Request for Information (RFI) Questionnaire

Self-Administered Pension Fund Member Management & Financial System

Part 1: Introduction & Project Background

- **Fund Overview**
  - The Germiston Municipal Retirement Fund (GMRF) is a fully funded and self-administered retirement fund operating as a defined contribution scheme under Pensions Fund Act ,1956 . Established originally in 1924, the Fund services members across the local government structures of the Ekurhuleni Metropolitan Municipality.

- **Purpose of RFI**
  - The purpose of this RFI is to evaluate market-ready, modern, scalable, and secure Member Management System solutions. The target platform must seamlessly deliver end-to-end member administration, strict regulatory compliance, alignment with international security standards, financial systems integration, and digital stakeholder portals to fundamentally improve operational efficiency and member engagement across our approximately 2,000-member baseline.

- **Procurement Disclaimer**
  - This RFI is for information-gathering purposes only. It does not constitute a binding tender, contract, or commitment to purchase on the part of the GMRF.

- **Administrative Information**
  - RFI Issuing Date: 24 August 2026
  - Submission Deadline: 30 October 2026
    - **No submissions received after the submission deadline will be considered.**
  - Contact Person: Principal Officer principal@gmrf.co.za Submission Format: All responses must be provided in electronic format, by no later than 16h00 on the submission deadline, to the address of the Contact Person.
    - Vendors may, in addition to the electronic format submission, deliver hard-copy documents (4 copies) to the GMRF, ensuring they are adequately sealed/secured, at the following physical address:
      - Attention: Principal Officer
        RFI 02/2026
        Germiston Municipal Retirement Fund,
        53 Rendell Road
        Wadeville
        1429

- **Next Steps:**
    - Information gathered will be used to refine a forthcoming Request for Proposal (RFP). Response to this RFI is voluntary but highly encouraged for inclusion in a potential future tender process. The GMRF retains the right, at its sole discretion, to engage in an open or closed RFP or not to proceed with an RFP.
- **Clarifications & Queries:**
    - Vendor requirements for additional information and/or clarification must be sent to the Contact Person in writing at the contact email address provided.
        - Strict Provisions:
            - No telephonic or in person engagement on this RFI with any personnel or Trustees of the GMRF are allowed.
            - Responses for clarification sought and additional information required may, at the sole discretion of the GMRF, be published publicly on the official GMRF website.
            - Responses for clarification sought and additional information required must be communicated to the GMRF by no later than one working week prior to the Submission Deadline.
    - Vendors can also make us of the facility on the GMRF website https://gmrf.co.za to post questions and/or requests for clarification.
        - Click on the "RFI" button
            - When you click on it you will be asked to enter your name and contact details (email) and there will be a place to enter your question.
            - The GMRF will review the questions and post responses which will be publicly visible on the web site.

Part 2: Vendor Profile, Corporate Ownership & Financial Sustainability

- **Concise Corporate Profile:**
    - Provide a detailed overview of your operational capacity, corporate structure, and long-term viability.
- **Company Footprint:**
    - State your exact total years in business, current geographic footprint, and the physical location of your primary support services, data centres, and core development hubs.
- **Corporate Ownership & Shareholding:**
    - Provide a transparent breakdown of your organizational equity structure.
    - Detail your ultimate beneficial owners and any parent holding companies.
    - State your formal Broad-Based Black Economic Empowerment (B-BBEE) equity status and verification level under South African legislation and provide a copy of the valid certificate.
- **Financial Sustainability Information:**
    - Provide concrete evidence of financial stability to guarantee long-term system support, maintenance, and compliance updates.
        - Summary Indicators:

      - Disclose summary financial metrics from your audited financial statements for the past two audited financial years, explicitly confirming sustainable operating capital.
    - Financial Ratios:
      - Provide your multi-year profitability trends, debt-to-equity status, and liquidity ratios.
- **Product Maturity:**
  - Detail the established market footprint of the proposed software solution.
  - State the total number of active pension fund system installations globally.
  - State the total number of active pension fund system installations locally within South Africa.
  - State the number of solution users
- **Cradle-to-Grave Capability:**
  - Provide confirmation and supporting evidence that your organization possesses the internal capacity, engineering skill, and professional experience to manage and implement this system end-to-end.
  - Vendors must demonstrate capability across all phases, including customization, long-term live operational support, and ongoing engineering support ("cradle-to-grave").
- **Fidelity Insurance:**
  - Confirm your risk mitigation and professional liability protections.
    - Confirm whether your organization carries comprehensive Professional Indemnity and Fidelity Guarantee Insurance cover.
    - Specify the total limit of financial indemnity per claim.
    - State the formal business name of your underlying underwriting insurer.
- **Professional Association Memberships:**
  - List your current institutional memberships in relevant professional associations (e.g., Institute of Retirement Funds Africa (IRFA), Pension Lawyers Association, BATSETA or equivalent tech bodies).
- **Quality & Security Standards Compliance:**
  - Confirm and provide evidence of your compliance with formal quality and security benchmarks.
  - Specify if your organization and/or hosting environments are certified in ISO/IEC 27001 (Information Security Management), ISO 9001 (Quality Management), or an equivalent standard (e.g. NIST).
- **Key Vendor Contact Details:**
  - Provide the contact profile for the primary person managing communications for this RFI submission:
    - Full Name & Designation
    - Corporate Physical & Postal Address
    - Direct Telephone & Mobile Number
    - Dedicated Business Email Address

