

Instructions for responding to Requirements Workbooks:

These requirements have been formatted into workbooks as a more efficient and effective way not only for a vendor to respond; but for KHPA to evaluate as well.

The workbooks have been compiled by category. Within each category subsections have been broken down into worksheets and placed into tabs that have been labeled accordingly.

Within the worksheets notice that after the "Requirement" column the columns proceed as followed: "Requirement for Phase 1, Response, Explanation of Response and Response Reference."

The purpose of each column is defined below.

- Implementation Phase - Respond with a 1, 2 or 3 to indicate the anticipated phase of implementation (A detailed description of the three phases can be found in the RFP.)
- Response - is the column where the proposer will respond to whether or not the requirement is met and to what extent. (Detailed instructions below.)
- Explanation of Response - Please provide an Explanation of how the requirement is or isn't met and validate the (0-5) rating given in the "Response" column.
- Response Reference - Please indicate where, throughout your response proposal, this is described in detail.

Proposer Fit Rating Response Codes: In the "Response" column please provide a Yes or No indicating whether or not the requirement is met. In addition to Yes or No, include a number rating indicating to what level the proposed solution meets the requirement. (Example of Response – Yes/3)

Fit Rating 5: Solution meets the requirement without any customization or configuration to implement.

Fit Rating 3: Solution mostly meets the requirement, but will require minor customization or configuration to implement.

Fit Rating 1: Solution somewhat meets the requirement, but will require significant customization or configuration to implement.

Fit Rating 0: Solution does not meet the requirement at all, and cannot do so through customization.

(Rating system and brief explanation can be found at the top of each worksheet as a reference tool.)

Please note that some requirements have been highlighted. These requirements have been deemed optional and KHPA requests pricing be cost out separately for the indicated requirements. Please Respond to these under the "Optional Costs" in the Separate Cost Proposal.

Proposer Fit Rating Response Codes: In the "Response" column please provide a Yes or No indicating whether or not the requirement is met. In addition to Yes or No, include a number rating indicating to what level the proposed solution meets the requirement. (Example of Response - Yes/3)

Fit Rating 5: Solution meets the requirement without any customization or configuration to implement.

Fit Rating 3: Solution mostly meets the requirement, but will require minor customization or configuration to implement.

Fit Rating 1: Solution somewhat meets the requirement, but will require significant customization or configuration to implement.

Fit Rating 0: Solution does not meet the requirement at all, and cannot do so through customization.

Function: Security (SECU) - This module provides requirements to ensure adequate system controls are in place to protect data from unauthorized view and use.

Req #	Requirement	Implementation Phase	Response	Explanation to Response	Response Reference
SECU-001	The system must require standard Internet security, including secure socket layers (SSL3/TLS) and secure hypertext transfer protocol (HTTPS).				
SECU-002	System must utilize an industry standard solution for customer authentication and password control/authentication.				
SECU-003	Access requirements through firewalls must be clearly identified and must follow standard port designations.				
SECU-004	Must outline their development process and explain how it complies with the SDC (Secure System Development LifeCycle).				
SECU-005	Must further outline how their SDC complies with process avoids the SANS/CWE TOP-25 dangerous programming errors for web applications and the OWASP TOP 10 Web Application Risks.				
SECU-006	Prior to system production phase, 'go live', Contractor must have a third party entity perform a penetration test and a separate vulnerability assessment, provide KHPA with all results, jointly review any security vulnerabilities & provide recommendations to address/remediate findings prior to production installation. KHPA will coordinate and schedule deadlines for fixes to be implemented by vendor.				
SECU-007	Third party selected for security reviews must be approved by KHPA prior to engagement.				
SECU-008	Regularly scheduled audits of the system must be performed post-installation, and vendor must review the findings and remediate as part of vendor on-going warranty & maintenance support.				
SECU-009	Third party applications must adhere to any applicable KHPA system security practices, configurations & procedures.				

SECU-010	Must have ability to create, delete, modify and assign role-based security to grant view and modify access to individual window, report, data element & field levels.				
SECU-011	System must generate unique log-on IDs for all accounts.				
SECU-012	User ID's must not use identifying information like SSNs, Beneficiary IDs, etc. Must be unique to this system. Login name may incorporate a user's name, or may be an ID randomly generated by the system.				
SECU-013	Online portal accounts must be granted access to system/beneficiary data separate from login creation process.				
SECU-014	Failed login messages must be generic and not indicate the status or validity of the account.				
SECU-015	Must have ability to configure a series of challenge questions at user's first login.				
SECU-016	Must have online self-service password capability (password reset using a series of security questions).				
SECU-017	Vendor's system password reset procedures must be subject to KHPA approval.				
SECU-018	Password change procedure must include on-screen helpful hints for password selection.				
SECU-019	Must have ability to automatically suspend user ID after a defined number of unsuccessful logon attempts.				
SECU-020	Must have ability to automatically deactivate a user ID after a defined period of inactivity.				
SECU-021	Must have ability for authorized personnel to manually deactivate a user ID on a temporary basis.				
SECU-022	Must have ability for authorized personnel to manually deactivate a user ID permanently so that it can not be made valid again.				
SECU-023	Must comply with KHPA password security policy requirements.				
SECU-024	Must automatically require user password changes after a defined period of time.				
SECU-025	Must have ability for authorized personnel to force user to change password upon next login.				
SECU-026	Must have ability to send system generated email notification of password change events and expiration warnings in compliance with KHPA password security policy requirements.				
SECU-027	System must log & audit user actions including login events, record access & record modification.				

