CAMPUSGUARD®

Vendor Verification Checklist

Prevent payment fraud and invoice scams by verifying vendor details before processing requests. Review our checklist for actionable steps to verify vendors.

☐ Email & Domain Validation

- Does the sender’s email match the official vendor domain exactly (no misspellings or substitutions like “vend0r.com”)?
- Is this the same email/contact you’ve used in previous, verified communications?
- Hover over links and check the actual destination before clicking.

☐ Invoice & Document Review

- Does the invoice match the standard format (logo, layout, payment terms)?
- Is the invoice number consistent with previous sequences?
- Are there changes in the bank account or contact details? (Flag for extra review and approval.)
- Does the invoice reference an actual product/service received and a corresponding purchase order?

□ Direct Confirmation

- Did you verify the request (especially changes to banking information or urgent payment requests) using a known contact method, such as a previously used phone number, rather than via the email in question?
- Did the requestor provide enough context (e.g., recent activity, contract reference) to justify urgency?

□ Cross-Check Internally

- Has someone else in your department or procurement team approved or seen this request?
- Is this vendor still active or under contract?
- Are they flagged in any known fraud bulletins or internal alerts?

□ Red Flag Review

Watch out for:

- Urgency or threats (“Pay now or lose service”)
- Requests outside of normal business hours or processes
- Grammar/style inconsistencies compared to previous emails
- Pushback when asked to verify through another channel

When in doubt, pause, verify, and escalate. Fraudsters rely on rushed decisions.

A quick double-check can stop a costly mistake.