CMMC Level 2: Physical Protection Evidence Planning

Visitor evidence checklist and suggested pack structure | Reviewed October 30, 2026

This is a planning checklist, not the specification of a generated SecurePoint export. It does not certify CMMC compliance. Agree on the governing contract, assessment scope, and required standard revision with the customer and assessor. A visitor application supports only part of the customer's Physical Protection program.

Assemble the evidence set

Evidence area	Suggested contents	Responsibility
Scope and policy	Sites, controlled areas, visitor policy, owners, approved exceptions	Customer security team
Visitor authorization	Visitor and host reference, purpose, approved visit, relevant decision	Configured visit records plus customer approvals
Supervision	Escort assignment and recorded events; procedure and supervision evidence	Application records where configured; staff and physical controls
Access records	Arrival, checkout, badge record, distinction between observed and automatic closure	Configured visit records; separate door-system records if needed
Decisions	Relevant screening results and reviewer rationale where customer policy calls for screening	Configured workflow and authorized reviewers
Protection and retrieval	Access permissions, retention schedule, retrieval sample, audit integrity review	Customer and provider responsibilities agreed for the deployment

Sanctions screening, citizenship collection, or government-ID capture should not be presented as universal CMMC requirements. Determine whether separate export-control or site-policy needs make them relevant. Visitor software does not monitor doors, observe a visitor's route, or prove continuous escort supervision.

Suggested pack structure

1. Scope, review date, owners, and applicable requirements.
2. Policy and procedure references.
3. A representative sample of actual visit records and recorded decisions.
4. External approvals, physical-access records, and other customer-held supplements.
5. Gaps, exceptions, assigned actions, and reviewer conclusions.

Export contents depend on the workflow and data actually recorded. Inspect a sample before promising fields, list versions, attachments, signatures, or formats. Do not infer that every item above is automatically collected or included in an evidence pack.

Review checks

Confirm that incomplete required evidence prevents admission or badging. Confirm that reviewers can retrieve a complete sample and distinguish missing evidence from a negative finding. Test the chosen device and printer path. Preserve personal data only as needed under the applicable policy and agreement.

References: NIST SP 800-171 Revision 2, including Physical Protection 3.10; 32 CFR Part 170. NIST has superseded Revision 2 with Revision 3; use the version required by the governing contract and program, not the publication date alone.