functionality, including the ability for the EUTF to set validations or limits on queries such that System performance is not affected. | 2 |  |  |
| T09.08 | Development | The System must provide the capability to perform ad-hoc reporting and query functionality, including the ability export into other documentation formats (e.g., CSV, JSON, XML). | 2 |  |  |
| T09.09 | Development | The System must provide the capability to perform ad-hoc reporting and query functionality, including the ability to easily extract reports and queries to MS Excel. | 2 |  |  |
| T09.10 | Development | Reports must be of professional appearance: they must be paginated, with a header, footer, report title, a brief narrative of the report reason, total counts, UserID, date, and time. | 2 |  |  |
| T09.11 | Development | All reports must contain data classification metadata such as Confidential, Internal, External, Public etc. The data classification must be printed on the report. | 2 |  |  |
| T09.12 | Development | The data classification metadata must be includable in reports, forms, letters, and e-communications. | 2 |  |  |
| T09.13 | Development | The data classification metadata must be capable of being queried. | 2 |  |  |
| T09.14 | Policy | Reports must not contain a person’s full SSN unless otherwise approved by the EUTF. | 2 |  |  |
| T09.15 | Policy | The reporting tool must provide for the ability to mask fields, such as SSN. | 2 |  |  |
| T09.16 | Sizing | For purposes of completing Attachment 2, Offer Form OF-2, assume the following quality and complexity of reports, forms, letters and e-communications; 1) 250 High Complexity reports & queries, 2) 500 Medium Complexity reports & queries, 3) 100 High Complexity forms, letters & e-communications and 4) 150 Medium Complexity forms, letters & e-communications. | 2 |  |  |

## T-10\_Security

| **ReqID** | **Sub-process** | **Requirement Details** | **Flexibility Rating** | **Degree of Customization** | **Comments** |
| --- | --- | --- | --- | --- | --- |
| T10.01 | Access | The System must restrict user access to data through multiple and alternate methods (Roles/Permission Matrix). For example, running a query, report, or a search for the restricted data on the front-end, user interface, or integrated reporting solution. | 2 |  |  |
| T10.02 | Access | The System must support the principle of “least privilege” when granting access to processes or resources. | 2 |  |  |
| T10.03 | Access | The System must provide the ability to define and assign access security based on roles within the System. The opportunity to perform these actions must be restricted to privileged accounts (Administrative groups). | 2 |  |  |
| T10.04 | Access | The System must provide functionality to create/modify user groups, roles, permission, users, and access privileges. | 2 |  |  |
| T10.05 | Access | The System must provide the ability to require the time of day access control. | 2 |  |  |
| T10.06 | Access | The System must provide the granularity of access control at the screen, field, data value, report, and process level. | 2 |  |  |
| T10.07 | Access | The System must allow functionality to be determined by role, such that a user may be limited in their ability to perform certain functions, access certain screens, view certain participant data, and certain groups of participants such as EUTF's employees (as well as other limitations) based on their role. | 2 |  |  |
| T10.08 | Access | The Offeror must establish a formal process, covering personnel and third parties, to ensure that the access rights of terminated individuals are promptly disabled and removed. Offeror personnel tasked with managing access controls must promptly change access rights to reflect the termination, maintain a record regularly review that such changes have been appropriately made. | 2 |  |  |
| T10.09 | Access | The Offeror must ensure that the System is configured such that it does not permit unauthorized access to itself or State networks. | 2 |  |  |
| T10.10 | Access | The System must not be configured such that it permits anonymous access to the System, except to the extent that such access is required for an authorized purpose. (e.g., FTPS services or general public web pages or other general public accessible service). | 2 |  |  |
| T10.11 | Configuration | The Offeror must fully configure the security, access points, and roles in the System in conjunction with the EUTF staff before delivery. | 2 |  |  |
| T10.12 | Data protection | PII and nonpublic data must be encrypted at rest and in transit with controlled access. | 2 |  |  |