Part 3: Source Code Escrow & Business Continuity Provisions

- To safeguard fund operational continuity and insulate member records from vendor business disruptions, the GMRF mandates a comprehensive Source Code Escrow Framework. Vendors must confirm their willingness and technical capability to enter into a tri-partite escrow agreement under the following strict terms:
- **Escrow Mechanism:**
    - Confirm your commitment to deposit and maintain the full, compilable source code, database schemas, object libraries, deployment documentation, and configuration scripts of the proposed system with an independent, certified third-party escrow agent.
    - Disclose how frequently the escrow deposit is refreshed with new software iterations.
    - Triggering Events for Release:
        - Confirm your acceptance that the independent escrow agent will be contractually authorised to release the full source code and related technical documentation directly to the GMRF under the following conditions:
            - Corporate Mergers, Acquisitions, or Control Shifts: Should the vendor merge with, or be acquired by, another entity, and the successor entity fails to formally guarantee or execute identical or superior SLA, compliance, and support obligations.
            - Cessation of Service or Support Breach: Should the vendor become un-contactable, fail to provide ongoing statutory compliance updates (e.g., SARS/FSCA changes), or repeatedly breach critical Priority 1 SLA remediation windows over a rolling 30-day period.
            - Insolvency & Business Failure: Should the vendor be legally declared insolvent, enter into business rescue, initiate liquidation proceedings, or otherwise cease active trading operations.
        - Post-Release Operational Rights: Confirm your acceptance that, upon the occurrence of any triggering event, the GMRF will be automatically granted a non-exclusive, perpetual, royalty-free license to use, modify, compile, and maintain the source code solely for the continued internal administration of its member database.

Part 4: Solution Development Approach & Release Strategy

- **Software Development Methodology:**
    - Describe your core engineering approach (e.g., Agile, Scrum, DevSecOps, Waterfall). Explain how security checks and quality compliance reviews are built directly into your active coding pipeline.
- **Code Quality & Testing Strategy:**
    - Detail your Quality Assurance (QA) protocols for new software modules. How do you utilise automated testing, regression tracking, and sandboxed environments to verify financial calculation engines before deployment?

- **Software Release Lifecycle:**
  - Outline your global roadmap and release strategy for major system upgrades, minor feature iterations, and security hotfixes. Detail your regular cadence for system updates, minor patches, and major version upgrades. Detail how testing, deployment windows, and rollback protocols are managed in production environments.
- **Deployment & Upgrade Mechanics:**
  - Detail the process for moving your live application from an older software version to a newly released version. Explain how you prevent downtime, preserve custom code branches, and safeguard fund-specific metadata configurations during a version upgrade.
- **Client Validation & Sandbox Access:**
  - Do you provide a dedicated, isolated staging/UAT environment running the upcoming system release to allow GMRF internal teams to validate workflows before the production database is upgraded?
- **Pension Industry Regulatory Alignment:**
  - Detail the operational framework used to monitor, code, test, and push updates in response to shifting South African retirement legislation (e.g., updates from the FSCA, National Treasury, and SARS).
- **Proactive Change Management Framework:**
  - Explain how the core software architecture accommodates sudden industry adjustments (such as the Two-Pot retirement parameters or updated Regulation 28 investment ceilings). Specify whether these changes require extensive, chargeable codebase modifications or if they can be managed seamlessly via client-managed, rule-based system configuration tables.

Part 5: Implementation Methodology, Duration & Deployment Approach

- **Deployment lifecycle:**
  - Vendors must detail their deployment framework strategy, timeline estimates, training protocols, and execution pathways for bringing the platform live based on a member baseline of approximately 2,000 active/deferred members with standard national and corporate integrations (SARS, DHA, Banking, ERP):
- **Implementation Approach & Methodology:**
  - Provide a comprehensive breakdown of your software deployment framework (e.g., Agile, Waterfall, or a Hybrid iterative rollout blueprint). The description must be structured cleanly into logical delivery phases: as per the following point.
- **Project Duration Estimates by Phase**:
  - Provide specific, conservative duration estimates (expressed in weeks or months) for each of the following execution segments:
    - Phase 1: Discovery
    - Phase 2: Scoping & Gap Analysis
    - Phase 3: System Configuration & Customization

    - Phase 4: Legacy Data Migration & Cleaning
    - Phase 5: Integrations (Banking, ERP, SARS, DHA) & Testing
    - Phase 6: Training (Super User and staff – 3 x Super users and 2 x staff)
    - Phase 5: User Acceptance Testing (UAT) & Parallel Run
    - Phase 6: Go-Live
    - Phase 7: Hypercare Support Stabilization Period
- **Project documentation/artefacts:**
  - Provide a comprehensive list of all documentary deliverables that will be generated and be approved during the 7 phases referred to in the previous point.
    - List these deliverables in a tabular format, per Phase.
- **Data Migration Strategy Framework:**
  - Detail your strategy for extracting, transforming, loading, cleaning, and validating historical member record histories from legacy administration systems without disrupting the fund's day-to-day administrative output.
- **Change Management & Training Execution:**
  - Provide a detailed overview of your deployment methodology for role-based user adoption programs, material transfers, and system training protocols aligned directly to your implementation quality assurance benchmarks.

