

RFP NO. 20260801

REQUIREMENT SPECIFICATION

Table of Contents

1.0	INTRODUCTION	3
2.0	BACKGROUND	4
3.0	SCOPE OF WORK	5
4.0	FUNCTIONAL REQUIREMENTS	7
4.1	FUNCTIONAL REQUIREMENTS (Applicable to Contract & Policy Registries)	7
4.2	CONTRACT REGISTRY – FUNCTIONAL SPECIFICATION	11
4.3	POLICY REGISTRY – FUNCTIONAL SPECIFICATION	13
4.4	SYSTEM ADMINISTRATION & USER ADMINISTRATION	14
5.0	TECHNICAL REQUIREMENTS	16
5.1	BROWSER AND DEVICE COMPATIBILITY	16
5.2	TWO-FACTOR AUTHENTICATION (2FA)	16
5.3	SINGLE-SIGN ON (SSO)	16
5.4	SYSTEM & APPLICATION ARCHITECTURE	16
5.5	BACKUP & RESTORATION	16
5.6	SERVICE RELIABILITY	17
5.7	AUDIT REQUIREMENTS	17
5.8	DATA PROTECTION TRUSTMARK CERTIFICATION	17
5.9	INTELLECTUAL PROPERTY AND OWNERSHIP	17
5.10	INFORMATION ON THIRTY PARTY SECURITY EVALUATION	18
	Annex A – Cost Schedule	19
	Annex B – Service Level Agreement	20
	Annex C – NKF Statistics	22
	Annex D – Thirty Party Security Evaluation	24
	Annex E – Evaluation of the Vendor Solution	28
	Annex F – Resume of Vendor's Personnel	30
	Annex G – Statement of Compliance	31

REQUIREMENT SPECIFICATIONS

1.0	INTRODUCTION
1.1	The National Kidney Foundation Singapore (hereinafter referred to as “NKFS”) invites qualified vendors to propose and deliver one or both of the following digital registry solutions: a) Contract Registry System; and/or b) Policy Registry System. NKFS reserves the right to award the contract(s) in whole or in part, including appointing separate vendors for each system.
1.2	The Contract Registry System shall serve as a centralised digital platform to store, manage, and track contracts across their full lifecycle. Acting as a single source of truth, it will provide NKFS with complete visibility and control over all contractual agreements, including procurement contracts, service agreements, leases, and other legal documents. This system will support regulatory compliance, mitigate operational risks, and enhance decision-making by providing timely insights into contract obligations, renewal dates, milestones, and key terms.
1.3	The Policy Registry System shall function as a central repository for all NKFS internal governance documents, including policies, procedures, and Work Instructions (WI). It will ensure effective document management through version control, approval governance, and accessibility, enabling staff to consistently reference the most current and approved information.
1.4	The proposed Contract Registry System and Policy Registry System should preferably be delivered using a market-proven, cloud-based Software-as-a-Service (SaaS) platform, provided and fully managed by the Vendor, specialising in Contract Lifecycle Management (CLM) and/or Policy / Document Governance. The solution shall be vendor-hosted and vendor-operated, leveraging the Vendor’s native SaaS capabilities rather than NKFS internal application platforms. Custom development shall be minimised, and the solution shall primarily utilise out-of-the-box functionalities with configuration¹. The proposed solution must: a) Meet or exceed the functional, technical, security, and compliance requirements set out in this document; b) Support integration with NKFS enterprise systems, including identity (SSO), email, and collaboration platforms where required; c) Demonstrate proven deployment in organisations of comparable scale and complexity; d) Provide full transparency in subscription licensing, implementation, and support costs; and e) Avoid reliance on customer-built or internally managed applications. The solution must also support governance, auditability, and security requirements, including appropriate access controls, audit logging, and traceability of system activities.

¹ **Configuration** refers to out-of-the-box settings, admin screens, workflows, metadata, templates

REQUIREMENT SPECIFICATIONS

	The Vendor shall clearly specify all SaaS subscriptions, licences, and services included in the proposed solution. All licensing assumptions shall reference <u>Annex C – NKF Statistics</u> .
2.0	BACKGROUND
2.1	Currently, NKFS manages contract and policy tracking through largely manual and decentralised processes. Communication and coordination are primarily conducted via email, often requiring multiple back-and-forth exchanges to obtain approvals, clarify terms, or confirm updates. This manual approach results in operational inefficiencies, delays in processing, and increases the risk of miscommunication. It also limits transparency, traceability, and timely monitoring of contract and policy-related activities.
2.2	In the absence of a centralised system for storing and managing contract and policy documentation, multiple versions of the same document are frequently stored across various internal locations, including shared drives, email threads, and individual staff devices. This fragmented storage approach creates challenges in maintaining version control, document integrity, and audit trails. It significantly increases the risk of users referencing outdated or incorrect information and weakens governance, compliance, and accountability over critical documents.
2.3	NKFS currently lacks a centralised and integrated system to effectively manage contracts and internal governance documents across their respective lifecycles. The reliance on manual processes, decentralised storage, and email-based coordination has resulted in limited visibility, fragmented information, and reduced operational efficiency. These challenges have led to key control and governance gaps, including: a) Inadequate visibility and tracking of contract obligations, key dates, and policy updates; b) Weak version control and the absence of a single source of truth for critical documents; c) Limited auditability and traceability of user actions, approvals, and document changes; d) Increased risk of non-compliance due to inconsistent document management practices; and e) Operational inefficiencies arising from manual coordination and duplicated efforts. As a result, NKFS is exposed to operational, compliance, and governance risks, and is constrained in its ability to effectively monitor, manage, and enforce contractual and policy-related obligations. To address these challenges, there is a need to implement a centralised, system-driven solution that provides structured workflows, controlled access, comprehensive audit trails, and real-time visibility over contracts and policies. This will strengthen governance, improve operational efficiency, and support NKFS's compliance and risk management objectives.

