ANNEXURES

1.0 Technical Requirements:

Overview of the proposed platform
The proposed system shall contain the following technical requirements/functionalities, but not limited to:

- Admin/Supervisor management module; a system that is user friendly; helps the admin/supervisor to oversee each clerk (Data Capturer) work; manage users, assign work to clerks; Alerts overdue work or any stale job, document tracking and view system reports etc.
- Clerk (Data Capturer) module; have a checklist on documents and processes required before capturing school forms, user friendly interface, alert potential errors, view work summary and alerts on overdue work.
- Accountant module; facilitating payments by running pay sheet, verification of pay sheets, following up on payment outcomes and generate reports on payments made, payment requests, payment outcomes as and when required; payments audit trail.
- Data Manager; set amounts to be paid to schools, allocate resources and tasks, track requests and allocations, analyze each clerks work. Track status of each school (e.g. status of acknowledgement and acquittal) and obtain list of each status including, the list of rejected schools.
- Coordinator; overall supervision and monitoring of the processing of pay sheets. Accessing various reports for decision making. Approving pay sheets.
- Guest module; able to view only specific data reports generated by the system
- Integration; allow integration of existing EMIS data to SIG
- Easy to use, intuitive user-experience and interface.
- Easy management of users and school information.
- System should allow for easy administration of all components by the Super-User/Admin.
- Secure, using ISO standard security and encryption methods.
- Implement data validation for both client and server.
- Don't Repeat Yourself (DRY) principle in coding is recommended.
- Implement Search, Create, Read, Update and Delete (SCRUD) operations.
- Adopt Role-Based Access Control (RBAC) to authorize system resources allocation to users based on roles.
- Scalable[1] and upgradeable as and when the number of users and content increases.
- Maintain and ensure that the solution supports maximum concurrent users.
- The system should run optimally on a networked environment
- Image and other content customization features should be inbuilt within the system to allow standard content sizes (e.g. standard image sizes for easy uploading and processing).
- The system should allow uploading of imagery (JPEG), PDF files and FAT32 compression for storage and transmission of data.
- Provide user help functionality on major components

2.0 Password policy

2.1. Introduction
Usernames and passwords are utilized in order to access SIG. They also protect user data from unauthorized individuals, both internally (other staff) and externally (hackers).

2.2. Password changes
System should ensure users change their passwords periodically. The Systems Administrator should select an appropriate time frame for changing passwords.

2.3. Minimum password length
The length of passwords must always be checked automatically at the time that users x`construct or select them. The system must enforce passwords of at least eight (8) characters.

2.4. Complex passwords required
The system must enforce a password that contains at least:
-1 lowercase and 1 uppercase letter.
-1 special character (! @#$%^&*)
-1 number (0–9)

[1] Ability of a system to handle growth in data, users and modules

2.5. Limit on consecutive unsuccessful attempts to enter a password

The system should be able to prevent password guessing attacks, the number of consecutive attempts to enter an incorrect password must be three (3) unsuccessful attempts. The involved user account must be suspended until reset by the Systems Administrator.

2.6. Encryption

Passwords must always be stored in an encrypted format in the database. Developer must use universally accepted encryption standards that helps protect against the threat of malicious activity by performing real-time encryption and decryption of the database.

The developer shall also adhere to following security requirements:

- Information Security which is based on the following elements:
  - **Confidentiality** - ensuring that information is only accessible to those with authorized access.
  - **Integrity** - safeguarding the accuracy and completeness of information and processing methods.
  - **Availability** - ensuring that authorized users have access to information when required.
  - **Compliant use** - ensuring that the platform meets all legal and contractual obligations.
  - **Responsible use** - ensure appropriate controls are in place to enforce ethical and law-abiding behavior, conservation of common resources, and respect for other users within the system.
  - **Auto Backups** – the system should allow the administrator to create time frames for system auto backups or select an appropriate time frame for creating a backup when need arises.
  - **External Data** - the system should allow exporting of data using database tools such excel, text file, XML file, PDF or XPS, email and Access
- The software should provide audit trails and logs mechanism for content changes performed by system users.
- Maintain time series data so that certain information is not lost with passage of time and repeated updating.
- Handle session hijacking and session replay.
- Input validation to prevent attacks such as buffer over -flow, cross-site scripting and SQL Injection.