Part 6: Implementation Quality Assurance Approach

- **Quality Assurance (QA) Framework**
  - To guarantee project success, the fund requires a rigorous, metrics-driven Quality Assurance (QA) Framework integrated directly into the deployment plan.
    - Vendors must detail their methods, tracking metrics, and gates across the following operational domains:
    - Timeous Completeness (Schedule Quality):
      - Detail your controls for schedule adherence.
    - Critical Path Tracking:
      - Explain your continuous tracking of project dependencies via a formal Project Management Office (PMO) structure.
    - Milestone Gate Reviews:
      - Provide details on your formal "Go/No-Go" verification gates at the conclusion of every delivery phase. Confirm that implementation cannot advance to a subsequent phase until all preceding milestone deliverables are signed off.
    - Slippage Recovery Controls:
      - Describe the structured mechanisms used to instantly trigger resource reallocation or parallel tracking workflows the moment any timeline indicator slips past predefined project tolerances.
    - Functional Adherence (System Mapping Quality):
      - Detail your quality gates for system mapping.
    - Requirements Traceability Matrix (RTM):

      - Confirm the mandatory implementation of an active RTM mapping every single requirement listed in this RFI down to a specific configuration table, software test case, and verified User Acceptance Testing (UAT) sign-off line.
    - Multi-Tiered Automated Testing:
      - Explain your continuous application validation protocols utilizing Unit Testing, Automated System Integration Testing (SIT), Regression Testing, and End-to-End processing simulations.
    - Discrepancy Severity SLA:
      - Detail your timeline constraints for resolving defects discovered during configuration and UAT, ensuring no software can go live with active critical flaws.
    - Completeness of Information (Data Migration Quality):
      - Detail your technical quality gates for data migration.
    - Pre-Migration Integrity Checks:
      - Describe the automated routines used to scan legacy data sets for structural anomalies, unmapped characters, invalid South African ID structures, and orphaned member records before extraction begins.
    - Reconciliation Balancing Sheets:
      - Detail your triple-point financial balancing workflows ensuring total fund asset values, individual member savings pots, and contribution histories reconcile perfectly down to the single cent between the legacy environment and the new core ledger.
    - Data Field Validation Exceptions:
      - Explain the real-time generation of custom exception dashboards identifying fields with missing critical metadata (such as missing beneficiary nominations or incomplete historical tax directives) for clean-up.

Part 7: Success of Systems User Training (UAT & Operational Readiness)

- **Detail your training metrics:**
  - Role-Based Training Modules:
    - Describe your tailored training curriculums designed specifically for distinct user paths, including Fund Trustees, System Administrators, Back-Office Accountants, and Employer HR personnel.
  - Formal Competency Appraisals:
    - Detail your structured testing and execution certifications for system users. Confirm that no internal administrator will be provisioned access to the live production database until they successfully achieve a minimum passing grade on core processing simulations.
  - Post-Go-Live Hypercare Monitoring:
    - Confirm the provision of on-site and dedicated virtual technical engineering support stationed within the fund operations for a

minimum of 30 days post go-live to manage real-world user queries and optimize user confidence.

Part 8: Standard & Native Core Functional Solution Capabilities

- **Solution overview:**
    - Provide a clear and concise description of the solution capability for the following components, declaring if each is Out-of-the-Box (OOB), requires Custom Development (CD), or is supported via a Third-Party Integration (3P):
        - Core Membership Administration & Profile Management:
            - Data Onboarding:
                - Automated processes for new member registration and employer data uploads.
            - Profile Management:
                - Maintenance of personal details, beneficiary nominations, employment history, and contact information.
            - Differentiated Member Profiles:
                - Capability to configure and manage highly unique, differentiated contribution values (fixed amount, tiered scaling, or variable percentages) and distinct benefit scales per member profile or employer category within a single fund structure.
                - Capability to calculate additional Bonus allocations for specific category of members , at 20 years and every 5 years thereafter.
        - Workflow Automation:
            - System-driven tracking for lifecycle status changes and processing events (e.g., divorces, maintenance court orders, disability, deaths).
        - Fund Accounting, Unitisation & Investment Controls:
            - Fund Accounting General Ledger: Built-in general ledger accounting capabilities natively tailored to institutional fund accounts, supporting direct ledger balancing or seamless synchronization hooks.
        - Real-Time Unit Pricing & Allocation:
            - Daily API ingestion of asset manager Net Asset Values (NAVs) to execute automated unitisation, unit pricing updates, and real-time member balance allocations.
        - Monthly Interest Processing:
            - Automated calculation and allocation of fund interest components or investment portfolio returns across past operational periods.
        - Membership Value Movement Validation:
            - Specialized administrative utility allowing users to generate, simulate, and audit membership value movements, asset balancing sheets, and individual growth factors across

customized, variable evaluation periods (e.g., specific date ranges or custom accounting windows).