REQUIREMENT SPECIFICATIONS

3.0	SCOPE OF WORK
3.1	The scope of this document is to subscribe to, configure, implement, and support a vendor-provided, SaaS-based Contract Registry and Policy Registry solution. a. Implementation & Onboarding The Vendor shall: i. Configure the SaaS platform to support NKF workflows, metadata, approval rules, and security roles, with minimal customisation; ii. Perform data migration from existing sources, where applicable; iii. Configure standard integrations supported by the SaaS platform (e.g. identity federation, email notifications, e-signature); and iv. Deliver user onboarding and administrator training. b. SaaS Subscription & Support Services The Vendor shall: i. Provide subscription access to the SaaS platform; ii. Provide vendor-managed application operations, monitoring, updates, and patches; and iii. Provide functional support, incident management, and defect resolution. c. Environments The Vendor shall: i. Provide two (2) environments: 1) UAT/Test for pre-production validation before migrating to Production and 2) Production; ii. Ensure NKF is not required to provision, host, or manage application environments. d. Change & Enhancement Services i. Enhancements shall be delivered through SaaS configuration and/or the Vendor's standard product roadmap; ii. Any unavoidable custom development must be explicitly identified, justified, and costed separately. iii. Refer to Annex B – Service Level Agreement.
3.2	<u>Optional Services</u> a. Extended Maintenance and Support The Vendor shall provide optional application maintenance and support services for an additional two (2) years (i.e. Years 3 and 4), following completion of the Base Services maintenance period. This shall include: i. Ongoing incident management and defect resolution; ii. Support for enhancements, configuration changes, and performance optimisation; iii. Continued compatibility with updates to NKF's enterprise platforms (e.g. Microsoft ecosystem). b. Additional Enhancement Services The Vendor shall provide enhancement services through Change Requests (CRs) and Service Requests (SRs) to support future functional,

REQUIREMENT SPECIFICATIONS

	technical, workflow, reporting, and integration requirements. Refer to <u>Annex B – Service Level Agreement</u>. All enhancements shall be subject to NKF's approval, prioritisation, and governance processes.
3.3	<u>Vendor Demonstration & Evaluation</u> a) Shortlisted vendors shall be invited to deliver a presentation demonstrating the proposed solution's features, integration capabilities, and user experience. b) Within one (1) week of the presentation, a two (2)-hour briefing session shall be conducted to commence a three (3)-week trial period at no additional cost. Refer to <u>Annex E – Evaluation of the Vendor Solution</u>. c) The Vendor shall provide a minimum three (3)-week trial period with full access to core functionalities for evaluation by up to ten (10) internal stakeholders.
3.4	<u>Proposal Submission Requirements</u> a) All deliverables and associated costs must be itemised in accordance with <u>Annex A – Cost Schedule</u>. b) Vendors must clearly indicate all mandatory and optional items. Failure to comply may result in disqualification.
3.5	<u>Pricing and Contract Terms</u> a) Base services shall be delivered at a fixed charge to NKFS; b) NKFS will not reimburse any cost overruns beyond the agreed estimate; c) The Vendor shall propose a standard man-day rate for additional services (CR/SR), clearly indicated in <u>Annex A – Cost Schedule</u>.
3.6	<u>Project Team and % of Solution Customisation</u> a) Vendors shall provide CVs of proposed personnel (<u>Annex F</u>); b) Vendors must indicate the percentage of customisation required (in the compliance table) and associated cost implications (in <u>Annex A – Cost Schedule</u>).
3.7	The Vendor shall: a) Provide full pricing details in <u>Annex A</u>. b) Complete <u>Annex D – Thirty Party Security Evaluation</u>; c) Submit <u>Annex F – Resume of Vendor's Personnel</u>; d) Complete <u>Annex G – Statement of Compliance</u>; Incomplete or non-compliant submissions may result in disqualification.

REQUIREMENT SPECIFICATIONS

4.0	FUNCTIONAL REQUIREMENTS
4.1	FUNCTIONAL REQUIREMENTS (Applicable to Contract & Policy Registries)
4.1.1	The solution shall be delivered as a vendor-managed SaaS application, comprising: a) Identity & Access: Federated authentication with NKF's identity provider (e.g. SAML 2.0 / OpenID Connect); b) Application Layer: Vendor's native SaaS web application; c) Workflow Engine: Built-in SaaS workflow and approval capabilities; d) Repository: Vendor-managed secure document repository; e) Notifications: Native SaaS email and collaboration notifications; and f) Search: Vendor-provided metadata-based and full-text search capabilities. The solution shall not require NKF to deploy, operate, or maintain any application platforms, low-code tools, or automation services.
4.1.2	Modular Design The solution shall be modular, comprising: a) ^[**4] Contract Registry (CRY) and Policy Registry (PRY) registries. b) ^[**5] Functionality to regularly export the latest registries (exclude records pending approval) for deposit into each registry's NKF Internal SharePoint². c) Shared services: Security, audit, reporting, migration, retention, notifications. ^[**4] Registries are restricted to designated users by RBAC, while Read Only repositories are open to more users and can be integrated easily. ^[**5] Searching and processing records must remain within either CRY or PRY, to ensure that records are not transferred or managed between CRY and PRY.
4.1.3	Identity Integration & Role Management The solution should preferably support integration with NKF's identity provider (Microsoft Entra ID / Azure AD) to enable synchronisation of users, groups, and role assignments. In the event that native integration is not supported, the solution must allow administrators to configure and manage users, roles, and action parties (refer to clause 4.1.4) directly within the system through out-of-the-box configuration (without requiring custom development). All role assignments, changes, and user activities shall be auditable.
4.1.4	Action Parties a) Support Role-Based Access Control (RBAC) with multi-level permissions; b) Support configurable routing matrices³⁴ (e.g. approval based on value, risk category, department); c) All role assignments and changes shall be auditable. Roles shall include (non-exhaustive): Requestor, Endorser, Approver, Legal, Procurement, Finance, Compliance, Policy Owner, Publisher, Registry Owner, System Administrator.

² Where out-of-the-box **SharePoint** integration is not supported and customisation is required, the Vendor shall provide an export function to enable the publisher to manually import the final version into Microsoft SharePoint.

³ A **contract management** approval workflow ensures that all contracts undergo structured review and authorisation before execution. It defines the sequence of approvals, from contract drafting through legal, purchasing, finance, and functional unit validation, to final sign-off.

⁴ An internal **policy** manual approval workflow governs the review and endorsement of new or updated policies before publication. It typically involves subject matter experts, compliance, corporate, and senior management to validate accuracy, regulatory alignment, and organisational relevance. This structured approach ensures policies are current, authoritative, and formally endorsed for adoption.

