# 19.4 Full Security Model

Go To Top

Return to Phase 0 Non-Goals

Phase 0 does not implement the full security model. It may avoid obvious unsafe practices, such as logging secrets or embedding credentials in containers, but it does not provide production-grade authentication, authorization, encryption, key management, identity governance, audit controls, secure deployment, or policy enforcement.

The team should still handle credentials and sensitive values carefully during Phase 0. Configuration, logs, evidence, containers, scripts, and repository files should not expose secrets, private keys, tokens, passwords, or sensitive local values.

Later phases should define and validate the security model appropriate to the deployment context, DDS security requirements, IEF policy constraints, operational governance, and cross-organizational participation.

---