Document #:6253247

POLICY

LOGAN CITY COUNCIL

Date adopted: 30/05/2017
File no: 860137-1
Minute number: 148/2017

Policy title: **ELECTRONIC FUNDS TRANSFERS AND ONLINE BANKING SYSTEMS**

Directorate: ORGANISATIONAL SERVICES

Branch: FINANCE

Policy objective: To provide a framework for the control and administration of Council's electronic funds transfers and online banking systems.

Policy scope:

This policy is designed provide reasonable assurance of the accuracy and suitability of Council's electronic funds transfers and online banking systems by addressing key process, application, approval and audit controls.

The policy will address the following through the administrative procedure:

1. There is to be a separation of duties between key functions, inter alia payment approval, processing, remittance and confirmation.
2. There is to be restricted access to banking processes by limiting work stations and through password control.
3. There is to be approval, according to Council's delegation of authority 'Authorisation of Expenditure', prior to funds transfer and independent confirmation after transfer has been completed.
4. There is to be a documented approval and review procedure for processing exceptions and interruptions.
5. There are to be independent bank reconciliation and audit trail records.

Definitions:

TERM	DEFINITION
EFT	Electronic funds transfer

Policy statement:

Administrative procedures

1. <u>Accounts payable</u>
   (a) Council encourages payment of supplier accounts by EFT, although cheque payments are permitted.
   (b) Supplier invoices are only released for payment once approved per Council's delegation of authority for Payments and based on confirmed service completion and/or delivery.

(c) The Accounts Payable Supervisor ensures that invoices released for payment are in accordance with Council's payment terms and conditions specified in Council's Accounts Payable system and policy.

(d) One off payments are processed on completion and approval of a "Miscellaneous Payment Form".

(e) Accounts Payable officers reconcile supplier statements to individual supplier records monthly including payment validation. The Accounts Payable Supervisor reviews supplier reconciliations monthly.

(f) Accounts Payable officers generate and sign a proposed payment report for EFT payments for approval by cheque signatories.

(g) An authorised Funds Transmission Log is given to the Banking Officer by Accounts Payable.

2. Pay office

(a) Staff payments are processed by EFT only, direct to a nominated bank account.

(b) Staff payments are restricted to existing employees based on pay conditions administered by the People and Culture branch and recorded in Council's pay system.

(c) Any variation to pay terms and conditions is approved by the People and Culture Manager and entry restricted to People and Culture branch passwords.

(d) The Pay Office has responsibility to the Finance Manager and does not have access to create or amend employee pay rates or terms and conditions.

(e) Fortnightly pay amendments (e.g. for overtime or higher duties) are recorded to timesheets authorised by Council management.

(f) Payroll officers process the fortnightly pay run.

(g) The Payroll Administrator undertakes a payroll reconciliation to validate the accuracy of net pay amounts and completes a "Certificate of Preparation and Checking of Payroll" (pay certificate) for the pay period.

(h) The pay certificate is provided to the Chief Financial Officer for approval per Council's delegation of authority "Authorisation of Expenditure".

(i) An authorised Payroll Transmission Log is given to the Banking Officer by the Pay Office.

3. EFT payment

(a) A separate detailed banking procedure is maintained by the Financial Accounting section of Council (document ID 6133445 - Bank EFT Procedure)

(b) Creditor payments - Authorised Funds Transfer Transmission Log is given to Banking Officer by Accounts Payable.

(c) Payroll /Wages payments - Authorised Payroll Tranmission Log is given to Banking Officer by Pay Office.

(d) Banking Officer:

(i) Check requests are fully authorised.

(ii) Open Commonwealth Bank Commbiz. https://login.commbiz.commbank.com.au

(iii) Sign in using unique customer sign in and password

(iv) Click on "File Transfer" tab and import

(v) File type " Direct Entry "

(vi) Click on "Browse" and select the drive and path for the file type you are transmitting and click on open

(vii) Click "Set file as modifiable"

(viii) Import file

(ix) F5 to update "Import Status" - Awaiting Confirmation

(x) Select file - click on Proceed with Confirmation

(xi) Select file, check amount balanced and submit and check processing date is correct, and corrct if necessary

(xii) Click confirm

(xiii) Click OK

(e) 2nd Authorising Officer:

(i) Open Commonwealth Bank Commbiz https://login.commbiz.commbank.com.au

(ii) Sign in using unique Customer sign in and password

(iii) Click on Outstanding Austhorisations

4. EFT confirmation

Banking officer to print off Payment File Reports the next business day

(a) Sign on to Commbiz https://login.commbiz.commbank.com.au

(b) Click on Receivables tab and "Transaction Group Status List"

(c) Processing Date - Exact : Date of transactions

(d) Click on Search

(e) Click on "Print Page" top RH corner under Commbiz

(f) Print number of copies required

(g) Check amounts, and attached report to back of paperwork

(h) Check amounts agree to Bank Statement

(i) Give paperwork to Controls Officer

5. Bank reconciliation and audit trail

(a) The Controls Officer:

(i) Undertakes daily bank reconciliation.

(ii) Confirms EFT transfer amounts processed through the bank statement to the approved payment report/Pay Certificate.

(iii) An audit log is produced confirming operator, date and time and transaction details and is retained in a secure location on Council's network for audit purposes.

(iv) Amendment and delete access to audit trail reports is restricted to the Systems Administrator.

(b) The Systems Administrator is to undertake independent review of system audit logs.

6. Access controls

(a) Access to Council's online banking system is to be restricted to Council's Banking Officer in the first instance, Council's Financial Accountant and one other independent backup operator.

(b) Operators are to be allocated unique password and user identities to enable operator verification on audit trail. Passwords are to be memorised and not disclosed to other personnel.

(c) Banking workstations are to be located within the Finance branch and are to require logon after 10 minutes inactivity.

(d) Banking workstations are not left unattended while signed into online banking.

(e) Operators are to follow bank operating and security procedures, as per Council's banking services provider, when using online banking.

Related policies/legislation/other documents:

DOC ID	DOCUMENT TYPE	DOCUMENT NAME
8745519	Delegation of Authority	Authorisation of Expenditure
1502858	Application Form	Miscellaneous Payments Form
6133445	Procedure	Bank EFT Procedure