3.0 Responsibility

3.1 User

User refer to MoPSE officials:

- Shall ensure bi-weekly updates are reviewed and comprehensive requirement specifications are provided within review period.
- Shall maintain the delay register and notify the developer of all delays in writing; shall appoint the point of contact or project focal person(s).
- Inform the stakeholders and arrange for joint sessions with developers.

3.2 Developer

- Shall provide the management information system acceptable to user.
- Shall provide all details regarding licenses if required (based on selected solution).
- Shall maintain the delay register and inform the user on the delays.
- Shall appoint a project manager who shall be the point of contact; and
- Shall recommend suitable hosting environment (server specifications and similar) to host the portal safely and efficiently if necessary.
- Shall provide the system source code for the system as part of hand over – take over to the Ministry

4.0 Downstream Work: Warrant

Provide a two-year warranty after the user acceptance signoff. During this period, the developer is responsible for the following technical support:

- Update patches,
- Fix bugs,
- Make post-deployment changes to the system based on feedback from user experience.

5.0 Final test of the PV MIS and PV company MIS

The consultant will test the system using actual school data, to make sure the system work properly. The consultant will use the sample data which the PMO will provide to check the designed functions of system, including data entry, payment run, systems double check for grants to be disbursed, track on pending grants authorization, check list for schools on requirement of missing information, and print out required reports quarterly, biannually and annually.

5.1 Install the SIG system and train Ministry's staff

The consultant will install the system and train Ministry's staff in using the software. Training will be conducted at MoPSE head office. The consultant will be responsible for preparing training materials and conducting the training.

5.2 Install and test the Admin Module

The consultant will install the System and databases on the network, test and verify its proper operation and train the system administrator on major functionalities of the system.

6.0 Inception Report

The developer will assess the requirements and develop the inception report with time frames and requirements on financial payment modalities. The consultant will work closely with the MoPSE technical team to determine information to be stored, security arrangements; establish audit trails, data entry approaches, reporting requirements etc.

