Tertiary Scholarship and Loans Board

"Building a Smarter Fiji"

DOCUMENT MANAGEMENT SYSTEM

BUSINESS AND TECHNICAL REQUIREMENTS

BUSINESS REQUIREMENTS

- Ability to capture, store and allow retrieval of records/documents of 25000 students, expected to grow at a rate of 5000 plus each year.
- Provide the above functionalities at three business locations: Suva (Head Office), Labasa (Northern Office) and Lautoka (Western Office)
- Allow access to documents for remote locations via online/web based modules
- Allow access from other TSLB softwares/systems such as accounting and HR systems.

TECHNICAL REQUIREMENTS

1.0 Record Capture

- Capture student document both automated (online application portal) and manual (scan and upload by TSLB staff)
- Capture all metadata elements and retain them with the record in a tightly bound relationship.
- Ensure that records are associated with a classification scheme, and are associated with one or more electronic files.
- Register the record by assigning it a unique identifier and documenting the date and time when the record entered the recordkeeping system.
- The system must maintain a logical relationship between the record and the transaction it documents.
- The system must allow a compound document to be captured as a single record.
- The system must allow a compound document to be captured as linked simple records.
- The system must support versioning.
- The system must be capable of capturing transactional documents generated by other systems. These include student invoices, payment vouchers and payment requisitions
- The system must be able to capture a variety of different types of documents. These must include records from on-line transaction processing systems (OLTP), databases, scanned documents, the most commonly used office documents and e-mail messages.
- The system must be integrated with the e-mail system, and e-mail must be captured and registered either by requiring that users capture selected e-mail and/or by providing an automated process for capturing the e-mail messages.
- The system must ensure the reliability of the capture process.

2.0 Classification Scheme

- The system must support and be compatible with TSLB's classification scheme – file numbers, Student ID numbers etc
- The system must automatically assign appropriate classification metadata to records and files and to classes within the classification scheme at the point of creation and capture.

- The system must ensure that the authorization to reclassify, add, delete or otherwise modify the classification scheme is carefully controlled and monitored.

3.0 Authenticity

- The system must maintain secure and inviolate records, including record content and metadata that documents content, context and structure.
- The system must ensure that records cannot be deleted by any means except as directed by a retention schedule.
- The system must undergo regular and systematic audits to verify system integrity.

4.0 Audit Trails

- The system must maintain audit trails for all processes that create, update or modify, delete, access and use records, categories or files of records, metadata associated with records, and the classification schemes that manage the records.

  At a minimum, it tracks:
  - *what data or information was accessed, added, deleted or modified;*
  - *who performed these functions; and*
  - *when they were performed.*

- The system must automatically capture the audit trail.
- The audit trail data must be unalterable.
- The audit trail must be maintained for as long as required by law or policy or to facilitate continued access to records.
- The audit trail must be logically linked to the records they document, so that users can review audit information when they retrieve records.
- The audit data must be available for inspection or export (without affecting vital audit trail data) by authorized users with little or no experience with the system.
- The system must maintain basic system documentation and audit trails of system modifications as long as they are required to facilitate continued access to records.
- The system must provide reports for actions taken on basis of audit trail data.

  The department or organization will determine what audit trail reports are needed and how they are organized. Possible reports include, but at not limited to, a chronological listing of activities for the entire system; a listing of activities involving an individual record, file, or class; a listing activities taken by a particular user; and a listing of activities taken at a particular workstation.

Since the volume will be quite large, on-line audit trail data may periodically be moved to off-line storage. Also, some audit trail data may be deleted once the records referred to are destroyed according to an approved retention schedule. In some cases, management may

decide that some activities do not need to be recorded. Notations about all of these issues and their results must be kept with the system documentation or within the audit trail itself.

5.0 Metadata

- The system must be capable of extracting metadata elements automatically from records when they are captured.
- The system must permit metadata values to be retrieved and captured from lookup tables or from calls to other software applications.
- The system must allow creators of records to enter manually pertinent record metadata that cannot be captured automatically.
- The system must support the validation of metadata that is entered by users, or metadata that is imported from other systems.
- Metadata must be logically linked to the records, files, and classes it documents, so that users can review metadata information when they retrieve records.
- The system must allow for the modification or reconfiguration of metadata sets, but the authorization to make changes must be restricted.

6.0 Security and Control

The system must include quality control mechanisms to ensure that consistent and accurate business records are created.

- The system must allow only authorized personnel to create, capture, update or purge records, metadata associated with records, files of records, classes in classification schemes, and retention schedules.
- The system must control access to the records according to well-defined criteria.

> *A user must never be presented with information that he or she is not permitted to receive. The criteria for access will vary according to the type of data or records contained in the system.*

7.0 Retention and Disposition

The system must include an automated, schedule-driven disposition management plan.

- The system must provide for the automated retention of records with long-term value in accordance with authorized and approved record retention schedules.
- The system must provide for the automated destruction of records in accordance with authorized and approved records retention schedules.
- The system must be capable of associating a retention schedule with all records, record metadata, files, or classes of a classification scheme.
- The system must automatically provide for the notification and approval of designated personnel in advance of disposition activities.

- The system must provide for the interruption of disposition activities on records or classes of records that have been or are expected to become the subjects of litigation.
- Within the system, every record in a file or class of records must be governed by the retention schedule associated with that file or class.
- The system must allow the administrator in charge of schedules to change or amend schedules associated with records at any point in the life of the record.

8.0 Preservation Strategies, Backups and Recovery

The system must incorporate a strategy or plan for backing up and preserving records.

- The system must ensure that records, components of records, audit trails, metadata, links to metadata or to files, and classification schemes can be converted or migrated to new system hardware, software and storage media without loss of vital information.
- The system must produce a report detailing any failure during a conversion or transfer and identifying records that were not successfully exported.
- The system must retain all records that have been exported until confirmation of a successful transfer process.
- The system must provide automated procedures that allow for the regular backup and recovery of all records, files, metadata, and classification schemes.

9.0 Access and Use

- The system must ensure that ALL records can be easily accessed and retrieved in a timely manner in the normal course of all TSLB business or for reference or secondary uses.
- The system must allow all record content and all record and file metadata to be searchable.
- The system must allow searching within an electronic file, across files, at any level in the classification scheme hierarchy.
- The system must ensure that all components of a record or file, including contents, relevant metadata, notes, attachments, etc., can be accessed, retrieved and rendered as a discrete unit or group and in a single retrieval process.

10.0 Documentation

- **System administrators must maintain policy and procedural documentation.**

The documentation should include at a minimum an overview of the purpose and uses of the system; policies and procedures for system operation and maintenance, quality control, security, testing, and records retention; and software/hardware specifications and operation.

- **Documentation must be**
    - **accurate and up-to-date.**

- **written clearly and concisely.**
- **readily available and accessible.**
- **retained according to a set retention schedule.**

11.0 System Testing

The performance and reliability of system hardware and software must be regularly tested. *The exact nature of the tests will depend on what is appropriate for particular hardware and software, and will be defined by system support personnel in conjunction with appropriate TSLB staff and Departments.*