Invoice Fraud Policy

Policy Details

Policy Category	Council Policy
Date Adopted	17th January 2023
Resolution Number	0124/012
Approval Authority	Council
Effective Date	17th January 2023
Policy Version Number	1.0
Policy Owner	Director of Corporate Services

Supporting documentation

Legislation	• Local Government Regulation 2012
Policies	• Cyber Security Policy
Delegations	• Nil
Forms	• Electronic verification; or • Bank Statement
Supporting Documents	• Nil

Version History:

Version	Adopted	Comment	eDRMS #
1.0		Council Resolution # - Initial Implementation	

Contents

This policy is applicable to

All executives, accounts payable employees and contractors of Carpentaria Shire Council.

Invoice fraud and how it works

Invoice redirection fraud is as simple as it is dangerous. A scammer will pose as a legitimate supplier and then request payment to a bank account they control. In order to make the invoice look legitimate, the scammer may have hacked your or your supplier's computer systems. The invoice may even come from a supplier's email address (if that's been hacked) or more likely from some subtle variation of it. Often, you won't know there's a problem until your supplier starts chasing you for the payment they haven't received.

Council needs to be extra vigilant to avoid:

- accidentally paying a fraudulent invoice, or
- being impersonated to their clients/customers and having their clients paying the fraudster instead of them.

Invoice fraud is a financial scam where someone steals, or attempts to steal, money from the Council. This can be done by someone external to our business like a scammer, or it could be a malicious employee with knowledge of our business operations.

The main objective of the scammer is to steal money by:

- tricking our accounts payable staff to change the bank account details of one of our existing suppliers to the details of a bank account they control, or
- tricking our accounts payable staff to pay a 'fake' creditor's invoice to a bank account they control.

Procedures to protect Council

The following procedures have been implemented to equip our employees to protect the council from invoice fraud. These procedures MUST be adhered to at all times without variation despite what pressure tactics maybe applied to employees to take actions that will lead to financial loss.

1. **Verify new details**

   If Eftsure is used to onboard new creditors, the system will independently verify business and account details.

   When adding a new creditors' company details manually, specifically their bank account details, always verify the details with a known employee of the creditor.

   NEVER use the communication instructions on a suspected fake invoice or the accompanying email or letter. CALL, not email, the new creditor using a phone number we have verified or a phone number we have used for them previously.

2. **Verify changes**

   If using Eftsure, no business or account detail changes are accepted via email, phone or in person.

If the changes will be made manually, when a request is made to change or update a creditor's bank account details, ALWAYS verify that:

1) the request to change or update the bank account details was actually requested by the creditor, and if so
2) the new bank account details are correct, with a known employee of the creditor, and
3) request a copy of the supplier bank statement showing the bank account details, account name, bsb and account number.

When verifying this information with the creditor, NEVER use the communication instructions provided on the invoice, email, or letter that requested the bank account details to be changed or updated. Look for verification of the bank details, that does not involve the party requesting the change of details.

CALL, not email, the new creditor using a phone number we have verified or a phone number we have used for them previously.

Other ways of verifying if you do not know an employee are to visit the website of the business for contact details, or if a large payment contact procurement and review contract details where the tender was submitted.

All manual verification must be double-checked by the direct supervisor (Senior Finance Officer, Manager of Finance and Admin)

3. Cross reference match

If using Eftsure, before processing a creditor pay run, the ABA file is uploaded in Eftsure to verify the account details from our synergy records. Any red flags are investigated before proceeding with payment and uploading the ABA file in Westpac.

If a manual process is used, all invoices must be cross reference matched to an approved purchase order before ANY payment is made. If the invoice cannot be cross reference matched, refer the matter immediately to your direct supervisor for further investigation and guidance.

4. Be vigilant for irregularities

The accounts team, when receiving requests to change bank details, are trained to look out for:

- slightly changed email addresses
- altered invoices, especially those with graphics of inferior quality
- different or mismatched fonts in the body of the email and invoice
- unusual or lower quality English in emails or on invoices.

5. Permissions of least privilege

Finance will limit the number of people with permission to change supplier bank details, and employees will have permissions of least privilege, so will only have access to what they need to perform their duties.

What to do if you become aware of fraud

Should you become aware of or have a suspicion about any activity that may lead to fraud please refer it immediately to your Manager or Director.

Adopted by Council on 17 January 2024 by Resolution 0124/012.

Mark Crawley
Chief Executive Officer