- Benefit Calculations & Disbursals:
  - Exit Calculations: Automated quotes, projections, and final computations for life-stage events, exits, resignations, normal or early retirements, and retrenchments based directly on fund rules.
- Pensioner Payroll:
  - Monthly annuity payment processing engine, managing legislative tax withholding (SARS directives), payroll runs, and standard bank export file generations.
- Statutory Claims Management:
  - Structured lifecycle management, trace mapping, and documentation tracking for legislative distribution claims (e.g., Section 37C death cases).

- Specialized Components & Ancillary Features:
  - Two-Pot Retirement System:
    - Native structural support for the multi-pot model design, including automated initial seeding calculations, daily monitoring of accessible savings pot limits, tax directive execution parameters, and withdrawal processing rules.
  - Life-Stage Model Management:
    - Automated de-risking switching matrices based on member age or years remaining to maturity, executing rule-based asset portfolio transitions smoothly.
    - Individual requests for switching between portfolios
  - Fund-Backed Housing Loans:
    - Administrative tracking, of application, for housing loan guarantees ,calculation of amount available for guarantee under Rules of the Fund.
  - Funeral Policy Administration:
    - Group scheme member onboarding, automated premium reconciliation matrices, and seamless backend integration links with third-party insurers for rapid claim validation and automated payouts.
  - Trace & Communication Log:
    - Native CRM functionality tracking all outbound letters, SMS updates, emails, and member query lifecycles directly against individual profile IDs.

Part 9: Technical, Infrastructure & Systems Architecture

- **Systems Architecture Overview:**
  - Provide an exhaustive narrative and block diagrams mapping the layers of software infrastructure, data flow boundaries, and operational relationships between the User Interface (UI) layer, application runtime layer, core

calculation engines, integration gateways, and core transactional data storage engines.

- **ICT Infrastructure Architecture Overview:**
    - Detail definitive server-side physical/virtual infrastructure configurations, hosting topologies (Cloud SaaS, On-Premises, or Hybrid alternatives), compute hardware resource dependencies (vCPU cores), storage cluster/SAN guidelines, and baseline operating system requirements used within your environments.
- **Database Software Engine Framework:**
    - Specify the underlying database engine utilized by the solution (e.g., MS SQL Server, Oracle, PostgreSQL) and its horizontal/vertical scalability capabilities under high transaction volumes.
- **Version & Patch Management:**
    - Outline your release cycle for core software updates, emergency patches, and how updates are pushed without disrupting client-specific customisations or custom configuration branches.

Part 10: Investment Unitisation & Financial Modules

- **Daily Unitisation:**
    - Explain how your platform manages daily, real-time investment unitising for individual member accounts based on fluctuating asset prices.
- **The Computation and distribution of interest each month.**
    - If Unitising is not deployed, can the system compute interest on a monthly basis.
- **Real-Time Processing:**
    - Can the system dynamically process micro-transactions and calculate interim growth for intra-day exits?
- **Ledger Segregation:**
    - Detail how the system structures and maintains separate accounting ledgers for the fund's operational expenses vs. member asset pools.
- **3rd-Party Financial ERP Integration:**
    - Describe your platform's capability to integrate with third-party Enterprise Resource Planning (ERP) systems (e.g., SAP, Sage, Microsoft Dynamics, Oracle).
        - Detail the integration methods used (e.g., RESTful APIs, secure file transfers via SFTP) to synchronize general ledgers, accounts payable, and cashbook reconciliations.

Part 11: Employer Functions, Non-Contribution Management & Integrations

- **Employer Contribution Portals:**
    - Provide details on your secure web portal for participating employers to upload monthly contribution schedules (CSV/Excel formats) and log employee exit notifications with built-in real-time validation checks.
- **Billing & Contribution Schedule Allocation:**

  - Detail your native module importing employer payroll schedules, reconciling expected vs. received contributions, and auto-matching variances.
- **Automated Exception Reporting:**
  - Explain how the system generates real-time discrepancy logs detailing data mismatch items, unmapped member IDs, over/under payments, or critical structural formatting errors before schedules pass to the core ledger.
- **Payment Holidays & Approved Extensions:**
  - Describe the capabilities within your specialized administrative console to track, configure, and approve employer payment holidays, temporary partial funding states, or extended approved non-contribution scenarios. Confirm that the system prevents late-payment penalization routines during these legally authorized windows.