REQUIREMENT SPECIFICATIONS

4.1.5	Unique Reference Numbers a) The system shall auto-generate unique reference numbers upon request creation: i. Suggested format: ▪ Contracts: C-[FY][DeptCode]-[AutoSeq] (e.g., C-25FIN-0123) ▪ Policies: P-[FY][DeptCode]-[AutoSeq] (e.g., P-25OPS-0045) If a vendor uses a different format, it shall be able to identify whether it is a contract, policy, or indicate the contract year. ii. Fit criteria: Uniqueness guaranteed; prefix clearly differentiates Contract vs PM/WI records. Format: ○ FY (2 digits) – ‘25’ for FY2526, ‘26’ for FY2627, ○ DeptCode (3 Alphanumeric characters) ○ AutoSeq – running number starts with 1 and padded with ‘0’ for 4 or less digits.
4.1.6	Document Access & Management a) The system shall support ‘SharePoint’-based document⁵ access through all workflow stages. b) The system shall allow attachments (supporting common formats: PDF, DOCX, XLSX, image files). c) The system shall maintain full versioning for all documents and store signed versions alongside their records. d) Version numbering shall be system-controlled and immutable once approved. e) The system shall apply metadata tagging to documents (linked to CR/PR records) for search and retrieval. f) Mandatory metadata fields shall be enforced at submission and approval stages.
4.1.7	Bulk Upload & Data Migration The Vendor shall provide native SaaS data migration utilities, supporting: a) Pre-upload validation and preview; b) Field mapping and document association; c) Audit logs and migration reports; and d) Post-migration reconciliation support.
4.1.8	Search, Reporting & Analytics The solution shall provide native SaaS reporting and dashboards suitable for operational and management use. NKF is using Power BI for analytics.
4.1.9	Notifications, Reminders & Escalations a) The system shall send email/Teams notifications at key stages (submission, endorsement, approval, signing, publishing). b) The system shall support configurable reminders (relative to contract/policy dates and task SLAs). c) The system shall support escalations to alternates/managers after configurable thresholds (e.g., n business days overdue).
4.1.10	Delegation & Coverage a) The system shall allow users to set out-of-office delegations, including date ranges and alternates. b) Delegated users shall receive routed tasks during the coverage period, with full audit logging.

⁵ Documents are centrally managed and accessed via a ‘SharePoint’ like solution across all workflow stages

REQUIREMENT SPECIFICATIONS

4.1.11	Audit Trail a) The system shall maintain a comprehensive audit trail: - Every action has a timestamp, actor, action type, and data changes. - Covers submissions, reviews, approvals, rejections, signatures, publications, edits, and archival.
4.1.12	Security & Compliance The SaaS solution shall implement: a) Encryption of data at rest and in transit; b) Role-based and attribute-based access controls; c) Secure tenant isolation; and d) Compliance with NKF data protection, confidentiality, and audit requirements.
4.1.13	Data Retention & Purging a) The system shall enforce retention schedules per registry owner's policy. b) The system shall auto-purge/archive records based on configured rules and approvals. c) Purge actions shall be logged and are reversible for a configurable grace period (optional).
4.1.14	Non-Functional Requirements a) Availability target: $\geq 99.9\%$. b) Performance: Typical form load $\leq 3s$; search results $\leq 5s$ for standard queries. c) Scalability: Support growth of records/documents without degradation. d) Accessibility: WCAG-compliant UI (where feasible). e) Localisation: English baseline; extensible for multilingual metadata if needed.
4.1.15	The solution may provide a vendor-embedded AI-assisted or advanced search capability , subject to NKF approval, which: a) Operates entirely within the SaaS platform; b) Respects NKF access controls; c) Provides explainable results with source references; and d) Maintains audit logs of AI-assisted interactions.
4.1.16	Document Ingestion & Indexing a) Ingest, and index documents from multiple sources and formats. b) Extract text, tables, and key metadata to support accurate retrieval.
4.1.17	Unified Semantic & Keyword Search a) Provide a single search experience combining keyword, Boolean, and natural-language semantic search. b) Allow users to search across all authorized contracts, policies, and metadata fields.
4.1.18	Contextual Answer Generation a) Generate concise, grounded answers based strictly on retrieved documents. b) Provide citations and highlighted snippets showing the exact source and version. c) Offer summaries, key clause extraction, and obligation insights.
4.1.19	Metadata-Based Filtering a) Enable refinement of results using structured fields such as contract type, counterparty, effective/expiry date, status, and other custom metadata.
4.1.20	Access Control & Auditability a) Enforce strict role-based and attribute-based access, ensuring users only access permitted documents. b) Apply access checks at both retrieval and AI generation stages. c) Maintain immutable logs of all queries, viewed documents, and AI interactions for compliance.

REQUIREMENT SPECIFICATIONS

4.1.21	User Interface & Experience (UX) - Landing Pages
4.1.22	The system shall provide two distinct landing pages: a Contract Registry Landing Page and a Policy Registry Landing Page.
4.1.23	Each landing page shall display personalized, role-based statistics for the logged-in user.
4.1.24	The landing pages shall display the following user-specific metrics: a) New Workflows relevant to the user. b) Pending Workflows Requiring My Action. c) Completed Workflows the user has participated in. d) My Tasks list with actionable items.
4.1.25	All statistics and task listings shall reflect only data the user is authorized to access, based on the system's access control model.
4.1.26	The landing pages shall provide registry-specific insights, including: a) For Contract Registry: contract expiries, renewals due, obligations due. b) For Policy Registry: policy acknowledgements pending, new or updated policies.
4.1.27	Each tile (KPI/list/chart) shall allow drill-down to a filtered results page showing underlying records or workflows.
4.1.28	The system shall allow administrators to configure tile layout, including adding, removing, reordering, and resizing tiles on both landing pages.
4.1.29	Administrators shall be able to configure metric definitions, filters, and data sources for each tile.
4.1.30	Administrators shall be able to target specific tiles to specific user groups, roles, departments, or audience segments.
4.1.31	Administrators shall be able to define, publish, and manage different landing page templates for different user roles or user groups.
4.1.32	All landing page interactions, tile loads, and drill-down actions shall be audited.
4.1.33	Landing page data shall update in real-time or near-real-time, with timestamps visible to users.
4.1.34	Full Sync-up with Microsoft SharePoint Preferably, the solution shall integrate with Microsoft SharePoint to retrieve the final version directly from the proposed solution repository for either the Contract or Policy Registry. Where direct integration is not available, the solution shall support exporting the full registry for import into Microsoft SharePoint.

