Security Overview

How ExecWing protects client data. Version 1.1, October 2026.

Summary

ExecWing places dedicated assistants based in the Philippines, Mexico and Colombia with US businesses in all 50 states and Washington, D.C., on a part-time or full-time basis (typically 20- or 40-hour workweeks). Assistants work inside client systems under client-controlled access. This overview describes our practices. It is not a certification or audit report.

Access control

- Named user accounts for every assistant. No shared logins.
- Least-privilege roles set with the client during onboarding.
- Multi-factor authentication required on every system that supports it.
- Credentials shared through a password manager, never by email or chat.
- Same-day access revocation and credential rotation at offboarding.

Devices and workspace

- Updated, supported operating system with automatic updates.
- Full-disk encryption, screen lock and endpoint protection required.
- No client data stored on personal or removable storage.
- Private, quiet workspace; backup internet connection and backup power required.

People

- Multi-stage vetting: skills tests, English assessment, structured interviews.
- With written candidate consent: government ID verification, a police clearance (an NBI clearance in the Philippines, or the national equivalent in Mexico or Colombia) and at least two references.
- Signed confidentiality and data-privacy agreements before any client access.
- Security and privacy training (including phishing awareness) completed before placement.

Data handling

Client data stays in client systems wherever possible. Assistants do not use public AI tools with client data unless the client approves in writing. ExecWing personnel are located in the United States, the Philippines, Mexico and Colombia, and data may be accessed from these countries under contractual safeguards. We draw on the NIST Cybersecurity Framework and the data-protection law of each assistant's Delivery Country: the

Philippine Data Privacy Act of 2012 (RA 10173), Mexico's LFPDPPP or Colombia's Law 1581 of 2012.

Financial data (bookkeeping)

- Bookkeepers never hold or store online banking credentials.
- Separation of duties: bookkeepers prepare payments, clients approve and release.
- Vendor bank-detail changes verified through a known contact.
- ExecWing does not provide tax preparation, tax filing, attest or CPA services.

Health data

For medical administrative placements we sign a HIPAA Business Associate Agreement before any access to protected health information, apply minimum-necessary access, and prohibit local storage of PHI. Assistants perform no clinical work.

Contracts available

- Master Services Agreement and Order Form
- Data Processing Addendum
- HIPAA Business Associate Agreement (when applicable)
- Bookkeeping Services Addendum (when applicable)

Compliance status and roadmap

ExecWing is an early-stage company. We do **not** hold SOC 2 or ISO 27001 certification today and do not claim to. A SOC 2 readiness effort is on our roadmap; we will update this document if and when an independent audit is completed. We are glad to complete your security questionnaire.

Contact

Security questions or incident reports: hello@execwing.com. More: execwing.com/trust/

General information only; not legal, tax or compliance advice. Terms of any engagement are set by your Master Services Agreement and related addenda.