| T10.13 | Data protection | The Offeror must ensure that production data is not used in testing and development environments. | 2 |  |  |
| T10.14 | Data protection | The System must provide for all emails outbound to external domains, containing PII, EPHI, PCI DSS or CJIS information must be encrypted. | 2 |  |  |
| T10.15 | Interoperability | The System must have Microsoft EUTF Active Directory integration and must support a password policy as defined by the EUTF. | 2 |  |  |
| T10.16 | Interoperability | The System must use the State IP scheme. | 2 |  |  |
| T10.17 | Policy | The Offeror must ensure that all personnel, contractors, vendors, partners, visitors, and others with access or potential access to State information and information assets receive appropriate information security training and/or awareness and are provided with information security awareness materials on a regular basis. This includes regular security training requirements as defined by legal or regulatory requirements (e.g., HIPAA, CJIS, PCI DSS, and IRS). | 2 |  |  |
| T10.18 | Policy | All security testing must be done in a secure environment that is not connected to the production network and must not be performed on production systems. | 2 |  |  |
| T10.19 | Policy | The Offeror must access and test for vulnerabilities as defined on following websites: 1) SANS top 20 internet security methods of protection. http://www.sans.org/top20/ and 2) Open Web Application Security Project (OWASP) top 10 internet security methods of protection. http://www.owasp.org/index.php/Top 10 2007 | 2 |  |  |
| T10.20 | Policy | The Offeror must not attach a device, computer system, or network to State networks without explicit authorization from the EUTF. | 2 |  |  |
| T10.21 | Policy | The Offeror must ensure that the System is configured such that it does not provide network services or permit network connections that are not required for a business purpose. | 2 |  |  |
| T10.22 | Policy | The System must not use Network Address Translation (NAT) or Port Address Translation (PAT). | 2 |  |  |
| T10.23 | Policy | The Offeror must ensure that production systems are physically segregated from development environments through the use of firewalls. | 2 |  |  |
| T10.24 | Policy | The Offeror must ensure that appropriate security features, including preventing the display of sensitive information to unauthorized individuals, are included in the System. | 2 |  |  |
| T10.25 | Policy | The Offeror must ensure that the source code of the System is safeguarded and access to such source code is limited to only personnel with a legitimate business requirement. | 2 |  |  |
| T10.26 | Policy | The Offeror must ensure that personnel responsible for implementing or developing the System receive training, at least annually, with respect to security and coding best practices. | 2 |  |  |
| T10.27 | Policy | The System may not use local password protecting or pre-encrypting of content or attachments. | 2 |  |  |
| T10.28 | Policy | The System will adhere 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 | 2 |  |  |
| T10.29 | Portal | The System must provide a Self-Service Portal that must include access to security features via secure sign-on with a username/password. | 2 |  |  |
| T10.30 | Portal | The System must have the capacity for the Self-Service Portal to mask any field, such as Social Security Numbers. | 2 |  |  |
| T10.31 | Portal | The System must, for the Self-Service Portal, provide authentication techniques to ensure the participant requesting sign-on credentials is, in fact, an EUTF participant. Authentication techniques must include SSN, zip code, a series of security questions, mandatory two-factor authentication, or combinations of these. | 2 |  |  |
| T10.32 | Portal | The System must, for Self-Service Portal, provide the capability for the participant to create his/her own username and password. | 2 |  |  |
| T10.33 | Portal | The System must, for Self-Service Portal, provide the capability for bulk creation of participant usernames and initial login passwords. | 2 |  |  |
| T10.34 | Portal | The System must, for the Self-Service Portal, reset the counter for unsuccessful sign-on attempts to zero upon a successful login. | 2 |  |  |
| T10.35 | Portal | The System must, for the Self-Service Portal, provide the capability for the participant to recover a forgotten username. Recovery of a username must require that the user is authenticated again. | 2 |  |  |
