DOCUMENT REF: IDG-SEC-ISO-27001

Category: Information Security | Classification: Sovereign Official | Release Year: 2026

Information Security & ISO-27001 Implementation Manual

1. Information Security Management System (ISMS)

This manual establishes the institutional framework for implementing ISO/IEC 27001:2022 controls across all IDG government-facing assets, ensuring confidentiality, integrity, and availability.

- Continuous threat modeling and enforcement of least-privilege role-based access control (RBAC).
- Automated SAST and DAST vulnerability scanning embedded directly into CI/CD release pipelines.
- Mandatory multi-factor hardware security key authentication (FIDO2/WebAuthn).

2. 24/7 Security Operations Center (SOC) & Rapid Incident Response

The IDG Sovereign SOC delivers round-the-clock behavioral threat monitoring, anomaly detection, and automated mitigation.

- Sub-60 second detection latency for volumetric and zero-day threat patterns.
- Automated isolation and quarantining of suspicious network endpoints.
- Cryptographically sealed forensic event logs compliant with legal evidentiary standards.

3. Disaster Recovery & Business Continuity

Resilience architectures tested biannually under simulated catastrophic failure conditions to guarantee uninterrupted national service delivery.

SOVEREIGN CERTIFICATION & INSTITUTIONAL SEAL

This document is formally ratified by the IDG Engineering Council and Governance Directorate. Full technical adherence is mandatory across all connected platforms.