

Security working brief

A discussion guide for your scoped engagement.

Ownership

Use client-owned repositories, systems, and credentials. Define IP assignment on payment and the documentation needed for handover in the agreement.

Access and changes

Agree least-privilege permissions and change approvals before onboarding. Platform release branches use reviewed pull requests, not direct commits.

Data handling

Define approved storage, candidate data and footage access, purpose, transfers, retention, return, and deletion. Confirm applicable Indian and US privacy obligations with counsel.

Recruiting boundaries

Use approved scripts and outreach channels. Define consent and opt-out handling. Employers retain hiring and adverse-action decisions; checks stay with authorized providers. No timekeeping edits.

Incident and exit plan

Agree escalation contacts, notification responsibilities, service coverage, access revocation, and knowledge transfer. A 30-day exit notice is proposed, subject to the signed scope.

Evidence and review

Request relevant controls and documentation before signing. No SOC 2, ISO 27001, or other certification is asserted by this brief. Website targets are not historical results.

Proposed working principles. Review with counsel. Final commitments are in the signed scope.

Foldtech Technologies | October 2026 | Not a certification or legal opinion.