Visitor Compliance Checklist

ITAR, EAR, CMMC Level 2, DFARS, and sanctions screening workflows for regulated facilities.

> **Use this checklist to pressure test your current visitor process.** *If you can not produce the evidence listed below within 24 hours, you are not audit ready.*

What auditors and primes look for

[ ] A defined visitor policy, roles, and enforcement, not tribal knowledge
[ ] Screening results tied to identity, with reviewer actions logged
[ ] Escort rules and controlled area boundaries documented and enforced
[ ] Evidence packs, retention, and exports that survive an audit
[ ] Human decision making documented, especially when AI is used to assist

1) Before the visitor arrives

[ ] Define your visitor types: vendor, customer, candidate, foreign national, courier, VIP
[ ] Map your facility zones: public, visitor allowed, controlled, export controlled, CUI areas
[ ] Maintain a host list and approved escorts, with training acknowledgement if required
[ ] Pre register visits with purpose, areas requested, start and end time, and host
[ ] Require NDA and safety briefing where applicable, track completion timestamps
[ ] For foreign nationals, document export control review steps and approval authority
[ ] Establish denial and escalation playbooks, include who can override and why

Evidence to keep:

[ ] Visitor policy and site specific SOP
[ ] Zone map or access matrix
[ ] Escort training acknowledgment logs
[ ] Pre registration records and approvals

2) Check in, identity, and screening

[ ] Capture visitor identity, at minimum full name, company, email, and a government ID check
[ ] Screen names against sanctions and restricted party lists, log list versions and results
[ ] Handle potential matches with a human review step, record the reviewer and outcome
[ ] If using AI assistance, log the AI signal and the human decision separately
[ ] Issue a badge and record badge number, check in timestamp, and host notification
[ ] Enforce photo capture rules consistently, if photos are used

Evidence to keep:

[ ] ID verification audit record, do not store more ID data than required

[ ] Screening result record, including match review notes and disposition

[ ] Check in event log and host notification proof

3) During the visit

[ ] Enforce escort requirements for restricted zones, record escort assignment and changes

[ ] Track location or zone access when required by policy, even if done via checkpoints

[ ] Record incidents, policy exceptions, and approvals, with who approved and why

[ ] Control physical access to CUI and export controlled technical data, include visitor device rules

Evidence to keep:

[ ] Escort logs and exceptions

[ ] Incident and exception audit logs

[ ] Records of access restrictions communicated and acknowledged

4) Check out and after visit actions

[ ] Record check out timestamp and badge return

[ ] Trigger an after visit report to the host when required, capture completion status

[ ] If controlled technology was shared, log what was shared and under what authorization

[ ] Store records under retention rules, support legal hold and export

Evidence to keep:

[ ] Check out event log and badge return record

[ ] After visit report, including approvals and acknowledgements

[ ] Controlled technology disclosure records if applicable

5) What an audit ready evidence pack should include

When an auditor, a prime, or your internal security team asks for proof, you should be able to export a complete evidence pack per site, per date range, and per visitor.

[ ] Visitor roster export with timestamps, host, purpose, and zones

[ ] Screening export with list sources, match confidence, reviewer notes, and disposition

[ ] Adjudication queue history, who approved, who denied, and why

[ ] Audit log export of key actions: create visit, edit, approve, override, check in, check out

[ ] Exception log: policy overrides and compensating controls

[ ] NDA and safety training completion records

[ ] Controlled tech alerts and after visit reports, if enabled

[ ] Retention and deletion settings, plus proof of enforcement

Quick self test

[ ] Can you produce the last 90 days of visitor logs in CSV within 5 minutes

[ ] Can you show the exact sanction list sources used for a past screening result

[ ] Can you show who overrode a screening hold and what note they left

[ ] Can you prove an escort was assigned to a foreign national visitor

[ ] Can you explain, in one sentence, how AI is used, and where humans decide

Need a second set of eyes?

SecurePoint USA is built for ITAR, EAR, CMMC, and audit evidence from day one. Start with the checklist page or request beta access.

Checklist page: https://www.securepointusa.com/resources/checklist
Request beta: https://www.securepointusa.com/request-demo