REQUIREMENT SPECIFICATIONS

4.2	CONTRACT REGISTRY – FUNCTIONAL SPECIFICATION
4.2.1	The system shall support end-to-end contract lifecycle management, including request, review, approval, e-signature, counterparty execution, finalisation, repository management, renewals, amendments, and notifications.
4.2.2	The system shall support integration with NKF's preferred e-signature solution (e.g. Foxit eSign). If unavailable (out of the box and need customisation), the Vendor shall propose integration with equivalent platforms such as DocuSign or Adobe Acrobat Sign.
4.2.3	Actors a) Requestor (originates contract); b) Endorser(s) (HOD of Requestor/Functional Head, subject matter / functional, derived from Azure AD (refer to clause 4.1.4 & 4.1.5)); c) Approver(s) (Legal, Procurement, as configured); d) NKF Signatories (authorised signers, as setup for the contract by requestor); e) Counterparty Signatories (coordinate by Requestor); f) Registry Owner, System Admin, User Administrator.
4.2.4	Metadata Schema (minimum) a) Contract Ref No (auto) [Refer to clause 4.1.4], Title, Type, Category, Department, Counterparty, Contract Value, Currency; b) Effective Start Date, End Date, Renewal Terms, Notice Period, Termination Rights; c) Risk Classification, Confidentiality Level, Jurisdiction; d) Internal Owner, Requestor, Endorser(s), Approver(s), Signatory(ies); e) Status (Draft, Under Endorsement, Under Approval, Signing – NKF, Counterparty Signing, Executed, Active, Expiring, Renewed, Terminated, Archived); f) Key Dates (submission, approvals, signature completion, renewal reminder dates); g) Linked Documents (drafts, signed PDFs, annexes, amendments); h) Audit fields (timestamps, user actions, and system-generated events); i) Mandatory fields shall be enforced at key workflow stages.
4.2.5	Workflow Management a) Request Creation & Submission ○ Users log in, select Contract workflow. ○ Users shall complete required metadata fields and upload contract drafts/supporting docs. ○ On submission, the system generates the unique Contract Ref No and routes to endorsers/approvers. b) Endorsement & Approval Routing ○ Endorsers/approvers receive notifications; may approve, request changes, or reject. ○ Support sequential and parallel approvals; conditional routing by amount/type/risk. ○ Rejection requires comments; request returns to the originator with audit log. c) Execution (E-Signature & Counterparty) ○ After approvals, NKF signatories are notified to sign electronically. ○ (Preferably) Foxit eSign is the default e-sign tool; system integrates via API/connector. ○ (Preferably) If Foxit cannot be supported, indicate compatibility with DocuSign / Adobe Acrobat Sign or equivalents.

REQUIREMENT SPECIFICATIONS

	○ After NKF signatures complete, system enables counterparty signing trigger and tracks status. ○ Integrity, non-repudiation, and traceability must be ensured for all signed docs. ○ Post-signing, only non-contractual metadata fields (e.g. administrative dates) may be edited, and all changes shall be fully audited. Contract documents shall remain immutable. ○ All approvals, rejections, and comments shall be captured in the audit trail. d) Contract Finalisation ○ System saves the fully executed contract (auto-save) to the repository, linked to the record. ○ Users may confirm/edit start & end dates, set reminder rules (e.g., 90/60/30 days before expiry). ○ All action parties receive execution confirmation with effective dates.
4.2.6	Repository, Search & Access a) Signed documents are captured, versioned, and stored in the solution with full audit trails. b) Advanced search by metadata (counterparty, dates, department, value range) and free text. c) Access to documents shall be enforced based on RBAC and confidentiality classification. d) All reminders and escalations shall be logged.
4.2.7	Notifications, Reminders & SLAs a) Configurable task SLAs per stage (endorsement/approval/signing). b) Automated reminders for key dates (renewal deadlines, expiry, notice periods). c) Escalation paths configurable (e.g., to manager after x days overdue).
4.2.8	Delegation & Coverage a) Users may set out-of-office delegation; delegated tasks route accordingly. b) All delegated actions shall be recorded in the audit trail with both delegator and delegatee.
4.2.9	Amendments, Renewals & Terminations a) Amendment workflow: creates child records linked to the parent Contract Ref No; manages updated clauses/values with approvals and signing. b) Renewal workflow: initiates review prior to expiry; supports auto-renew flags and new term dates; carries forward metadata with audit. c) Termination workflow: records notice, reason, effective termination date; captures supporting correspondence. d) All amendments shall retain historical versions and linkage to original contract. e) Renewals and terminations shall require appropriate approval workflows.
4.2.10	Reporting & Analytics a) Standard reports: cycle time, bottlenecks, expiring contracts, renewal actions due, approval SLA compliance, spend by department/counterparty. b) (Preferably) Reports shall support export and integration with analytics tools (e.g. Power BI).
4.2.11	Security & Access a) Access shall be restricted to authorised roles (e.g. Legal, Requestor, designated users) based on RBAC and confidentiality classification. b) Document permissions synced with record RBAC; confidential flag applies item-level permissions.

REQUIREMENT SPECIFICATIONS

4.3	POLICY REGISTRY – FUNCTIONAL SPECIFICATION
4.3.1	The system shall support end-to-end lifecycle management of Policy Manuals (PM) and Work Instructions (WI), including creation, review, endorsement, approval, publishing, version control, periodic review, and distribution.
4.3.2	Actors a) Policy Owner (requestor/author) b) Head of Department (HOD) (initial reviewer) c) Risk Domain Lead & Co-Lead (endorsement) d) CEO / MD (final approval for Clinical PM; CEO only for Non-Clinical PM) e) Publisher (publishes approved version); Publisher shall be responsible for releasing approved policies into the repository f) Acknowledgers (staff required to attest) g) Registry Owner, System Admin, User Administrator
4.3.3	Metadata Schema a) Policy Ref No (auto-generated) b) Policy Type (PM or WI) c) Policy Document Status (New, Revision, Retirement, Reviewed – No Changes) d) Version (auto-generated, major.minor) e) Title, Category, Department f) Effective Date, Next Review Date (auto-calculated) g) Reason for Update / Remarks h) Owner, Reviewer(s), Approver(s), Risk Domain Lead & Co-Lead i) Classification (Internal/Public/Restricted) j) Linked Documents (draft, tracked changes, clean version, final PDF) k) Audit fields (timestamps, actors)
4.3.4	Workflow Steps Step 1: Request Creation • User logs into the system and selects Policy Manual (PM) or Work Instruction (WI) workflow. • User fills in metadata fields (from PDAF form + Document Control & History section). • System auto-generates version number and Policy Ref No. • Selected data fields will be extracted later for the cover page. Step 2: Template Loading • System loads appropriate template from the proposed solution based on Policy Document Status: ○ New PM/WI → Blank template ○ Revision → Most recent version ○ Retirement → Most recent version ○ Reviewed – No Changes → Most recent version (version locked after approval) Step 3: Content Editing • The system shall support document editing either natively or via integration with document editing tools (e.g. Office 365 or Microsoft Word). Step 4: HOD Review • HOD receives email notification and logs in to review. • If approved:

