

| | |
|---------------------------------|--|
| Policy Reference Number: | 1.40 |
| Classification: | General |
| First Issued/Approved: | 9 June 2015 (Res. 487/2015) |
| Review Frequency: | After the general election – every 4 years |
| Last Reviewed: | |
| Next Review Date: | May 2019 |
| Responsible Officer: | Chief Executive Officer |
| Applicable Legislation: | |
| Relevant Policies: | |
| Related Procedures: | |
| Compliance Standard: | |

Introduction

It is imperative that Council's ensure that the internal controls surrounding the General Ledger are operating efficiently, as the financial information contained in the General Ledger is the basis of the financial statements and management reports.

Section 124 (1) of the Local Government Act states that '*a council must keep such accounting records as correctly and adequately record and explain the revenues, expenses, assets and liabilities of the council*'. Council can meet these obligations by developing and implementing effective internal financial controls in relation to the General Ledger.

Council should consider the following issues in relation to the General Ledger:

- Processing of accurate journals and effective review of such journals.
- Regular Balance Sheet Reconciliations that are reviewed independently.
- Adequate data security measures, including access controls and a formal disaster recovery plan.

Key Issues/Risks

In relation to the General Ledger, the major risks faced by Council is summarised as follows:

- General Ledger does not contain accurate financial information.
- Data contained within the General Ledger is permanently lost.

Segregation of Duties

The following segregation of duties should exist within the General Ledger cycle:

- Preparation of journals and Balance Sheet Reconciliations; and
- Review and approval of journals and Balance Sheet Reconciliations.

General Ledger Controls

Controls in place to prevent the General Ledger not containing accurate financial information include the following:

General Journals

General Journals are to be reviewed and authorised by the Deputy Chief Executive Officer who ensures the correct account allocation has been used and all other details on the journal are correct.

Before preparing a journal, a unique journal number is required to be obtained from the journal folder. This number is to be used as the general journal reference.

Each journal filed in the journals folder should have the following attached:

- A Council cover sheet.
- A print out of the batch that was loaded into SynergySoft.
- A print out of updating the batch in SynergySoft.
- Plus any additional supporting documentation.

Were possible, the duties of requesting the journal and processing the Journal should be segregated.

Once the journal has been posted into SynergySoft, journals are signed as being entered and filed to ensure that no journals are overlooked or posted twice.

General

All computer users are to have program access analysed in conjunction with their job descriptions to determine the appropriate access levels required to carry out their duties. Access to the General Ledger is restricted to approved personnel as per the Deputy Chief Executive Officer.

A separate supervisory password will be allocated to the Rates and Finance Officer for the purpose of system supervision tasks.

All new purchases of technology systems should be checked with the Rates and Finance Officer and the Deputy Chief Executive Officer, prior to purchase to ensure they meet Council's requirements and network capabilities.

Balance Sheet Accounts (including control and clearing accounts) are to be reconciled monthly and reviewed by the Deputy Chief Executive Officer. The clearing and suspense accounts are to be regularly cleared.

The chart of accounts is to be regularly updated to ensure correct account allocations are made.

Budgets are to be reviewed in compliance with Local Government (Financial Management) Regulation 9:

(a) at least twice, between 30 September and 31 May (both dates inclusive) in the relevant financial year (where at least 1 report must be considered before the consideration of the report under subregulation (1)(b), and at least 1 report must be considered after consideration of the report under subregulation (1)(b))—a report showing a revised forecast of its operating and capital investment activities for the relevant financial year compared with the estimates for those activities set out in the budget presented in a manner consistent with the note in the Model Financial Statements entitled Uniform Presentation of Finances;

(b) between 30 November and 15 March (both dates inclusive) in the relevant financial year—a report showing a revised forecast of each item shown in its budgeted financial statements for the relevant financial year compared with

estimates set out in the budget presented in a manner consistent with the Model Financial Statements.

Controls in place to prevent data contained in the General Ledger from being permanently lost include the following:

A formal Business Continuity Plan has been adopted by Council. The objective of this plan is to ensure that there is a set of clear and comprehensive instructions relating to the recovery of records, to ensure the minimum of loss and disruption of services in the event of an emergency or disaster.

Daily backup tapes for the main corporate computer system are to be kept in the Council office. Each day the daily backup tape from the previous day is taken to the Bendigo Bank for storage and each week a weekly back up tape is taken to the Bendigo Bank for storage.

FURTHER INFORMATION

This policy will be available for inspection at the Council offices listed below during ordinary business hours and available to be downloaded, free of charge, from Council's internet site: www.robe.sa.gov.au

Royal Circus, Robe SA 5276

Copies will be provided to interested parties upon request. Email council@robe.sa.gov.au

Any grievances in relation to this policy or its application should be forwarded in writing addressed to the Chief Executive Officer of Council.

POLICY REVIEW

This policy may be amended at any time and must be reviewed at least every four years since its adoption (or latest amendment).