Use the public security overview

Assess the published layers for identity, transport, isolation, storage, monitoring and secure development.

Task: Use the use the public security overview process consistently and retain the right evidence.

Audience: Security reviewers and procurement teams

Owner: Obedience Governance

Version 2026.08 | Reviewed 2026-08-22 | Next review 2027-02-22

Purpose and scope

Assess the published layers for identity, transport, isolation, storage, monitoring and secure development.

Use this guide as orientation, then rely on the signed agreement, current policy or named support response where those sources set a more specific obligation.

Prepare the right information

- The product and assurance scope.
- Required control domains.
- Questions that need restricted evidence.

Follow the controlled process

1. Frame the need

State the desired outcome, affected product and accountable contact. For use the public security overview, avoid assumptions that have not been confirmed in writing.

2. Review and decide

Use the current governed source, record material questions and obtain approval from the person who owns the decision.

3. Retain evidence

Keep the final reference, date, decision and any follow-up action together so a later reviewer can reconstruct what happened.

Expected record

- A mapped public control summary.
- Identified evidence gaps.
- A secure follow-up route.

Keep in mind

The overview intentionally omits secrets, exact defensive rules and exploitable infrastructure detail.

Security and disclosure boundary

- Never send passwords, authentication codes, private keys or recovery codes to Obedience staff.
- Share the minimum customer, project and commercial information needed for the stated purpose.

- Public documentation explains controls and responsibilities without publishing exploitable topology, credentials or confidential implementation detail.