Kiteworks

COMPLIANCE BRIEF

Kiteworks Supports the Australian Government Information Security Manual (ISM)

Meeting ASD's IRAP Controls on a PROTECTED-Assessed Platform with Data Sovereignty and Single-Tenant Isolation

Solution Highlights

- Strong double encryption
- FIPS 140-3
- SafeVIEW and SafeEDIT
- Data Sovereignty and Geofencing
- Single-tenant private cloud
- Comprehensive Audit Logs with SIEM feeds

The Australian Government Information Security Manual (ISM) is a cyber security framework produced and maintained by the Australian Signals Directorate (ASD), with the current release published in June 2026. The ISM provides the control set that underpins the Infosec Registered Assessor Program (IRAP), the assessment scheme through which systems demonstrate their security posture. It applies to Australian Government departments and agencies, and to the managed service providers, outsourced cloud service providers, and contractors that process, store, or communicate government data across classification levels ranging from non-classified and OFFICIAL: Sensitive through PROTECTED, SECRET, and TOP SECRET, including sensitive compartmented information. Rather than imposing statutory monetary fines, the ISM operates through an authorisation-to-operate mechanism in which system owners obtain authorisation from an authorising officer, or from Director-General ASD for TOP SECRET systems, following security assessments conducted by organisational assessors, IRAP assessors, or ASD assessors. Kiteworks supports organizations working toward compliance with the ISM. Here's how:

Encryption, Hardening, and Assumed-Breach Defenses for Classified Data

The ISM's cryptography controls require ASD-approved encryption at rest and in transit, full disk encryption, and pre-boot authentication (ISM-1059, ISM-2109). Kiteworks meets this with encryption at rest file and disk double encryption, the FIPS 140-3 validated encryption option, and TLS 1.3/AES-256 in transit (confirm disk-encryption infrastructure with Kiteworks). Malware handling relies on the built-in F-Secure antivirus/quarantine option, advanced threat prevention, and content disarm and reconstruct. Device and data separation is met by SafeVIEW and SafeEDIT, which keep classified data inside Kiteworks, plus mobile apps with remote wipe. Foreign-national restrictions rely on geography controls and attribute-based access policies. Hardening requirements across every classification level are addressed by the hardened virtual appliance, an embedded firewall/WAF, zero-trust internal separation, and AI-based intrusion detection. Authentication hardening draws on multi-factor authentication, certificate-based login and PIV/CAC, and configurable password policy. Backup protections combine double encryption, customer-owned keys, and role separation.

Least-Privilege Access Governance and Data Sovereignty Controls

Every user must be uniquely identifiable, enforced through Kiteworks authentication, RBAC/ABAC, and SCIM provisioning. Least-privilege access runs through the principle of least privilege and eight separated admin roles; break-glass access relies on short-lived, one-time-password credentials rather than standing accounts, with session revocation and automatic deactivation after inactivity. Sovereignty requirements draw on data sovereignty routing to keep data in an assigned country, geofencing and IP controls, and a single-tenant private cloud with customer-owned keys, backed by the Australia Private IRAP Hosted Option (PROTECTED-assessed). Data minimisation runs through time-based expiration and file-lifetime retention, and register/configuration controls through secure data forms, node/cluster management, and risky settings detection. AI-agent governance uses the same RBAC/ABAC controls on the MCP server, with approval workflows for higher-risk actions, while backup and software-supply-chain controls rely on high availability, file versioning, and open-source library sandboxing. Much of the ISM's access governance is organisational, not technical (board sign-off, documented procedures, media handling) and stays the customer's responsibility.

Centralised Event Logging and Searchable Retention for IRAP Evidence

Centralised event logging is met directly by comprehensive audit logs with SIEM feeds, which pull every Kiteworks activity into one stream and transmit it immediately and encrypted via log timeliness, a real-time SIEM feed, and syslog forwarding over TLS. Captured-field and structured-format requirements are satisfied by the audit log's Date, User, Activity, and IP Address fields across 632 documented events. Timely analysis comes from security analytics on the CISO dashboard, AI-based intrusion detection, and real-time threat notifications; separate controls capture unprivileged, privileged, break-glass, and authentication events, and incident-register requirements run through the persistent activity log, the interactive audit log map, and the insider threats report. Time accuracy relies on NTP synchronization tied to SNMP health monitoring, and retention is searchable with no fixed time-scope limit (confirm the retention window against your own requirements). Security-assessment controls draw on Kiteworks' DevSecOps practices, penetration testing, and AI-augmented detection, and logs stay protected through anonymization and restricted admin access.

Kiteworks' platform (not only its hosting environment) has been IRAP assessed against PROTECTED-level ISM controls, with the assessment covering the application's own data handling, access control, cryptography, and system management capabilities, in addition to infrastructure. The assessment was first achieved in 2022, with the most recent reassessment completed in July 2026. Kiteworks gives Australian Government entities and their service providers a practical route through the ISM's control set on one assessed platform. Protection comes from the hardened virtual appliance itself: double encryption, FIPS 140-3 validated cryptography, SafeVIEW and SafeEDIT data isolation, and multi-factor authentication defend classified data across every classification level. Control follows from least-privilege authorization, eight separated admin roles, data sovereignty routing, geofencing, and single-tenant private cloud deployment, which keep access and data residency firmly within organisational and national boundaries. Tracking is handled by a centralised, real-time audit log with SIEM feeds, structured event capture, and searchable retention: the evidence IRAP assessors actually expect to see. Deployed through the Australia Private IRAP Hosted Option, assessed against PROTECTED-level controls, Kiteworks unifies protection, control, and tracking so organisations can pursue their authorisation to operate with confidence.

Ready to Support Your ISM and IRAP Assessment?

www.kiteworks.com

Kiteworks

Kiteworks' mission is to empower organizations to effectively manage risk in every send, share, receive, and use of private data. The Kiteworks platform provides customers with a secure data exchange that delivers data governance, compliance, and protection in a unified control plane. Kiteworks unifies, tracks, controls, and secures sensitive data moving within, into, and out of their organization, significantly improving risk management and ensuring regulatory compliance on all private data exchanges. Headquartered in Silicon Valley, Kiteworks protects over 100 million end-users and thousands of global enterprises and government agencies.