| T10.36 | Portal | The System must, for the Self-Service Portal, provide the capability for the participant to reset forgotten passwords. | 2 |  |  |
| T10.37 | Portal | The System must, for the Self-Service Portal provide the capability for the participant to change the password at any time once signed-on successfully. | 2 |  |  |
| T10.38 | Portal | The System must, for the Self-Service Portal, dynamically employ role-based security schemes based upon business data to control access to information. For example, active participants, benefit recipients, employers, business representatives, etc. | 2 |  |  |
| T10.39 | Portal | The System must, for the Self-Service Portal, provide EUTF system administration personnel with role-based capabilities to maintain the Portal. Such privileged tasks include locking participants out of the Portal, resetting Portal passwords for participants, creating username/password on behalf of a participant (one-time password), and other tasks normally delegated to System administrators and help desk roles. | 2 |  |  |
| T10.40 | Portal | The System must, for the Self-Service Portal, provide secure/encrypted transmission of all data on the Portal, including authentication and sign-on credentials. | 2 |  |  |
| T10.41 | Portal | The System must, for the Self-Service Portal, provide the capability to require users to change their password based on EUTF-determined frequency. | 2 |  |  |
| T10.42 | Portal | The System must, for the Self-Service Portal, display the date and time of the last login by the user. | 2 |  |  |
| T10.43 | Portal | The System, prior to access to any PHI, will display an EUTF-approved configurable warning or login banner (e.g., "The System should only be accessed by authorized users"). In the event that a System does not support pre-login capabilities, the System will display the banner immediately following authorization. | 2 |  |  |
| T10.44 | Portal | The system will have the capability to provide employer user access to the portal at the employer and employer sub-group level (if needed). | 2 |  |  |
| T10.45 | Portal | The system will, for the Self-Service Portal, provide capabilities to authenticate a user who has called EUTF for technical support. The EUTF support personnel may need to have access to the user’s authentication tools (security questions, image keys, etc.) within the portal in order to authenticate a caller. | 2 |  |  |
| T10.46 | Sign-on | As required by the EUTF, the solution must support multifactor authentication for all users and administrators. | 2 |  |  |
| T10.47 | Sign-on | The System must support Password length of 10 characters minimum. | 2 |  |  |
| T10.48 | Sign-on | The System must support password complexity requirements enabled to include one upper case letter, lower case letter, number, and non-alphabetic character. | 2 |  |  |
| T10.49 | Sign-on | The System must not allow for the UserID to be any part of a user's password | 2 |  |  |
| T10.50 | Sign-on | The System must support minimum password age X days (users cannot reset their passwords more frequently than X days) where X is defined by the EUTF. | 2 |  |  |
| T10.51 | Sign-on | The System must support maximum password age of 90 days (must require users to reset their passwords after a maximum of 90 days). | 2 |  |  |
| T10.52 | Sign-on | Password history of normal business operations passwords remembered (must require users to use a password that is different from their last 20 passwords). | 2 |  |  |
| T10.53 | Sign-on | Passwords cannot be identical to the username. | 2 |  |  |
| T10.54 | Sign-on | The System must have the ability to modify the parameters above based on future policy changes. Detailed requirements must be provided during requirements validation phase of the project. | 2 |  |  |
| T10.55 | Sign-on | The System must support the creation of local user/IDs, independent of Active Directory, within the System; for example, System accounts, test accounts, and disaster recovery. | 2 |  |  |
| T10.56 | Sign-on | The System must support Account lockout after an EUTF specified number of failed attempts. | 2 |  |  |
| T10.57 | Sign-on | The System must support limiting the number of concurrent sessions for each user login. | 2 |  |  |
| T10.58 | Sign-on | The System must support automatic account reset after the lockout with the following parameters; 30 minutes after first failure/lockout (or as defined by the EUTF), 60 minutes after second failure/lockout (or as defined by the EUTF), and no reset after third failure/lockout. | 2 |  |  |
