5.0 PROCEDURE

5.1 FRS Document Requirements

The FRS document shall at minimum contain the following information. Other sections may be included which are individual requirements for a specific Project.

5.1.1 Each internally generated FRS is to be issued with a unique number.

5.1.2 If the FRS document is supplied by an external supplier, it is to be registered with a unique number.

5.1.3 The start of the document should provide:

5.1.3.1 The name(s), signature(s), date and position of the personnel involved in the preparation of the specification.

5.1.3.2 The name(s), signature(s), date and position of the personnel approving the specification.

5.1.3.3 Table of Contents.

5.1.4 An Amendment List must be included to document any changes made to the specification.

5.1.5 The management of changes should be clearly described. If for any reason the approved FRS is subject to change, the change control procedure must be used.

5.2 FRS Contents

The following steps (**Steps 5.2.1 to 5.2.7**) of this procedure detail the contents for each of the sections. For internally developed FRS documents, all sections shall be present, but if no requirement has been specified, then the section shall state “Not applicable”. For FRS documents supplied by external vendors, the equivalent information detailed in **Steps 5.2.1 to 5.2.7** should be included in the FRS.

5.2.1 Introduction

This section shall provide a brief description of the purpose of the FRS. This introduction should include the relationship to other documents.

5.2.2 Project Overview

5.2.2.1 Purpose and Scope of the Required System

Provide a brief description of the System, its installation site and intended use.

5.2.2.2 Objectives and Goals of Project

Provide any organizational goals and objectives to be met.

These requirements also apply to internal software development or modification.

5.2.6 Security Requirements

Security measures must be considered for the proposed System. Consideration must be given to the following:

5.2.6.1 Physical Security of Hardware

Include information regarding locking of computer hard drive, limited access to computer facility, etc.

5.2.6.2 Access

A hierarchy of permitted access to enter, amend, read or print data should be established based on job responsibility and authority. Include the number of security levels the system shall support; e.g. Operators, Supervisors, Administrator, etc.

Suitable methods of preventing unauthorized access should be available; example passwords, bar codes or automatic log off due to a specified number of log in attempts, etc.

Regular change of access codes must be in place possibly by means of an automatic prompt from the System.

5.2.6.3 Data

Security measures should describe who has authorized access to and/or alteration of data. The System should create a complete record (non mutable audit trail) of all entries and amendments to the database. This audit trail can either be manual or electronic (preferable) and must include identification of the original data entry, the new entry, the date of the change, by whom and reason for change.

Subject to the format and method of transfer of data, security measures are to be established to ensure integrity of the data whilst in use or archived. (Measures should be in place to ensure data is secured against theft, loss or alteration).

5.2.6.4 Software

Authorized access to software for modification.

5.2.7 Backup and Recovery Requirements

The requirements for Backup of data and Recovery from a System failure (includes power failure, communication breakdown between interfaces and equipment) need to be identified in this section. Issues which should be covered are: frequency of backup, adequate identification and storage of backup media, contingency plans if the system is not operational for an extended period of time.