Part 12: Solution Banking, Third-Party ERP & Communication Channels data transaction management

- **Core Banking Platform Integration:**
  - Detail pre-built, secure host-to-host or API connections with South Africa's major clearing banks to support automated member payout processing, real-time validation of member banking details, and electronic fund transfers (EFTs).
- **Payment Portals:**
  - Provide a detailed explanation of any integrations with regional or international retail payment gateways (e.g., PayFast, Ozow, Netcash) for direct electronic payments
- **Third-Party ERP Interoperability:**
  - Confirm availability of certified connectors or bi-directional APIs designed to sync directly with market-leading corporate ERPs (e.g., SAP, Oracle, Microsoft Dynamics) for the automated exchange of trial balances, cashbooks, and ledger matching.
- **Financial capability:**
  - Does the system feature a built-in, proprietary sub-ledger financial accounting system capable of compiling and balancing ledger accounts in strict compliance with the formats, structures, and reporting regulations dictated by the FSCA?
- **Omnichannel Communication Engine:**
  - Detail native integration with online programmatic communication platforms to dynamically dispatch transactional alerts, benefit statements, balances, and operational notifications directly via SMS, MS Outlook (Email), and WhatsApp Business API.

Part 13: Stakeholder Portals, Reporting & Document Management

- **Member Online Self-Service:**
  - Describe your secure web portal and mobile application enabling active and deferred members to view personal profile details, historic contribution statements, investment choices, track claim statuses, model retirement

projections, update beneficiary profiles, and view live estimated pot values online.

- **Website & Portal Turnkey Development:**
    - Detail your framework for deploying client-branded, turnkey customized front-end websites and digital communication engines for trustee and member updates. Can the front-end look-and-feel (UI/UX) be completely modified using templates, custom CSS, and widgets while maintaining secure API communication with the core system?
- **CMS and Domain Hosting:**
    - Does your custom web site deployment support hosting on a client's custom domain (e.g., portal.gmrf.co.za)? Detail the content management tools available to the GMRF to update text, upload documents, and publish regulatory notifications independently.
- **Comprehensive Operational & Custom Reporting:**
    - Detail your built-in dashboard, report writing technology, and template engines providing comprehensive regulatory, custom operational, and accounting reports. Confirm if the system accommodates both highly optimized, print-ready paper layout definitions and high-density, filterable online interactive dashboards for power users and administrators.
- **Document Management System (DMS) Capabilities:**
    - Provide a detailed breakdown of how the platform natively stores, categorizes, metadata-tags, indexes, and secures member source documentation (e.g., identity documents, marriage certificates, beneficiary nomination forms, and court orders) or integrates with external repositories.

Part 14: Regulatory Compliance, Cybersecurity Frameworks & Local Integrations

- **Compliance information:**
    - Vendors must detail native compatibility , pension industry relevant statutory legislation, and international cyber security and cyberresilience, technical infrastructure and application security frameworks:
        - Core Statutory Compliance (Pension Funds Act No. 24 of 1956):
            - Confirm that your system design natively enforces compliance, automates audit tracking, and generates mandatory statutory reporting under the following specific sections of the Act:
                - Section 13A Contribution Tracking:
                    - Monitoring employer contribution timelines. The system must natively flag unpaid amounts past the legislated 7-day period, calculate statutory compound interest, and auto-generate compliance alerts for the Principal Officer.
                - Regulation 28 Portfolio Restrictions:
                    - Systemic enforcement of asset allocation limits (e.g., capping equity at 75% and offshore assets at 45%) at both fund-wide and individual

member investment selection levels, blocking non-compliant portfolio switches.

- Section 14 Asset Transfers:
  - Tracking execution workflows and statutory documentation for member transfers between funds. The system must securely log values, monitor certificate approvals, and prevent duplicate processing.
- Section 19(5) Housing Loans:
  - System-enforced compliance rules restricting fund-backed home loan guarantee values to legally permissible thresholds of a member's withdrawal benefit footprint.
- Section 37A & 37B Benefit Protection:
  - Systemic blocks ensuring member benefits cannot be attached by creditors, reduced, or assigned, except for legally permissible deductions.
- Section 37C Death Benefit Management:
  - Workflow logging, centralized documentation repository, and dependency tracking for trustees during complex death benefit investigations and allocation determinations.
- Statutory Returns Export:
  - Out-of-the-box export engines for annual financial statements, triennial valuations, and FSCA electronic quarterly returns.

- South African National & Institutional Integrations:
  - Provide detailed architectural explanations of native interface capacities with national endpoints:
    - SARS Integration & Tax Automation:
      - Real-time API interface for electronic tax directive applications. Direct secure data transmission to SARS using approved channels like Connect:Direct or Secured File Gateways.
- Automated Data Requests:
  - Native capabilities to systematically trigger data pull requests from SARS for external IT3 certificates (e.g., IT3(b), IT3(c), or IT3(f)).
- Automated IRP5/IT3(a) Generation:
  - Automatic compilation and generation of pre-populated IRP5/IT3(a) tax certificates following member withdrawals, separations, or transfers.
- DHA Identification Verification:
  - API integration with the Department of Home Affairs (DHA) for real-time member ID validation, biometric checks, and automated death master file updates.