| T10.59 | Sign-on | The System must be configurable to limit session connection time, as determined by the EUTF. | 2 |  |  |
| T10.60 | Sign-on | The Offeror must ensure that Offeror personnel remote access is restricted to only pre-approved individuals, and that such access is permitted only using an approved VPN device. | 2 |  |  |
| T10.61 | Sign-on | The Offeror must not configure devices for dial-up (e.g., modem) access to State networks or systems without EUTF approval. | 2 |  |  |
| T10.62 | Sign-on | The Offeror must ensure that any remote access solution used by the Offeror to access the System for support or maintenance purposes is configured to have the least access necessary, and their access is in compliance with State policies, statutes, regulations, and standards; including, if applicable, two-factor authentication for remote network access. | 2 |  |  |
| T10.63 | Sign-on | When re-setting a password, the System must be able to prohibit re-set passwords that not incrementally different from the previous password (e.g., Rj24\*Jan, Rj24\*Feb, and Rj24\*Mar). | 2 |  |  |
| T10.64 | Sign-on | The System must not insert passwords into electronic messages or included in information transmitted by an electronic messaging system; the only exception is when the message is protected by a State approved method or the password is a one-time use password. | 2 |  |  |
| T10.65 | Sign-on | The Offeror must immediately report any known or suspected compromise of a password to the EUTF. | 2 |  |  |
| T10.66 | Sign-on | The System must be configured to store passwords only when required and only in encrypted form. | 2 |  |  |
| T10.67 | Sign-on | The Offeror must ensure that passwords for service accounts are not provided to individuals without a legitimate requirement, are disabled when not in use, and are changed whenever there is a change in Offeror personnel. | 2 |  |  |
| T10.68 | Sign-on | The Offeror must ensure that a mechanism is in place for each system, network, and application account with system-level privileges that allows the actions of an administrator to be uniquely associated with that individual. | 2 |  |  |
| T10.69 | Sign-on | The Offeror must not assign the same password to accounts with system-level privileges as is used for non-administrator accounts. | 2 |  |  |
| T10.70 | Sign-on | The Offeror must ensure that vendor supplied default passwords for systems or applications are changed before the systems or applications are used for EUTF purposes. | 2 |  |  |
| T10.72 | Standards | The System must ensure that TLS certificates and data encryption are applied to all external components. | 2 |  |  |
| T10.73 | Standards | The System must support a variety of open, industry-accepted crypto-graphical standards, such as Advanced Encryption Standard (AES). Data Encryption Standard (DES), Triple DES (3DES), RC4, or any other weak ciphers must not be used. Preferably, options to use these ciphers should not exist by default. | 2 |  |  |
| T10.74 | Standards | The System must provide industry-standard security for the display of Personally Identifiable Information (PII) for electronically submitted documents. | 2 |  |  |
| T10.75 | Standards | The Offeror must ensure transactions with bank cards or other financial account data or information meet or exceed the Payment Card Industry Data Security Standard (PCI DSS). | 2 |  |  |
| T10.76 | Standards | The System must, at a minimum, provide a mechanism to comply with security requirements and safeguard requirements of the following Federal agencies / entities:  a. Health & Human Services Centers for Medicare & Medicaid Services (CMS) b. NIST 800-53 r4 and NIST Moderate high  Baseline r4 c. IRS pub 1075, which points back to NIST 800-53 rev 4 d. Federal Information Security Management Act (FISMA) of 2002 e. HIPAA f. Health Information Technology for Economic and Clinical Health Act of 2009 g. Privacy Act of 1974 h. e-Government Act of 2002 i. Patient Protection and Affordable Care Act of 2010, Section 1561 Recommendations | 2 |  |  |
| T10.77 | TLS | The solution must be designed to allow TLS offloading to decrypt external user connections to allow inspection of traffic. | 2 |  |  |
| T10.78 | Validation | Any validation done in client-side scripts must be replicated on the server-side. | 2 |  |  |

## T-11\_Self Service

| **ReqID** | **Sub-process** | **Requirement Details** | **Flexibility Rating** | **Degree of Customization** | **Comments** |
| --- | --- | --- | --- | --- | --- |
