BlueCrest Accounting Solutions

ABN 88 904 505 485 | bluecrestaccounting.com.au

DATA SECURITY SUMMARY

Effective 12 June 2026

How We Protect Your Client Data

This document answers the security questions most commonly asked during onboarding.

■ Encryption

- AES-256 encryption at rest
- TLS encryption in transit
- Google Workspace infrastructure
- 99.9% uptime SLA (Google)

■ Access Control

- Two-factor authentication (2FA) mandatory
- Role-based, need-to-know access only
- Password reset on suspected compromise
- Auto logout on inactivity

■ File Transfer

- Files shared via dedicated Google Drive folders
- One folder per client — no email attachments
- Folder access revoked on engagement end
- Version history: 30 days / 100 versions

■ Staff & Confidentiality

- All staff sign Confidentiality & NDA
- Strict no-personal-device policy
- No data outside authorised systems
- Supervised, access-controlled environment

■■ Data Retention & Disposal

- 7-year retention per ATO requirements
- Secure deletion within 10 business days
- on request after engagement end
- Purpose-limited — no secondary use

■ Incident Response

- Internal assessment within 2 hours
- Client notification within 2 hours of confirmed breach
- OAIC notified as required by law
- Full incident report within 24 hours

■■ Regulatory Compliance

- Australian Privacy Act 1988 (APPs)
- APP 8 cross-border disclosure
- India DPDP Act 2023
- ATO & ASIC record-keeping standards

■ Cross-Border Transfer

- Delivery team based in Ahmedabad, India
- Data processed under contractual safeguards
- APP 8 compliant transfer protocols
- Google Workspace AU/global data centres

Questions about our security practices?

compliance@bluecrestaccounting.com.au | +61 2 8006 6770 | bluecrestaccounting.com.au/data-security/