- Data Privacy & Legislative Protection Compliance (POPIA / GDPR):
  - Demonstrate your strict systemic adherence to the Protection of Personal Information Act (POPIA), No. 4 of 2013 and, where applicable, the General Data Protection Regulation (GDPR):
- Lawful and Condition-Based Processing:
  - Explain how systemic workflows enforce accountability, processing limitation, and purpose specification boundaries to ensure member data is exclusively processed for authorized pension administration.
- Data Minimisation & Information Quality:
  - Natively restrict data input fields to what is strictly necessary. Provide details on automated tools that ensure member profiles remain complete, accurate, and regularly updated.
- Secured Data Minimisation & Retention:
  - Describe the automated rule engines used to enforce legal retention periods for retirement fund records. Detail the systemic capability to execute secure, unrecoverable data deletion or irreversible anonymization protocols once statutory retention windows expire.
- Data Subject (Member) Rights Access:
  - Detail turnkey functionality within the member portal enabling data subjects to securely request access to personal information, update demographic profiles, or request corrections/deletions of inaccurate history.
- Cross-Border Transfer Security:
  - If hosted or backed up internationally, explain how the system architecture explicitly complies with POPIA Section 72 and GDPR Chapter V cross-border transfer rules, proving data is bound to jurisdictions with equivalent or superior data protection laws.
- Breach Monitoring & Direct Notification:
  - Detail automated logging, structural telemetry, and immediate alert generation interfaces designed to support the Information Officer in identifying data breaches and compiling mandatory notifications to the Information Regulator and impacted members within legislated timeframes.

o Cybersecurity & Governance Standard Alignments:
- Confirm system structure compliance and alignment with the following security frameworks:
  - FSCA Cybersecurity Joint Standard: Explicit compliance with the FSCA/PA Joint Standard 2 of 2024 regarding Information Technology Governance and Cybersecurity Risk Management.
  - ISO Compliance Alignment: Formal alignment with, or certification under, ISO/IEC 27001 (Information Security Management System) and ISO/IEC 27701 (Privacy Information Management).

- NIST Framework Compliance: Structural adherence to the NIST Cybersecurity Framework (CSF) core functions (Identify, Protect, Detect, Respond, Recover) to actively safeguard sensitive retirement data.
- Data Security Technical Protocols: Detail technical mechanisms used for data encryption (AES-256 at rest, TLS 1.3 in transit), mandatory Multi-Factor Authentication (MFA) protocols for administrative, employer, and member portals via SMS OTP, email OTP, or authenticator apps, and granular role-based database permissions.

Part 15: Implementation, Operations & Lifecycle Governance Structures

- **Governance Framework:**
  - To protect fund assets and maintain absolute administrative control, the GMRF mandates a strict Joint Governance Framework spanning across the system's initial deployment and long-term operational lifecycle.
    - Joint Governance Committee Mapping:
      - Detail how your implementation and operational delivery models physically plug into and support the following mandatory organizational bodies:
        - Steering Committee (SteerCo):
          - Responsible for overarching governance oversight, scope boundaries, and ultimate financial approvals.
        - Project PMO (Project Managers):
          - Managing day-to-day delivery management and baseline coordination.
        - Operations Committee:
          - Driving runtime execution oversight and procedural quality control.
        - Incident & SLA Control:
          - Monitoring defect mitigation, systems availability, and ticket loops.
        - Change Advisory Board (CAB):
          - Authorizing configuration modifications, integrations, and database patches.
        - Technical Working Group:
          - Managing technology environments, API links, and lower-level code validation scripts.
- **Governance RACI Matrix: Roles & Responsibilities**
  - Please complete the matrix guidelines below by defining the exact allocation of baseline operational and transitional responsibilities expected from the Vendor and the Client (Fund) across implementation and ongoing operations:
    - Implementation Phase Responsibility Split
      - Vendor Responsibilities: [Vendor to specify key execution lines, e.g., ETL scripting, environment tuning, core code configurations]

            - Client (Fund) Responsibilities: [Vendor to specify expected client interaction boundaries, e.g., mapping approvals, rule configuration signing]
        - Operational Phase Responsibility Split
            - Vendor Responsibilities: [Vendor to specify core maintenance lines, e.g., third-level patch deployments, regulatory configuration tables]
            - Client (Fund) Responsibilities: [Vendor to specify daily operations boundaries, e.g., first-line profile management, clearing bank interface file approvals]
- **Staffing & Governance Resource Model:**
    - Detail your proposed staffing model, demonstrating how your personnel map into these essential structural roles:
        - Implementation Governance Roles: Detail staff quantities and capability frameworks:
            - Joint Project Sponsors (Shared Role)
            - Project Managers (Client PM & Vendor PM Roles)
            - Lead Solutions Architect (Vendor Role)
            - Data Migration Specialist (Vendor Role)
            - Business Analyst / Retirement Rules Engineer (Vendor Role)
            - User Acceptance Testing (UAT) Coordinator (Client Role)
- **Operations Governance Roles:**
    - Detail headcount allocations and role interfaces:
            - Account Executive / Service Delivery Manager (Vendor Role)
            - Principal Officer (Client Role)
            - System Administrators (Client Roles)
            - Information Security Officer (Client Role) & Cyber Incident Commander (Vendor Role - driving ISO/NIST/POPIA/Joint Standard compliance loops)

