

How Collar Assist Protects Your Data

Collar Assist handles bookkeeping, tax, payroll, and compliance data for US businesses. This overview summarises the controls, restrictions, and audit habits we apply to every client account.

Information Security Controls

- **Restricted, role-based access:** client data is visible only to the team members assigned to that account, with every access event logged.
- **Firewall and antivirus protection:** enterprise-grade firewall and continuously updated antivirus on every workstation.
- **Encrypted data transfer:** files move over encrypted, access-controlled channels. No ad hoc email attachments or personal cloud links.
- **Blocked removable media:** USB ports and external drives are disabled on workstations handling client records.
- **No personal email or unmonitored web:** production machines are limited to what the work requires.
- **Continuous activity monitoring:** workstation activity is logged and reviewed on a regular cycle.

Physical Security

- Manned entry points with round-the-clock CCTV coverage
- Access-controlled production floor, entered only with an authorised card
- A separately secured server room, entered only by IT staff
- No CD, DVD, or removable drives on any client workstation
- Locked storage for any physical records still in transition to digital

Data Handling

- Need-to-know access, scoped to the individuals working your account
- Signed confidentiality agreements before anyone touches a live file
- Defined retention periods, with secure archival or destruction after use
- Client-by-client segregation, never mixed in shared folders or templates
- Written incident response steps with a fixed resolution timeline

People

- **Background checks before hiring,** required for anyone with access to client financial data.
- **Signed NDAs without exception,** in place before onboarding to any client account.
- **Ongoing security awareness training** on data handling policy and phishing recognition.

Our Approach to Data Protection

We hold ourselves to a high standard for how client data is collected, stored, and protected, and we keep strengthening that programme as we grow.

DATA PROTECTION PRACTICE

GDPR-aligned data handling

- Data minimisation, collecting only what a service genuinely requires
- Defined data retention and secure deletion schedules
- Client data segregation across every account we manage
- A named point of contact for any data protection query

ONGOING GOVERNANCE

Reviewed, tested, and retrained

- Regular internal reviews of access permissions and security policy
- Periodic incident response testing across the team
- Refresher security awareness training for all staff
- Ongoing risk review of any vendor or software we rely on