REQUIREMENT SPECIFICATIONS

	○ For New / Revision / Retirement, HOD selects Risk Domain Lead & Co-Lead from dropdown. ○ For Reviewed – No Changes, version is locked. • If rejected: request returns to user with comments. • All approvals, rejections, and comments shall be logged. Step 5: Risk Domain Endorsement • Risk Domain Lead & Co-Lead receive notifications. • If endorsed: ○ Clinical PM → Route to CEO & MD for approval. ○ Non-Clinical PM → Route to CEO for approval. • If not endorsed: request returns to user. • Routing to Risk Domain Leads shall be system-driven based on predefined rules where applicable. Step 6: CEO / MD Approval • CEO and MD (if applicable) receive notifications. • If approved: ○ Version locked. ○ System saves clean Word version and tracks changes version. • If rejected: request returns to user. • Upon approval, the version shall be finalised and locked from further modification. Step 7: Finalisation • User receives approval notification. • Updates shall be restricted to authorised metadata fields and fully audited. • System auto-generates Next Review Date based on review cycle. Step 8: Cover Page & PDF Generation • System pulls data from metadata fields and auto-generates a cover page. • The system shall (preferably able to automatically) generate a final PDF by combining cover page metadata and approved document content. • Both clean Word and tracked changes versions remain stored for audit. • Generated documents shall be version-controlled and immutable. Step 9: Publishing & Integration • Final PDF stored in registry. • Once published, registry updates status to Published. A Read Only version is sync up to the registry / repository. • (preferably) Integration with Microsoft SharePoint to pull the final version directly from the proposed solution repository. An alternative is to export (current or full registry) from the solution and then import into Microsoft SharePoint. • (preferably) Where out-of-the-box SharePoint integration is not supported and customisation is required, the Vendor shall provide an export function to enable the publisher to manually import the final version into Microsoft SharePoint.
--	--

REQUIREMENT SPECIFICATIONS

4.4	SYSTEM & USER ADMINISTRATION
4.4.1	System administration shall be performed via vendor-provided SaaS administration consoles. The Vendor shall provide administrative capabilities supporting: a) User and role management; b) Workflow and system configuration management; c) SLA, notification, and escalation configuration; and d) Audit logging and reporting access.

REQUIREMENT SPECIFICATIONS

5.	TECHNICAL REQUIREMENTS
5.1	BROWSER AND DEVICE COMPATIBILITY
5.1.1	The solution shall ensure consistent functionality across supported browsers and devices (with the latest two (2) major versions): a) Microsoft Edge (Chromium-based). NKF's corporate standard (mandatory full compatibility for both desktop and mobile versions); b) Google Chrome; c) Mozilla Firefox; d) Apple Safari.
5.1.2	The registry solution shall support widely used mobile platforms (Android and iOS) on the latest two (2) major versions.
5.1.3	The solution shall adopt a responsive web design to ensure optimal rendering and usability across varying screen sizes and resolutions.
5.1.4	Vendor must disclose any functionality that is not fully compatible with Microsoft Edge in their proposal.
5.2	TWO-FACTOR AUTHENTICATION (2FA)
5.2.1	The solution should preferably integrate with NKF's Microsoft Entra ID (Azure AD) MFA policies. Where such integration is not supported, the Vendor must provide equivalent MFA capabilities within the SaaS platform without requiring custom development.
5.2.2	All authentication events, including MFA challenges and failures, shall be logged and auditable.
5.3	SINGLE-SIGN ON (SSO)
5.3.1	The registry solution shall leverage NKF's existing Microsoft Azure Active Directory (Azure AD) for Single Sign-On (SSO). All NKF users shall authenticate via Azure AD using their corporate credentials. The vendor shall ensure: a) Proper configuration of SSO for all components of the registry solution. b) Enforcement of NKF-defined session timeout and auto-logout policies. c) Audit logging of user sessions, including client IP, user ID, last login, session timeouts, and accessed dashboards. d) Support for conditional access policies and multi-factor authentication (MFA) as configured in NKF's Azure AD tenant. e) The vendor shall highlight any limitations in applying NKF's Azure AD security policies to the registry solution.
5.3.2	Where native SSO integration is not supported, the Vendor must propose an alternative secure authentication mechanism and clearly state limitations and mitigation measures.
5.3.3	The system shall enforce secure session handling, including protection against session hijacking and replay attacks.
5.4	SYSTEM & APPLICATION ARCHITECTURE
5.4.1	The Vendor shall clearly indicate any third-party components or dependencies within the architecture. The Vendor shall provide architecture diagrams illustrating: a) SaaS application components; b) Hosting model and declared data residency; c) Standard integration points; and d) Security, availability, and scalability measures.
5.5	BACKUP & RESTORATION
5.5.1	Backup and restoration services shall be vendor-managed, with documented RPO and RTO, regular backups, and tested restore procedures.

REQUIREMENT SPECIFICATIONS

5.5.2	Backup and restoration procedures shall be tested periodically (by default annually), and evidence/results shall be made available upon request at no additional cost (for filing).
5.6	SERVICE RELIABILITY
5.6.1	The SaaS platform shall provide a minimum 99.9% availability SLA , excluding scheduled maintenance.
5.7	AUDIT REQUIREMENTS
5.7.1	NKF shall have the right, upon reasonable prior notice, to audit the registry solution's configuration, processes, and records to verify compliance with: a) Contract terms; b) NKF security and governance policies; c) Applicable laws and industry best practices.
5.7.2	The vendor shall: a) Ensure audit logging is enabled for all solution components. b) Provide detailed audit reports for privileged actions performed by vendor administrators and NKF users. c) Cooperate with NKF-appointed auditors (internal or external) up to twice annually. d) Maintain confidentiality while granting full access to relevant logs and documentation.
5.7.3	Audit logs shall include: a) User identity; b) Action performed; c) Timestamp; d) Source IP and device details; e) Session details (login/logout, timeouts).
5.7.4	Vendor shall highlight any limitations in its solution audit capabilities and propose mitigation strategies.
5.8	DATA PROTECTION TRUSTMARK CERTIFICATION
5.8.1	The vendor remains responsible for ensuring that all operational and administrative activities comply with the Personal Data Protection Act (PDPA) and NKF's data governance policies. https://www.imda.gov.sg/how-we-can-help/data-protection-trustmark-certification
5.8.2	Vendor are encouraged to hold Data Protection Trustmark (DPTM) certification to demonstrate accountable data protection practices. a) Evidence of certification shall be submitted with the proposal. b) If not certified at submission, the awarded vendor is encouraged to obtain DPTM within 12 months of contract award. Vendor shall also ensure that all personnel handling NKF data follow PDPA-compliant processes, including secure access, retention, and disposal of sensitive information.
5.9	INTELLECTUAL PROPERTY AND OWNERSHIP
5.9.1	NKF shall retain ownership of: a) All NKF data; b) NKF Background IP; c) Foreground IP; and d) NKF-specific configurations and content stored within the SaaS platform. The Vendor shall retain ownership of the SaaS platform, underlying software, and all platform intellectual property. NKF does not require ownership of source code or standard SaaS platform IP.