Part 16: Client Resource, Information & Logistical Requirements

- **Information Requirements:**
    - Vendors must specify the exact structural and operational requirements they expect the client to satisfy to ensure project success:
        - Outline necessary technical documents required from the fund at project kick-off (e.g., legacy database schemas, active payroll sample files, existing member policy rules, historical Section 37C legal templates).
        - Staffing Requirements (Implementation Phase):
            - Define the required client-side project team structure needed to match your methodology (e.g., part-time Subject Matter Experts, a dedicated Project Coordinator, and designated senior business owners for validation signoffs).
        - Staffing Requirements (Operational Phase):

            - Detail the recommended ongoing administrative headcount needed by GMRF to operate the system based on your tool's automation level for 2,000 members.
        - Logistical Requirements:
            - Specify any unique physical infrastructure or local access configurations required by the vendor's team to execute delivery (e.g., secure remote VPN profiles, dedicated on-site workshops in Germiston).

Part 17: Hosting, Infrastructure & Disaster Recovery

- **Deployment Options:**
    - Confirm if your architecture supports both SaaS/Cloud Hosting and On-Premises Deployment options for a 2,000-member scale.
- **Solution Image Replication & High Availability:**
    - Does the system provide full environment image replication to a secondary cold, warm, or hot site for Disaster Recovery Planning (DRP)? Detail backup frequencies and hot-site failover execution workflows.
- **Recovery Metrics:**
    - What are your standard architectural commitments and system capabilities regarding Recovery Time Objective (RTO), Recovery Point Objective (RPO), and Time to Repair (TTR) in case of primary infrastructure outages?

Part 18: Client System Requirements

- **User PC Specifications:**
    - Specify the minimum and recommended client-side user workstation hardware specifications required to run your workstation applications or web interfaces smoothly:
        - CPU (Processor) Core minimums:
        - RAM (Memory) minimums:
        - Storage space required:
- **Software & Browser Dependencies:**
    - List all mandatory client-side operating systems, required software frameworks (e.g., specific .NET versions), and supported desktop web browsers (e.g., Chrome, Edge) with minimum version numbers.

Part 19: Customer References & System Demonstration

- **References:**
    - Provide at least three verifiable customer references typed out on the respective customers' official company letterheads. References must be of a similar operating scale or larger (self-administered municipal/corporate funds or third-party retirement administrators).
- **System Demonstration Consent:**
    - Confirm that these three references have explicitly agreed to be contacted and are willing to host or participate in a live demonstration of your system in action for our evaluation team.

Part 20: Support Structure, SLA Levels & Costing Matrices

- **Services & Support Framework:**
    - Provide a narrative description of the support types offered (e.g., Dedicated Account Management, 24/7 Telephone Helpdesk, On-Site Technical Assistance, Ticketing Portal).
- **SLA Performance Tiers & Costing Matrix:**
    - Complete the standard SLA matrix below, outlining your commitments for response times, acknowledgment timeframes, and targeted resolution paths structured by issue impact classification. Specify what support service types are natively bundled within your base software fee structure versus items requiring professional service hourly rate drawdowns:

Priority Category	Target Response Time	Target Resolution Time	Support Service Type Offered	Included in Base License Cost? (Yes / No)
Priority 1 (Critical) System Down / Blocked Payouts	*E.g., < 1 Hour*	*E.g., < 4 Hours*	*E.g., 24/7 Dedicated Developer Support*	*Vendor to specify*
Priority 2 (High) Core Feature Impaired / Slow Unitisation	*E.g., < 4 Hours*	*E.g., < 12 Hours*	*E.g., Helpdesk Ticket Escalation loops*	*Vendor to specify*
Priority 3 (Medium) Minor Discrepancy / Portal UI Issue	*E.g., < 8 Hours*	*E.g., < 24 Hours*	*E.g., Standard Email Assistance*	*Vendor to specify*
Priority 4 (Low) Ad-Hoc Change / Report Request	*E.g., < 24 Hours*	*E.g., < 5 Business Days*	*E.g., Professional Services Allocation*	**No** (Billable at standard rate of: **R___________ / Hour**)

Part 21: Software & Hardware Licensing Responsibility Split

- Please explicitly clarify which entity pays for, provisions, and maintains core system dependencies by completing the structural summary table below. Differentiate responsibilities clearly between the Vendor and the Client (GMRF):

Component Category	Entity Responsible for Purchasing & Provisioning	Entity Responsible for Ongoing Maintenance & Patching
Hosting Infrastructure *(e.g., Cloud VMs, local server blades)*	*Vendor to specify*	*Vendor to specify*
Core Software Engines *(e.g., core administration application)*	*Vendor to specify*	*Vendor to specify*
Database & Security Licenses *(e.g., SQL server runtime keys, firewall tokens)*	*Vendor to specify*	*Vendor to specify*
3rd Party Integrations *(e.g., bank API channels, SARS direct gateways)*	*Vendor to specify*	*Vendor to specify*