SECU-028	Must provide audit capabilities for queries and reporting.				
SECU-029	Must comply with application NIST security standards. http://csrc.nist.gov/				
SECU-030	Must comply with applicable federal and state rules and requirements (e.g. HIPAA, ARRA/Hi-TECH, etc.)				
SECU-031	Must have ability to restrict access to data and reports for specific user profiles.				
SECU-032	Administrative interfaces, including but not limited to user administration, role administration & audit interfaces, must not be accessible from the public internet.				
SECU-033	User login habits (e.g. location, times, etc.) must be audited and access restricted when anomalies are detected.				
SECU-034	Must have a single log-on for users with access to multiple modules. (e.g. Application module, Eligibility module, interfaces, etc.)				
SECU-035	Must allow access and role changes to be made in real-time.				
SECU-036	Must support either a hierarchical role structure whereby user and password define program or individual menu item access or logon program/device security based strictly on user and password or PIN. (e.g. supervisor, clerical, worker, consumer, advocate, provider, etc.)				
SECU-037	The system must not permit the alteration of any security log audit trail.				
SECU-038	The system must provide notification, user lockout and audit trail entry, after a set number of unsuccessful login attempts.				
SECU-039	Must provide tools, such as alerts or reports, which identify users who may have misused the system. (e.g. staff inquiry on family members, creating fake cases, etc.)				
SECU-040	System must provide notification and user-lock when a user hasn't accessed the system for a set period of days.				
SECU-041	Must provide ad hoc reporting capabilities on the security system.				
SECU-042	Must provide complete history of access and use by individual user.				
SECU-043	Must use a naming convention defined by KHPA for creating usernames.				
SECU-044	Must perform any recoveries when necessary. (e.g. system failure, etc.)				
SECU-045	Must comply with the State ITEC Policies found at: http://www.da.ks.gov/kito/itec/ITPoliciesMain.htm				

SECU-046	The system must maintain the state of the browser session without cookies.				
SECU-047	K-MED must meet all federal, state, and agency audit and compliance requirements (e.g. the system will also be subject to a federally mandated SAS 70 (Statement on Auditing Standards No. 70))				

Proposer Fit Rating Response Codes: In the "Response" column please provide a Yes or No indicating whether or not the requirement is met. In addition to Yes or No, include a number rating indicating to what level the proposed solution meets the requirement. (Example of Response - Yes/3)

Fit Rating 5: Solution meets the requirement without any customization or configuration to implement.

Fit Rating 3: Solution mostly meets the requirement, but will require minor customization or configuration to implement.

Fit Rating 1: Solution somewhat meets the requirement, but will require significant customization or configuration to implement.

Fit Rating 0: Solution does not meet the requirement at all, and cannot do so through customization.

Function: Security Profile Management (SEPR) - The solution must provide system wide security with access management and role management capabilities. It must support profile creation, maintenance and definitions.

Req #	Requirement	Implementation Phase	Response	Explanation to Response	Response Reference
SEPR-001	Must support a flexible business model which accommodates multiple roles, for example some offices use a single worker/case management model and the Clearinghouse operates a task-based model.				
SEPR-002	The Eligibility module must provide the ability to create, delete, modify and assign role-based security profiles quickly as KHPA business processes change.				
SEPR-003	The solution must include flexible profile-building which will allow the ability to define profiles at multiple levels (e.g. by screen, by field, by case, etc.), and by function (ability to view, update, authorize, activate, inactivate, etc.). For example, a profile to allow a user to update all fields, but does not allow the user to authorize coverage for a Medicaid case may be created.				
SEPR-004	Must provide customer/member access to their own information with security at an individual level.				
SEPR-005	Must provide a medical representative view so individuals can access information and act on behalf of another customer/member.				
SEPR-006	Must provide a facilitator view with read-only access to individuals helping others with a medical assistance application.				
SEPR-007	Must provide, at a minimum, the following profiles with the ability to easily add unlimited number of profiles:				
SEPR-007.1	Eligibility Worker - with the ability to limit by location, specific job function and medical programs				
SEPR-007.2	Clerical or support staff				
SEPR-007.3	Regional/Management Region Managers				