| T11.01 | Design | The System must provide a Self-Service capability to participants, employers, TPA, and other stakeholders as defined in the functional requirements. | 2 |  |  |
| T11.02 | Documentation | The System must provide the ability for users to submit supporting documentation through the portal as different formats. | 2 |  |  |
| T11.03 | Integration | The System must provide the capability to integrate with the BAS. The System must integrate Self Service Portal functionality seamlessly with the other components of the System, including ECM. | 2 |  |  |
| T11.04 | Integration | The System must be capable of integrating with ECM such that documents uploaded through the Portal by participants are properly indexed and placed in the participant's file in ECM. | 2 |  |  |
| T11.05 | Integration | The System must permit the user securely message EUTF directly through the Self-Service Portal. | 2 |  |  |
| T11.06 | Integration | The System must provide the capability of the Self-Service Portal to link to EUTF's existing public website. | 2 |  |  |
| T11.07 | Integration | The System must integrate with the Self-Service Portal so that all information and services presented on the Self-Service Portal are consistent with the information and services in the BAS. | 2 |  |  |
| T11.08 | Knowledge Management | The System must provide the capability to include and manage changes to a Knowledge Management Repository (e.g. frequently asked questions, standard problems, responses, and a glossary of terminology used by EUTF). | 2 |  |  |
| T11.09 | Policy | The System must require that a new user agrees to the terms of an End User Agreement before the user can create a username/password to the Portal. | 2 |  |  |
| T11.10 | Policy | The System must provide the capability for EUTF to require periodic and/or forced re-acceptance of the End User Agreement. | 2 |  |  |
| T11.11 | Policy | The Self-Service Portal must have the capability identify employers who have a BAA on file. | 2 |  |  |
| T11.12 | Policy | The Self-Service Portal must have the capability identify carriers who have a BAA on file. | 2 |  |  |
| T11.13 | Policy | The Self-Service Portal must have the capability to restrict employer user sharing and viewing of information to employers who do not have a current BAA on file. | 2 |  |  |
| T11.14 | Policy | The Self-Service Portal must have the capability to restrict carrier user sharing and viewing of information to carriers who do not have a current BAA on file. | 2 |  |  |
| T11.17 | Support | The System must provide capabilities to authenticate a user who has called the EUTF for technical support. The support personnel may need to have access to the participant's authentication tools (e.g., security questions, image keys) within the Portal in order to authenticate a caller. | 2 |  |  |
| T11.18 | Support | The System must provide the capability for the contact center to view the status of the participant's self-service account, such as date account was created, date account was last accessed, and whether the account is locked out. | 2 |  |  |
| T11.19 | UI | All functionality exposed to participants through the Self-Service Portal must have a consistent look and feel and must conform to the EUTF style standards and branding. | 2 |  |  |
| T11.20 | UI | The System must encode all HTML pages in HTML 5. | 2 |  |  |
| T11.21 | UI | The Self-Service Portal must not require the use of add-ons, plug-ins, or 3rd party tools. | 2 |  |  |
| T11.22 | UI | The portal links must be uniquely labeled, such that any two links with the same label should take the user to the same web page. | 2 |  |  |
| T11.23 | UI | The System must provide the capability to perform validations and provide an on-screen context-sensitive error, warning, and help messages where applicable. | 2 |  |  |
| T11.24 | UI | The System must provide the capability to navigate through screens based on standard browser-based navigation. | 2 |  |  |
| T11.25 | UI | The Self-Service Web Portal must support the top five (5) browsers (IE, Edge, Chrome, Safari, and Firefox). For each browser, the System must support all major versions released within 24 months of go-live and the most recent two (2) major versions as a minimum. | 2 |  |  |

# OPTIONAL REQUIREMENTS

OFFEROR must confirm if they can or cannot meet each requirement within their fixed price proposal. If the requirement can be met at additional cost, OFFEROR should select “Additional” and include details in the Summary tab of Appendix D, *Cost Proposal Workbook*.