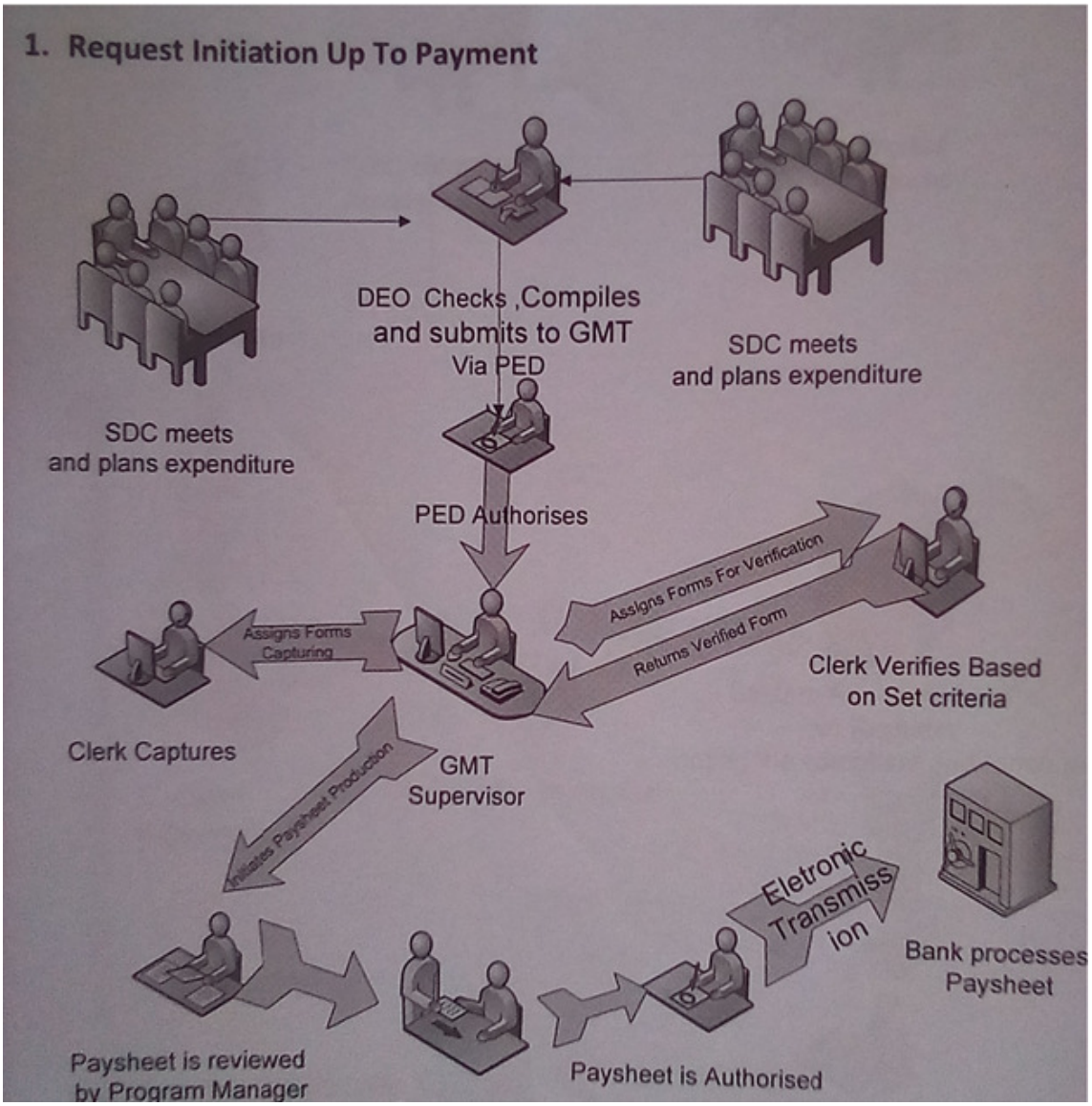
6.1 Provide System maintenance services

The developer will maintain the System and databases and upgrade as necessary, including providing troubleshooting services during the pilot run. This will include modifying the existing components and modules as and when required. This service will be required on an ongoing basis and immediately when errors are detected.

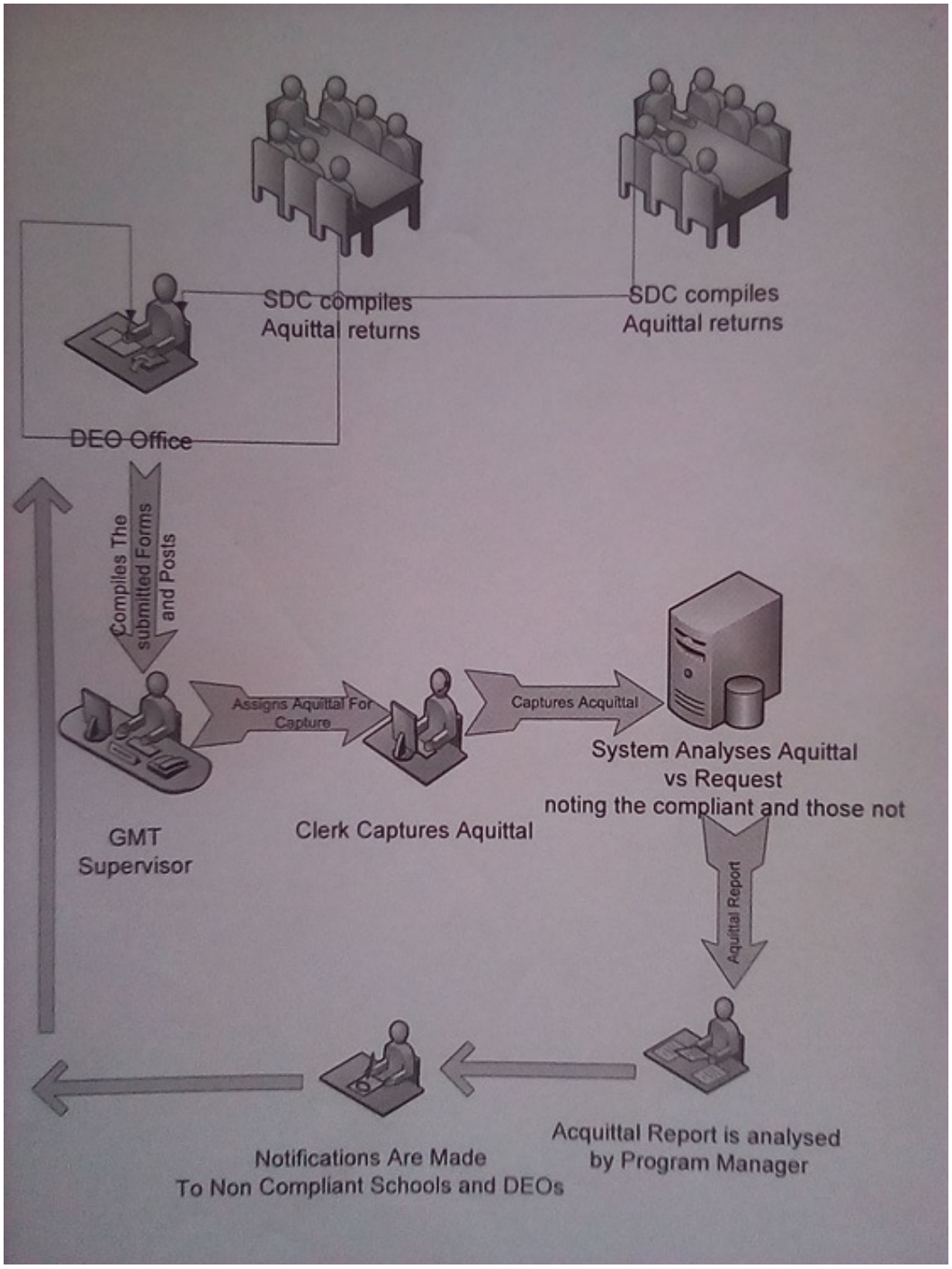
6.2 Computer hardware/software selection/installation/training