SEPR-007.4	Quality Assurance staff				
SEPR-007.5	Regional/Management Region Performance Improvement staff				
SEPR-007.6	Program/Policy/Rules Engine Managers - Administrative profile to allow internal staff to update rules tables and other elements necessary to support policy and process changes				
SEPR-007.7	Interface/Exchange Managers				
SEPR-007.8	Presumptive Eligibility Staff				
SEPR-007.9	Presumptive Eligibility Support Staff				
SEPR-007.10	System Administrator				
SEPR-007.11	Password Administrator				
SEPR-007.12	System Access Administrator				
SEPR-008	Must provide community partner views with access for approved external entities and allow viewing of protected information and interaction with other users for all cases with proper identification and authentication (e.g. nursing homes, facilitators, foster care contractors, etc.). These special profiles will allow the partner to view all appropriate case information with a single log on.				
SEPR-009	Must provide an administrative profile to allow internal staff to view a customer or community partner profile exactly as the customer or community partner is viewing it.				
SEPR-010	Must provide a profile to allow select staff to manually override an eligibility determination.				
SEPR-011	Must provide necessary profiles to support the pilot phase of the application system.				
SEPR-012	Maintain user security and profile management, including adding, deleting and changing individual access and creating, deleting or modifying new profiles.				
SEPR-013	Must provide a tool to allow for profile creation, modification and maintenance. The tool must document details of all profiles (e.g. screens the user can access with that profile, fields that can be updated, etc) and provide versioning control.				

Proposer Fit Rating Response Codes: In the "Response" column please provide a Yes or No indicating whether or not the requirement is met. In addition to Yes or No, include a number rating indicating to what level the proposed solution meets the requirement. (Example of Response - Yes/3)

Fit Rating 5: Solution meets the requirement without any customization or configuration to implement.

Fit Rating 3: Solution mostly meets the requirement, but will require minor customization or configuration to implement.

Fit Rating 1: Solution somewhat meets the requirement, but will require significant customization or configuration to implement.

Fit Rating 0: Solution does not meet the requirement at all, and cannot do so through customization.

Function: Audit Trail (AUDT) - This module covers requirements to ensure detailed transaction history is captured, stored and easily retrievable. This includes information changed or updated as well as queries or view-only access.

Req #	Requirement	Implementation Phase	Response	Explanation to Response	Response Reference
AUDT-001	Must automatically maintain a separate Audit Trail file for all transactions processed by the system.				
AUDT-002	Must automatically maintain a separate Audit Trail file for all transactions caused by a user.				
AUDT-003	Must automatically maintain a separate Audit Trail file of users who pass through or view a record, regardless of whether data is changed.				
AUDT-004	The Audit Trail file must contain transaction history at the field level.				
AUDT-005	The System must not permit the alteration of any data on the Audit Trail.				
AUDT-006	The System must recognize a Contractor Audit Trail Administrator to administer the Audit Log.				
AUDT-007	Must be able to log/audit based on user ID and IP address.				
AUDT-008	Must support debug system error auditing for system troubleshooting.				
AUDT-009	Must have security audit trail reporting capabilities for a variety of criteria. (e.g. security, level, locale, IP address, user ID, what was modified and what to, etc.)				
AUDT-010	Ability to create an audit trail for "back door" database changes.				
AUDT-011	The Audit Trail record must contain information such as, but not limited to:				
AUDT-011.1	Case identifier.				
AUDT-011.2	Recipient identifier.				
AUDT-011.3	User/system action performing the action.				
AUDT-011.4	Location of the user performing the action.				
AUDT-011.5	Date the action was performed.				
AUDT-011.6	Time the action was performed.				

AUDT-011.7	Name of the field being processed.				
AUDT-011.8	Field value before processing.				
AUDT-011.9	Field value after processing.				
AUDT-011.10	Imaging document access that includes document type, user ID, date and time range, access by workstation / location.				
AUDT-012	The Audit Trail user must have the ability to:				
AUDT-012.1	View, via on-line processes, the contents of the Audit Trail permitted by the Audit Trail Administrator.				
AUDT-012.2	Determine the viewing criteria. (e.g. list Audit Trail records created during a specific period of time, etc.)				
AUDT-012.3	Determine the sort sequence for viewing the selected Audit Trail records. Sorting by any Audit Trail shall be available.				
AUDT-013	The Administrator responsibilities must include:				
AUDT-013.1	Maintaining a set of Audit Trail users having access to the Audit Trail.				
AUDT-013.2	Define the data allowable for viewing by individual Audit Trail users. (e.g. disallow access to certain fields containing financial or personal health information (PHI) for certain users, etc.)				
AUDT-013.3	Perform all activities permitted to any Audit Trail user.				
AUDT-013.4	Archive any portion of the Audit Trail onto an archival file.				
AUDT-013.5	Restore any archival data to the Audit Trail.				
AUDT-013.6	Back-up, restore and/or refresh the Audit Trail.				
AUDT-013.7	Shut-down or Start-up the Audit Trail.				
AUDT-013.8	Generate Audit Trail reports.				
AUDT-013.9	Generate limited ad-hoc reports. (e.g. limited by size, record count, etc.)				
AUDT-014	Must be able to create a history of all user and automated actions, including which user or process made the update, what information was changed down to the field level, the date and time of the change, where the change was made (IP address), the information prior to the change, information after the change, etc.				