

Payment & Invoice Verification Policy

Stops invoice fraud and business email compromise · SMB1001 Silver.

Most money lost by small businesses to cybercrime is lost through payments, not hacking. This policy makes verification the normal, required way we handle payments and supplier bank details at [Business name].

The rules

- **Verify by phone.** Any request to change a supplier's bank details is confirmed by phoning the supplier on a number from our own records — never a number from the email or invoice.
- **Urgency rule.** A request that is urgent, confidential, or 'can't follow the normal process' gets more scrutiny, not less. We are allowed to make anyone wait for a callback.
- **Two sets of eyes.** Payments above set amounts need a second approver (see the Payment Authority Matrix).
- **Write it down.** We record the date, who we spoke to and what was confirmed for every bank-detail change.

Bank detail change — the 7 steps

1. **STOP.** Don't action any change from an email.
2. **CHECK your records.** Find the supplier's number in your own files.
3. **CALL.** Confirm the request verbally.
4. **RECORD.** Date, time, who you spoke to, what was confirmed.
5. **GET APPROVAL.** Owner or a second authorised person signs off.
6. **UPDATE RECORDS.** Note the new details and the verification date.
7. **NEVER pay** to new bank details before completing steps 1–6. No exceptions.

Policy owner: _____

Reviewed (date): _____

Make it yours (with AI)

I run a [type of business] in [town], Australia, with [number] staff. Rewrite the policy below so it fits how my business actually works, in plain English my team will read. Keep it to one page. [paste the template]

Two rules: start a fresh chat, and never paste real customer names, bank details or staff records into a free AI tool.