Back Up and Disaster Recovery Policy

This policy is to ensure that all important documentation has been backed up and kept in a safe place by RGIT. All partner RTO’s of the RGIT are to supply RGIT with the RTO’s policy and procedure for Back up and Disaster Recovery.

All records related to training, as outlined in the Record Management Policy, will be kept in soft copies (with the option of hard copies). The following procedures have to be followed:

This procedure covers

- Secure data storage systems
- Student enrolment records and related forms
- Results of assessments
- Copies of issued qualifications
- Approved Recognition of Prior Learning
- Course Review records
- Resources developed by the RTO for delivery and assessment
- All training documents - including student enrolment records, RPL Applications, assessment documents, records of results, issued qualifications and Statements of Attainment, and developed resources for delivery and assessment purposes

Procedure
The RGIT IT Manager is responsible for:

- Reviewing the backup and disaster recovery system via regular audit.
- Ensuring secure storage of all student and administrative data. RGIT uses Wisenet, a complete student information management system for storage and access to its internal data.
- Disseminating relevant procedures, documentation and information to staff members to enable them to perform their designated duties via induction and regular staff meetings
- The maintenance and safe keeping of all quality records identified in this procedure, computerised and/or manual, via the use of a lockable filing system and password protected computer files

The RGIT Skills Vic Manager or nominee is responsible for:

- Establishing a centralised filing system for all manual and computer records.
- Backing up all computerised records and documentation on a hard drive daily. One hard drive is kept on site for daily update and another hard drive kept off-site for weekly update.