Part 22: Pricing Estimates & Models (Baseline: ~2,000 Members)

- **Once-Off Implementation Cost Estimate:**
    - Provide an all-inclusive estimated cost for the deployment lifecycle from Project Initiation (Discovery) through to Go-Live and Handover (including the Hypercare period).
- **System Rental Model (SaaS / Cloud Opex Alternative):**
    - Detail your ongoing operational rental pricing framework. Specify if this is billed as a flat monthly operational fee or as a Per Member Per Month (PMPM) subscription fee. Explicitly state all recurring software maintenance, cloud storage allocations, and ongoing infrastructure upgrade elements included under this fee.
- **Procurement Price Model (On-Premises / Perpetual Capex Alternative):**
    - Detail the initial capital acquisition costs for an outright software license procurement. Provide the separate, mandatory annual percentage fee required under an Annual Maintenance Contract (AMC) to retain software update privileges.
- **Ancillary & Auxiliary Cost Overviews:**
    - Explicitly itemize any estimated implementation fees, data migration setup costs, custom portal layout development fees, or unique integration setup costs omitted from your base rental/procurement lines above.

Part 23: Preferred Payment & Costing Approach

- **Phased Implementation Milestone Payments:**
    - Confirm that all upfront setup and implementation costs will be billed strictly against the successful completion and formal sign-off of project phases (e.g., 20% on Scoping, 30% on Data Migration, 30% on successful UAT sign-off, and 20% on final Go-Live).
- **Implementation Project Retention holdback:**
    - Confirm your acceptance of a standard 10% financial retention holdback on all implementation milestone payments. This aggregated retention value will be released exclusively upon the successful conclusion of the 30-day Post-Implementation Hypercare stabilization period.
- **Monthly In-Arrears Operational Billing:**
    - Confirm that ongoing monthly operational charges (including per-member-per-month licensing fees, SaaS infrastructure hosting, and standard helpdesk support allocations) will be billed monthly in arrears.
- **Service Level Agreement (SLA) Financial Credits:**
    - Confirm your acceptance of standard service credit penalties if systemic performance levels drop. In the event of unresolved Priority 1 (P1) or Priority 2 (P2) system errors that breach the agreed-upon SLA response/workaround timelines, financial penalty credits will be calculated and automatically deducted from the subsequent month's in-arrears operational invoice.
- **Fee Escalation Caps:**
    - Specify your maximum annual percentage price escalation cap for recurring software licenses and technical support fees over a prospective 3-to-5-year contracting term.

Part 24: Confidentiality and Information Usage Undertaking to Vendors

- **Our Commitment:**
  - The Fund issues this binding undertaking to assure you ("the Vendor") that your proprietary commercial interests and data privacy will be robustly protected throughout this market-testing exercise, while allowing the Fund to transparently transition its functional requirements into a subsequent procurement phase.
- **Protection of Vendor Submissions**
  - Statutory Shield:
    - As a registered private body under South African law, the Fund formally undertakes to refuse any third-party requests for access to your RFI submission in accordance with Section 63(1) of the Promotion of Access to Information Act 2 of 2000 (PAIA). This applies to any trade secrets or sensitive commercial, financial, or technical information that would cause your firm commercial prejudice.
- **POPIA Compliance:**
  - The Fund is a "Responsible Party" under the Protection of Personal Information Act 4 of 2013 (POPIA). We strictly undertake to process all corporate, financial, and personal information of both natural and juristic persons solely for evaluation and research purposes, ensuring it is kept secure from unauthorized access or accidental leaks.
- **Restricted Internal Access:**
  - Your submission will only be accessible to the Fund's internal administrative staff, executive committees, appointed Actuary, and Board of Trustees who are directly involved in analysing the RFI responses.
- **Permitted Right of Use for Future Request for Proposal (RFP):**
  - Formulating Requirements:
    - By participating in this RFI, the Vendor acknowledges and agrees that the Fund will use the insights gained from responses to formulate the technical, operational, and functional specifications of a future Request for Proposal (RFP).
- **Mandatory De-identification:**
  - The Fund gives a strict undertaking that any specific proprietary workflows, unique pricing methodologies, system algorithms, or intellectual property contained in your submission will be fully anonymized, generalized, and de-identified before being translated into generic functional requirements for the RFP.
- **No Common-Law Infringement:**
  - Provided that the Fund complies with the de-identification standards above, the inclusion of such generalised functional characteristics in a subsequent RFP will not be deemed a breach of confidentiality, a violation of trade secrets, or an infringement of South African common-law intellectual property rights.

- **Statutory Overrides and Lawful Disclosures:**
  - This confidentiality undertaking will not apply to information that:
    - Is or becomes part of the public domain through no fault or breach of the Fund.
    - Is required to be disclosed by order of a South African Court or the Information Regulator.
    - Is lawfully demanded under regulatory oversight by the Financial Sector Conduct Authority (FSCA) or the Pension Funds Adjudicator

END