The developer will assist the MoPSE technical team in procuring and installing new hardware and software where necessary and in training MoPSE staff in using such software and hardware. The consultant will develop a reliable information security system including secure procedures for data entry, data storage and backup, and establishing data entry/change audit trails.

7.0 Basic Workflow Process



8.0 Flow of Acquittal submission



9.0 SYSTEM REQUIREMENT SPECIFICATION

- **Database**
  The database should be normalized. The system must encrypt user data, usernames and password stored in the database using Advanced Encryption Standards (AES).

- **Backup & Recovery**
  Backup of information is fundamental to the reliability and recoverability of the system. A documented backup plan which defines the backup routines of the system shall be provided. A backup plan aims at ensuring that information in backups is complete and sufficient.

The system should automatically perform regular backups of all critical items including; user data, system logs, reports and the database in an encrypted format. The backups shall be stored in an off-site storage location or preferably a secure cloud storage. The backups will regularly be tested to ensure integrity of the backups

- **Technology Transfer**
  The developer needs to engage with the ministry technical team during the project period and avail the system source code so as to harness the transfer of technology as minor corrections and support will be done in house.

- **Deployment of the system**
  The developer is required to come up with a schedule of activities highlighting milestones and expected deliverables such as; signing of contract, collecting user requirements, the different phases of system development, deployment and roll out. The developer should also support user in terms of stabilization and making the system acceptable by the end users.

- **Training**
  The developer is required to provide training to the users on the management and administration of the system including basic system maintenance. This is to provide an understanding of the system, its database and infrastructure configurations used during the implementation of the system. Training on basic maintenance is for the purpose of sustainability so that the system can be managed when the warranty expires.

- **Documentation**
  Content Design Document (high level design, data model), user manuals (including screenshots) and any other documentation of the assignment have to be completed and handed over to the user.

- **Technical Support**
  The developer shall render all support activities related to the following up until the warranty period expires:
  - Troubleshooting at both application level and user level,
  - Assist focal official/client in operation of the portal,
  - Fixation of bugs, incorporation of minor changes, etc.

- **Ownership of Source Code**
  The final product, all source code, intellectual property, documentation and all items specific to this product will be under the client's exclusive ownership. The duration of this project is 3 months