REQUIREMENT SPECIFICATIONS

	Where any NKF Customisations are incorporated by the Vendor into its general SaaS offering for reuse across customers, such incorporation shall not restrict NKF's rights to continue using such customisations. The Vendor shall not reuse, commercialise, or disclose NKF Customisations outside NKF without prior written consent from NKF, where such Customisations are uniquely identifiable to NKF's operations. Any joint commercialisation of Foreground IP shall be subject to separate discussions between the parties and shall only proceed on mutually agreed terms documented separately. NKF Background IP shall mean all intellectual property rights owned or controlled by NKF prior to the commencement of the Services, or developed independently by NKF outside the scope of the Services, including any pre-existing data, materials, content, processes, methodologies, know-how, systems, documentation, and other intellectual property provided by or made available to the Vendor for the purposes of performing the Services. Foreground IP shall mean all intellectual property rights arising from, created, developed, configured, or customised specifically for NKF in connection with the Services, including NKF-specific configurations, content, customisations, workflows, and deliverables developed for NKF's use.
5.10	INFORMATION ON THIRTY PARTY SECURITY EVALUATION
5.10.1	The Vendor shall submit the required Information on NKF Third Party Information Security Evaluation Form using the template in Annex D .

Annex A – Cost Schedule

Refer to attachment: **RFP 20260801 Annex E Price Schedule.docx**

Annex B – Service Level Agreement

1) Problem Resolution Service Level Agreement (SLA)

Severity	Description	On Site Response Time	Resolution Time	Resolution %
Level 1	Impacts all users and operation cannot continue.	FOUR (04) hours or less	SIX (06) hours or workaround within EIGHT (08) hours or less	100%
Level 2	These problems affect a particular process, system or function in a service in many branches or more than 50% of services are down in one branch.	EIGHT (08) hours or less	TWELVE (12) hours	100%
Level 3	The problem has minimal or no effect on NKF's ability to perform its functions. The problem is an isolated case.	FOUR (04) working days or less	SEVEN (07) working days or less	90% resolution within SEVEN (07) working days; remaining 10% within TEN (10) working days

- Response time is the time period from when the Contractor is officially notified via telephone call (or email or system alert) to the time when a competent engineer responds.
- Resolution time is the time period from when the Contractor is officially notified via telephone call (or email or system alert) to the time when the problem is resolved to NKF's satisfaction.
- Workday refers to a working day for NKF HQ staff.

2) Service Level Agreement for Change Requests

#	CR Type	Definition	Response Time
(a)	Urgent Request	Requests that are urgently required.	Within <u>TWO (02)</u> working days
(b)	Normal Request	<u>Minor Change Request</u> Change Request that requires less than or equal to <u>TEN (10)</u> man-days to complete.	Within <u>FIVE (05)</u> working days
		<u>Major Change Request</u> Change Request that requires more than <u>TEN (10)</u> man-days to complete.	Within <u>TEN (10)</u> working days

REQUIREMENT SPECIFICATIONS

The Contractor shall note that response time includes the Contractor making an assessment of the Change Request and submitting a practical proposal to NKF for approval.

Completion: Time taken to complete the Change Request.

SLA: 100% should be completed within agreed date

REQUIREMENT SPECIFICATIONS

Annex C – NKF Statistics

For Contract Registry:

Total Number of users: (02 admin executive + 01 manager and 01 management) * (25 HQ + 47 DC) Cost Centre/dept = **288 users**.

Assuming legal and CEO are part of this figure in the respective departments. I.e. Legal and CEO serve as managers and management within their respective departments.

Total number of active documents (A) = 74 * 5 active documents annually. Each document needs around 3 e-signature portion/area (i.e., 1x support, 1 x reviewer and 1 x final approval)

Total number of eSign document = 75% * (A)

For Policy Registry

Total Number of users: (01 admin executive/manager + 01 HOD) * (25 HQ + 47 DC)

Cost Centre/dept = **144 users**.

Total number of active documents (B) = 74 * 2 active documents annually.

Total number of eSign document = 50% * (B) annually

a. Dept code:

System Code	Department/Function Name
CEO	Executive Office
DRD	Donor Relations
CCD	Corporate Communications
VMD	Volunteer Management
OPR	Outreach
CSS	Service Development (Com Supp Services)
OPS	Clinical Operations (Centre Ops)
OPR	Outreach Deactivated
STP	Strategy Planning
RMD	Risk Management
FIN	Finance
ITD	Information Technology
MED	Medical Services
NUR	Nursing Services
PDD	PD Community Support Program
PDC	PD Centre at Blk 109, Whampoa (Closed)
PDY	PD Centre at Yishun Community Hospital
NPD	National PD
CLA	Medical Affairs "MAF" (Clinical Affairs)
MRO	Medical Records Office Deactivated
DTD	Dietetics
ADM	Admin & Control (Admissions)
IRC	Integrated Renal Centre
THD	Therapy
BME	BME
ENF	Exercise & Fitness
CSM	Service Management (Case Mgt/MSW)
ADS	Administration Deactivated
PFM	Property & Facilities Management (Fac/Bldg)
LOG	Logistics
PUR	Purchasing

REQUIREMENT SPECIFICATIONS

HRD	Human Resource
ALJ	102 Aljunied DC
AM1	Ang Mo Kio_1 Dialysis Center (Closed)
AM2	633 Ang Mo Kio DC
AM3	565 Ang Mo Kio DC
BED	27 New Upper Changi DC
BBK	103 Bukit Batok DC
BPJ	274 Bangkit DC
CLE	326 Clementi DC
HON	Hong Kah Dialysis Center (Closed)
HG1	114 Hougang DC
HG2	628 Hougang DC
JW1	744 Jurong West DC
KKT	NKF Centre DC
PSR	180 Pasir Ris DC
SRG	201 Serangoon DC
SMI	101 Simei DC
UBK	19 Upper Boon Keng DC
TM1	935 Tampines DC
TWY	113 Teck Whye DC
TPH	225 Toa Payoh DC
WD1	825 Woodlands DC
WD2	365 Woodlands DC
YS1	203 Yishun DC
GMH	1 Ghim Moh DC
JW2	940 Jurong West DC
TM2	271 Tampines DC
YS2	639 Yishun DC
KLA	43 Bendemeer DC
BM2	128 Bukit Merah DC
BP2	275 Bangkit DC
YS3	840 Yishun DC
WCR	701 West Coast DC
ADT	761 Woodlands DC
URD	311 Ubi DC
MSD	204 Marsiling DC
QT1	55 Strathmore DC
PNG	Punggol Oasis Terrace DC
CP1	IRC Level 1 DC
CP2	IRC Level 2 DC
CP3	IRC Level 3 DC
RFH	Raffles Hospital Dialysis Center (Not in use)
JE1	240C Jurong East DC
TP2	Toa Payoh West CC DC
YS4	Yishun Community Hospital DC
BD2	105 Bedok DC
PR2	427 Pasir Ris DC
BB2	113A Bukit Batok West DC
SKG	Sengkang Community Hospital DC (SKCH)
PN2	One Punggol DC
BDR	213 Bidadari DC
FNV	465 Fernvale DC
SR2	"Serangoon Polyclinic"

