COMMERCIAL SECURITY / 01

BUILD A FACILITY-SERVICE BRIEF

Organize high-level facts without exposing sensitive details or designing a system.

A helpful preparation resource from PickYourPro.ai. Fill in digitally or print. Keep your completed copy private.

Facilities, general areas, entrances, operating hours, occupancy patterns, and business constraints

Access groups, visitors, deliveries, after-hours users, and accessibility needs to discuss

Observed events or service needs, including general area and timing, without assigning a threat level

Existing cameras, alarms, access mechanisms, intercoms, lighting, monitoring, or other systems

Known network, connectivity, power, cabling, account, contract, landlord, or ownership context

Authorized decision-makers and facility, IT, privacy, HR, accessibility, insurance, or emergency-access stakeholders

Preparation only. Not a risk, vulnerability, privacy, accessibility, cybersecurity, or compliance assessment; security design; emergency procedure; product recommendation; or legal guide. Keep sensitive security details private.

COMMERCIAL SECURITY / 02

DEFINE A COMPARABLE SYSTEM SCOPE

Ask each provider to document its proposed work, dependencies, and exclusions.

Provider-proposed site review and information needed before confirming scope

Areas, events, access needs, devices, software, and coverage objectives the proposal addresses

Installation, cabling, network, connectivity, power, mounting, restoration, and other dependencies

Recording, storage, monitoring, alerts, integrations, accounts, permissions, and administration included

Testing, training, documentation, maintenance, support, updates, replacement, and escalation included

Equipment, software, data, recording, account, configuration, documentation, and handoff ownership

Preparation only. Not a risk, vulnerability, privacy, accessibility, cybersecurity, or compliance assessment; security design; emergency procedure; product recommendation; or legal guide. Keep sensitive security details private.

COMMERCIAL SECURITY / 03

PROTECT ACCESS AND PLAN HANDOFF

Use approved private channels and assign every responsibility in writing.

- [ ] No codes, passwords, keys, tokens, or credentials are in the request
- [ ] No sensitive floor plans, blind spots, or vulnerabilities are in the request
- [ ] No private recordings, personnel records, or visitor data are attached
- [ ] Site review and stakeholder approvals are provider-proposed and documented
- [ ] Account, equipment, data, and recording ownership is clear
- [ ] Testing, training, maintenance, and support responsibilities are clear
- [ ] Changes and recurring terms require written authorization
- [ ] Handoff and end-of-service access removal are documented

Approved process for private site details, accounts, permissions, recordings, logs, and stakeholder review

Authorized administrators, approval roles, escalation contacts, and change-control process

Completion records, diagrams, inventory, configuration documentation, training, warranties, and transition materials promised

Preparation only. Not a risk, vulnerability, privacy, accessibility, cybersecurity, or compliance assessment; security design; emergency procedure; product recommendation; or legal guide. Keep sensitive security details private.

COMMERCIAL SECURITY / 04

QUESTIONS FOR A SECURITY PROVIDER

Record how this provider would review, scope, administer, support, and hand off the system.

Site review: what information and stakeholder input are needed before confirming the proposal?

Scope: what devices, software, installation, configuration, integrations, monitoring, and recording are included or excluded?

Dependencies: what network, connectivity, power, cabling, account, access, landlord, or other work is assumed?

Governance: how are permissions, privacy, accessibility, ownership, approvals, and sensitive information handled?

Operations: what testing, training, documentation, maintenance, support, updates, escalation, and outage handling are included?

Terms and handoff: what can change, recur, renew, cancel, transfer, remain, or be removed, and how is that documented?

Preparation only. Not a risk, vulnerability, privacy, accessibility, cybersecurity, or compliance assessment; security design; emergency procedure; product recommendation; or legal guide. Keep sensitive security details private.

COMMERCIAL SECURITY / 05

COMPARE THE SAME SECURITY SCOPE

Use A and B in every box. Clarify differences before choosing.

Provider A / Provider B / site-review and proposal dates

Proposed coverage, equipment, software, installation, integrations, monitoring, recording, and exclusions - A / B

Ownership, permissions, administration, dependencies, testing, training, maintenance, support, and handoff - A / B

Proposal total, recurring terms, assumptions, possible changes, written terms, and open questions - A / B

READY TO HEAR FROM PROS?

Create an account on PickYourPro.ai and start a Commercial Security Systems request. Share only high-level facility, operating, access-group, observed-event, existing-system, timing, and requested-outcome information so participating pros can compete with proposals. Keep sensitive layouts, vulnerabilities, credentials, codes, recordings, and personnel information out of the request. Compare proposed site review, system scope, responsibilities, ownership, support, recurring terms, documentation, and fit.

One request. Every pro's best offer.

Start a request

Participation varies. A site review and authorized stakeholder conversation may be needed before a final system proposal.

Planning guide: https://www.pickyourpro.ai/services/commercial-security

CISA: Security Planning Workbook (official reference)

CISA: Physical Security Resources (official reference)

Preparation only. Not a risk, vulnerability, privacy, accessibility, cybersecurity, or compliance assessment; security design; emergency procedure; product recommendation; or legal guide. Keep sensitive security details private.