|  |  |  |
| --- | --- | --- |
| **Flexibility Rating** | **Definition** | **Comments** |
| **Rating 3** | **Optional** – Desired if requirement can be met without additional cost | EUTF would like this requirement fulfilled, but understands it might be outside the scope of the vendor’s BAS solution. For each Rating 3 requirement:   * Indicate “Yes” if the function will be delivered as part of the fixed price. * Indicate “No” if the function will not be delivered as part of the fixed price proposal. * Indicate “Additional” if the function can be delivered at added cost and provide detail in the Summary tab of Appendix D, *Cost Proposal Workbook*. |

| **ReqID** | **Process** | **Sub-process** | **Requirement Details** | **Flexibility Rating** | **Meets Requirement?** | **Comments** |
| --- | --- | --- | --- | --- | --- | --- |
| T01.03 | Application Architecture | Data | The System must allow the EUTF to run data projections on the various populations within the System. For example, using the data retrieved for a scheduled report or ad hoc report, the System must determine trends in the data and project those trends into the future given an expiration or end date as defined by the user. | 3 | Yes No  Additional |  |
| T02.04 | Auditing/Logging | Logs | System logs must be available to the EUTF for analysis in real time. | 3 | Yes No  Additional |  |
| T02.24 | Auditing/Logging | Logs | The System must include tools that will record performance information and provide performance trend analysis and reporting. | 3 | Yes No  Additional |  |
| T02.25 | Auditing/Logging | Logs | The System must provide for real-time notification if performance thresholds are exceeded. | 3 | Yes No  Additional |  |
| T02.26 | Auditing/Logging | Logs | The System must provide for real-time notification if a logging system malfunctions or is shut down. | 3 | Yes No  Additional |  |
| T04.51 | Imaging/Workflow | Workflow | The System must provide the capability to send a transaction to a reviewer for audit or verification. | 3 | Yes No  Additional |  |
| T04.52 | Imaging/Workflow | Workflow | The System must provide the capability to organize workflows based on major work processes, such as meetings (Board, Counseling) estimate requests, terminations, refunds, retirements, or deaths. | 3 | Yes No  Additional |  |
| T04.53 | Imaging/Workflow | Workflow | The System must provide a graphical flow diagram in order to visually see the configuration of any workflow. | 3 | Yes No  Additional |  |
| T05.27 | Infrastructure | Environment | The System must provide an automated tool to maintain the multiple environments. | 3 | Yes No  Additional |  |
| T06.11 | Installation & Config | Integration | The Offeror must use an automated configuration management tool that is EUTF approved. | 3 | Yes No  Additional |  |
| T06.12 | Installation & Config | Integration | The Offeror must use an automated software testing tool proposed by the Offeror and approved in writing by the EUTF. This tool will be easily integrated and allow for traceability throughout the execution of all program logic to the requirements. | 3 | Yes No  Additional |  |
| T06.13 | Installation & Config | Integration | The Offeror must use and instruct the EUTF in the use of an EUTF-approved automated test tracking tool that tracks and facilitates management of issues, problems, and discrepancies found during testing or retesting, resolution of these issues, and progress towards User Acceptance Testing completion. | 3 | Yes No  Additional |  |
| T07.09 | Interfaces/Integration | Configuration | The System must provide for the ability to limit the size of email attachments. | 3 | Yes No  Additional |  |
| T07.15 | Interfaces/Integration | Integration | The System must provide the ability for scheduling file creating/processing using an EUTF-approved scheduling software. | 3 | Yes No  Additional |  |
| T07.28 | Interfaces/Integration | Portal | The system must integrate with the Axway file transfer system for employer file transfer | 3 | Yes No  Additional |  |
| T08.07 | Operational Requirements | Batch processing | The Offeror must use an EUTF-approved automated tool for job scheduling. | 3 | Yes No  Additional |  |
| T08.10 | Operational Requirements | Integration | The Offeror must use an automated tracking tool approved by the EUTF to track all reported problems and issues, including the current status and approvals, and for tracking other open Project issues that are not classified as software Defects. The EUTF currently uses Jira. | 3 | Yes No  Additional |  |
| T09.14 | Reports | Integration | The System must allow users the ability to push reports to the ECM solution for archival. | 3 | Yes No  Additional |  |
| T10.71 | Security | Sign-on | The System must have the capability to auto-generate web portal user accounts and default passwords per the EUTF business rules. | 3 | Yes No  Additional |  |
| T11.15 | Self Service | Policy | The Self-Service Portal must have the capability to notify the employer when the BAA is about to expire. | 3 | Yes No  Additional |  |
| T11.16 | Self Service | Policy | The Self-Service Portal must have the capability to notify the carrier when the BAA is about to expire. | 3 | Yes No  Additional |  |
| T11.26 | Self Service | Workflow | The System must, for changes made by users of the Self-Service Web Portal, have the capability to send change confirmation notification to the user based on a participant’s communication preferences (electronic or paper mail) at the EUTF's option. | 3 | Yes No  Additional |  |