Annex D – Thirty Party Security Evaluation

The purpose of conducting a Third-Party Security Evaluation is to ensure that any solution, system, or service proposed by a vendor meets the organisation's security, compliance, and risk-management requirements before adoption. Specifically, this evaluation aims to:

1. Assess the Security Posture of the Proposed Solution, and
2. Identify Potential Risks and Vulnerabilities

CONFIDENTIAL – FOR THIRD PARTY EVALUATION ONLY

Part I

NKF Third Party Information Security Evaluation Form

Name of Company	
Person Completing the Form	
Email Address	
Phone Number	
Company Website	
Date of Assessment	

Data Controls	3 rd Party Response (Yes / No / Partially Implemented)
1. Will store all NKF data in Singapore.	
2. Maintains an audit log for the location of all NKF data.	
3. Will not access NKF data from outside of Singapore.	
4. NKF data will be promptly deleted when retention is no longer necessary for legal or business purposes.	
5. NKF data is permanently erased when deleted.	

3 rd Party's Business Associates	3 rd Party Response (Yes / No / Partially Implemented)
1. Will any 4th parties have access to NKF data?	
2. Confidentiality agreements have been signed before proprietary and/or confidential information is disclosed to the 3 rd party's business associates.	
3. 3 rd party's business associate agreements document the agreed transfer of NKF data when the relationship terminates.	
4. 3 rd party performs periodic review on business associates that have access to NKF data.	

CONFIDENTIAL – FOR THIRD PARTY EVALUATION ONLY

Access Controls	3rd Party Response (Yes / No / Partially Implemented)
1. Has a policy to protect NKF information against unauthorised access.	
2. Has a policy that prohibits sharing of individual accounts and passwords.	
3. Has a policy that implements the need-to-know and separation-of-duties principles.	
4. Implements multi-factor authentication in order to access NKF resources.	
5. Immediately removes or modifies access when personnel terminate, transfer, or change job functions.	
6. Ensures that critical data, or systems, are accessible by at least two trusted and authorised individuals, in order to limit having a single point of service failure.	

Network Security	3rd Party Response (Yes / No / Partially Implemented)
1. NKF data are not directly accessible from the internet unless the NKF data is encrypted	
2. Servers holding NKF data connected to any network must run host-based firewalls configured to block all connections to the system other than the specific types of connections needed to perform the approved functions.	
3. Documented practices are in place and followed on maintaining the configurations of host-based firewalls.	
4. NKF data must be encrypted when it traverses any network (outside of a switch in a secure information centre).	
5. NKF data must never be sent via email except in encrypted files.	
6. All users who need to transfer NKF data must make use of a secure transfer method (e.g. encrypted email).	

Annex D – Page 2 of 4

REQUIREMENT SPECIFICATIONS

CONFIDENTIAL – FOR THIRD PARTY EVALUATION ONLY

Physical Security	3rd Party Response (Yes / No / Partially Implemented)
1. Controls access to secure areas.	
2. Controls access to server rooms and follows the principles of least privilege and need-to-know.	
3. Safeguards in place (e.g., cipher locks, restricted access, room access log, card swipe access control).	
4. Shreds or incinerates printed confidential information.	
5. Escorts visitors in computer rooms or server areas.	
6. Implements environmental controls to mitigate the environmental threats to equipment.	

Contingency Planning	3rd Party Response (Yes / No / Partially Implemented)
1. Has written and tested backup procedures.	
2. Maintains a documented and tested disaster recovery plan.	
3. Has a written contingency plan for critical computing operations.	

Incident Response	3rd Party Response (Yes / No / Partially Implemented)
1. Maintains incident response procedures, including notifying NKF in the event of a breach involving NKF data.	
2. Has cyber security / liability insurance coverage.	

Annex D – Page 3 of 4

CONFIDENTIAL – FOR THIRD PARTY EVALUATION ONLY

NKF Data Requirement					
As part of the outsourcing / contracted service arrangement, the service provider may collect, use, process or store the following types of data (please ☒ tick where applicable):					
Risk Level	Data Type	Collect	Use	Process	Store
High	☐ Personally Identifiable Information (PII)	☐	☐	☐	☐
	☐ National Registration Identity Card (NRIC) Number	☐	☐	☐	☐
	☐ Payment Card Information	☐	☐	☐	☐
	☐ Sensitive Research Data	☐	☐	☐	☐
	☐ NKF Mission Critical Information	☐	☐	☐	☐
Medium	☐ NKF Business Confidential Information	☐	☐	☐	☐
	☐ Anonymised Research Data	☐	☐	☐	☐
	☐ Other Confidential Information (Please indicate)	☐	☐	☐	☐
Low	☐ Non-Sensitive / Non-Confidential Information (Please indicate)	☐	☐	☐	☐
Additional Documents Furnished					
☐ Network Diagram ☐ Security Architecture ☐ Security Assessment Results ☐ Security Policies ☐ SOC 2, ISO Reports ☐ Change Management Policy ☐ Backup and Restoration Procedures ☐ Incident Management Plan ☐ Business Continuity Plan ☐ Disaster Recovery Plan ☐ Cyber / Liability Insurance Certificate ☐ All relevant test report(s) ☐ All relevant certification(s) ☐ Other relevant document(s)					

REQUIREMENT SPECIFICATIONS

Annex E – Evaluation of the Vendor Solution (for the trial functionalities during evaluation)

Please refer to clause 3.4 regarding a trail of the vendor solution, after the procurement presentation. Below are the functionalities to be tested. Preferably, the solution can be tested out of the box or with minimise configuration, able to meet the requirements specified in these documents.

User Accounts:

SN	Functional	Users Account
1	Requestor01	User1 (NKF <Email to be provided before the trail>)
2	Requestor02	User2 (NKF <Email to be provided before the trail>)
3	Requestor11	User3 (NKF <Email to be provided before the trail>)
4	Requestor12	User4 (NKF <Email to be provided before the trail>)
5	HOD01 (HOD for Requestor01/02)	HOD01 (NKF <Email to be provided before the trail>)
6	HOD21 (HOD for Requestor11/12)	HOD21(NKF <Email to be provided before the trail>)
7	Legal	Legal (NKF <Email to be provided before the trail>)
8	CEO	CEO (NKF <Email to be provided before the trail>)
9	Admin02 (User Admin)	Admin for User Account Management, Privileges / Role / Access Management, and managing and configuring workflow, notification.
10	Admin03 (IT/System Administration)	Full administration

Use Cases / Scenarios:

SN	Functional	Details
1	User/Privilege/Role Management	User Management
2	Workflow#1 (contract): 1. Contract	1. Requestor has a contract (main contract document + supporting other documents) ready, enters metadata (total contract value, start/end contract date, risk classification, milestones for 4 years of contract), initiates a workflow to attach the contract document and its supporting documents. and route for 3 different workflow approvals by HOD, Legal and CEO. 2. Different users (HOD, Legal & CEO) look at logon's landing page to look at the tasks pending them. 3. Users provide comments and perform workflow approval. 4. Generate audit trail on the transactions. 5. Bulk loading of contract (with full records) by a department admin.

REQUIREMENT SPECIFICATIONS

		6. GenAI to retrieve records on active contract by a specific vendor and period.
2	Workflow#2 (PM/WI): 1. PM / WI	1. Requestor has a revised policy document (main policy document) ready, enters metadata (reason of changes, risk domain, classification), initiates a workflow to attach the contract document and supporting documents. initiates a workflow and route for 3 different workflow approvals by HOD, MD and CEO. 2. Different users (HOD, Risk Manager & CEO) look at logon's landing page to look at the tasks pending them. 3. Users provide comments and perform workflow rejection and then approval after one round. 4. Generate audit trail on the transactions. 5. GenAI to retrieve policy records needing to be reviewed by next 6 month, and by which depts.
3	Email notification	1. Any update to the workflow (before final approval), email will be routed to requestor. 2. Notification before contract expiry. E.g., 90 days before. 3. Notification upon contract expiry. E.g., 1 day of expiry
4	eSignature / Foxit / DocuSign	eSignature

Annex F – Resume of Vendor’s Personnel

1. PERSONAL PARTICULARS

Name of Staff : _____
Designation : _____
NRIC / Passport No (last 3 Chars) : _____
Age : _____
Citizenship⁶ : _____
Country of Residence : _____
Role in this Project : _____

2. PROFILE (Brief description of past and present work portfolio)

3. EDUCATION / PROFESSIONAL QUALIFICATIONS

Period Discipline / University

4. EMPLOYMENT HISTORY

Period Appointment / Organisation Responsibilities

5. TECHNICAL EXPERIENCE

(e.g. experience on pre-requisite skill sets, length and period of exposure etc.)

Note: Experience in maintaining similar size and scope of system will be added advantage and should be elaborated.

⁶ Please indicate whether “Permanent Resident” or “Employment Pass Holder” if non-Singapore Citizen.

REQUIREMENT SPECIFICATIONS

Annex G – Statement of Compliance

1. Please state clearly the compliance to each clause. Where there is a failure to indicate any compliance against any clause, it shall be deemed that the Tenderer has indicated "Full Compliance" and the offer shall be evaluated accordingly. The Tenderer shall bear in mind the clauses on Compliance to Part 1 on Terms and Conditions in the Form of Tender and Evaluation Criteria when completing the Statement of Compliance.
2. The Tenderer shall not add comments against the clause that vary the meaning of full compliance to the clause. However, comments indicating references to literature to substantiate the response is permissible. Any other comments which will vary the meaning of full compliance will be ignored.
3. Only the following responses are acceptable:

Responses	Description
"FC" or Full Compliance with Third-party Add-on Component(s) or Module(s)	Able to comply fully. When the proposed System and services is able to meet the requirement with the need to install, configure, integrate and deploy additional add-on modules and/or components that is not supplied in the base product. The Tenderer shall indicate the name, version numbers (if applicable) and description of the proposed add-on modules and/or components in the proposal. If applicable, the Tenderer shall also indicate references to literature to substantiate the response. Any other comments which will vary the meaning of full compliance will be ignored.
"CC" or Compliance with Customisation	Able to comply fully When the requirement can be met only by a custom-made (customised codes) development to be supplied by the Tenderer. The Tenderer shall clearly indicate the type and nature of the proposed customisations required to meet the requirement. If applicable, the Tenderer shall also include reference site(s) in its proposal where the proposed customisations have been deployed. Any other comments which will vary the meaning of full compliance will be ignored.
"NC" or Non-Compliance Not Able to Comply Fully	When the System or Services does not fully comply with the requirements. If the proposed System does not provide for any of the stated requirements (utilising existing capabilities in the application; products or add-on modules developed by the Tenderer or third parties; or application customisations), the Tenderer shall provide alternative approach(es) to address each of these requirements in its proposed System for consideration and approval by the Authority.

Explanatory note must be provided under the column "Remarks" for cases where the compliance is "NC". If the compliance is "FC", there shall NOT be any explanatory notes. Where explanatory notes are provided in these cases, they shall not alter the meaning of full compliance. Vague responses such as "Refer to brochure attached" are not acceptable.

Must, Shall, Will or Mandatory	The item mentioned is an absolute requirement.
--------------------------------	--

REQUIREMENT SPECIFICATIONS

Should, Where Possible or Recommended	The item mentioned should be followed. Exceptions must be documented and approved by the Government Agency. Compensating controls must be in place
May or Option or Optional	The item mentioned is truly optional. It may be followed as a suggestion.

S/N	Paragraph Reference	Compliance (FC/NC)	Percentage of Customisation ('NA' if none)	Remarks
REQUIREMENTS SPECIFICATION				
4.0	4.0			
	4.1.1	..	..	
	4.1.2	..	..	
	4.1.3	..	..	
	4.1.4	..	..	
4.1	x	..	..	
	X	..	..	
	X	..	..	
	X	..	..	
	X	..	..	
x	x			
	X	..	..	
	X	..	..	
	X	..	..	
	X	..	..	
x	x	..	..	
	X	..	..	
	X	..	..	
	X	..	..	
	X	..	..	
5.0	5.0			
	5.1.1	..	..	
	5.1.2	..	..	
	5.1.3	..	..	
	5.1.4	..	..	
x	x			
	X	..	..	
	X	..	..	
	X	..	..	
	X	..	..	