Kiteworks

GUIDE

Canadian Program for Cyber Security Certification (CPCSC)

How Kiteworks Supports ITSP.10.171 Compliance for Canada's Defence Suppliers

Introduction: Why Kiteworks for CPCSC

The Canadian Program for Cyber Security Certification represents the most significant mandatory cyber security framework ever imposed on Canada's defence supply chain. Launched by Public Services and Procurement Canada in partnership with the Department of National Defence, the Standards Council of Canada, and the Canadian Centre for Cyber Security, CPCSC establishes three progressive certification levels that determine whether a defence supplier can bid on—and win—Government of Canada defence contracts. Level 1, required in select defence contracts beginning Summer 2026, requires a self-assessment against 13 foundational controls. Level 2 introduces triannual third-party assessments by accredited certification bodies across 98 security controls, plus an annual affirmation. Level 3 adds 200 controls assessed triannually by the Government of Canada, plus an annual affirmation. Levels 2 and 3 are currently under development and will be introduced in a phased approach. The business consequence is binary: no certification, no contract eligibility.

The standard underpinning CPCSC is ITSP.10.171—a Canadian adaptation of NIST SP 800-171, developed by the Canadian Centre for Cyber Security and aligned with ITSP.10.033 (Canada's version of NIST SP 800-53 Rev. 5). There are no substantial technical changes between ITSP.10.171 and NIST SP 800-171. The modifications reflect Canada's distinct regulatory and compliance landscape—different terminology ("specified information" instead of "controlled unclassified information"), different governing authorities (Treasury Board Secretariat policies instead of NIST directives), and different privacy frameworks (PIPEDA and provincial laws instead of the U.S. Privacy Act). The control requirements themselves are identical. Every lesson learned from the U.S. Cybersecurity Maturity Model Certification (CMMC) program applies directly to CPCSC.

That readiness data is stark. A Kiteworks and Coalfire survey of 209 Defence Industrial Base organizations found that only 46% consider themselves prepared for CMMC Level 2 certification—which shares the same NIST 800-171 control foundation as CPCSC Level 2. Fifty-seven percent have not completed a NIST 800-171 gap analysis, the foundational step for certification readiness. A separate Kiteworks survey of 104 organizations pursuing CMMC found that 62% lack adequate governance controls. Canadian suppliers face the same control requirements with less runway and fewer established assessment resources.

Kiteworks is purpose-built for this challenge. As the control plane for secure data exchange, Kiteworks consolidates email, file sharing, managed file transfer, SFTP, web forms, APIs, and AI integrations into a single platform governed by one policy engine, one audit log, and one security architecture. Kiteworks supports 80% of Level 2 controls.

For Canadian defence suppliers, Kiteworks offers a distinct advantage beyond CPCSC alone: Five Eyes interoperability. Because ITSP.10.171 is technically equivalent to NIST SP 800-171, organizations that certify to CPCSC with Kiteworks simultaneously position themselves for CMMC certification on U.S. DoW contracts. Kiteworks is FedRAMP Authorized with pre-mapped NIST 800-171 controls and provides CMMC 2.0 compliance reports with a Controls Addendum covering all 110 practices.

Canada's defence suppliers also face a sovereignty dimension their U.S. counterparts do not. Forty percent of Canadian respondents identify changes to Canada–U.S. data sharing arrangements as their top regulatory concern, and 21% flag the U.S. CLOUD Act as a direct sovereignty threat. Kiteworks resolves this with on-premises, private cloud in Canadian data centres, or hybrid deployment—combined with single-tenant isolation, customer-owned encryption keys, geofencing, and data sovereignty controls ensuring specified information never leaves Canadian jurisdiction.

This guide provides a complete control-by-control mapping of Kiteworks capabilities to the 98 ITSP.10.171 Level 2 requirements, drawn directly from the regulation text. Defence suppliers can use this mapping to accelerate their gap analysis, identify where Kiteworks provides control inheritance, and focus organizational effort on the process and physical controls that require human governance.

ITSP.10.171 Control-by-Control Mapping

The following tables map each of the 98 allocated ITSP.10.171 Level 2 controls to Kiteworks capabilities, organized by control family. Requirement text is drawn verbatim from ITSP.10.171 (requirement section only). Controls outside the Kiteworks application scope—primarily organizational, physical, or process-based—are noted as Out of Scope.

Access Controls

Control	Requirement (ITSP.10.171)	Kiteworks Supports Compliance	Kiteworks Solution
03.01.01 *Access Control* Account Management	A. Define the types of system accounts allowed and prohibited. B. Create, enable, modify, disable, and remove system accounts in accordance with organizational policy, procedures, prerequisites, and criteria. C. Specify: 1. authorized users of the system, 2. group and role membership, 3. access authorizations (i.e., privileges) for each account. D. Authorize access to the system based on: 1. a valid access authorization, 2. intended system usage. E. Monitor the use of system accounts. F. Disable system accounts when: 1. the accounts have expired, 2. the accounts have been inactive for [Assignment: organization-defined time period], 3. the accounts are no longer associated with a user or individual, 4. the accounts are in violation of organizational policy, 5. significant risks associated with individuals are discovered. G. Notify account managers and designated personnel or roles within: 1. [Assignment: organization-defined time period] when accounts are no longer required, 2. [Assignment: organization-defined time period] when users are terminated or transferred, 3. [Assignment: organization-defined time period] when system usage or the need-to-know changes for an individual. H. Require that users log out of the system after [Assignment: organization-defined time period] of expected inactivity or when [Assignment: organization-defined circumstances].	**Yes, supports compliance**	The Kiteworks platform enforces strict access controls to protect all data. It supports comprehensive account life-cycle management through LDAP/Active Directory auto-provisioning and de-provisioning, RBAC and ABAC governance controls, configurable inactivity timeouts, and domain-based user assignment. Eight or more default admin roles enforce separation of duties. All admin changes and account activity are captured in comprehensive audit logs.

Control	Requirement (ITSP.10.171)	Kiteworks Supports Compliance	Kiteworks Solution
03.01.02 *Access Control* Access Enforcement	Enforce approved authorizations for logical access to specified information and system resources in accordance with applicable access control policies.	**Yes, supports compliance**	The Data Policy Engine enforces both role-based (RBAC) and attribute-based (ABAC) access controls across all data exchange channels—email, file sharing, MFT, SFTP, web forms, and AI integrations. System administrators and data owners assign roles such as Owner, Manager, Collaborator, Downloader, Viewer, or Uploader to files and folders, limiting users to only the transactions and functions they are permitted to execute.
03.01.03 *Access Control* Information Flow Enforcement	Enforce approved authorizations for controlling the flow of specified information within the system and between connected systems.	**Yes, supports compliance**	The Data Policy Engine enforces information flow through ABAC runtime policies aligned to the NIST CSF Framework. Dynamic access controls evaluate data attributes (such as folder paths or sensitivity labels), user attributes (like domain or profile), and the actions being performed. The Email Policy Engine (EPG) enforces email-specific flow controls including encryption, DLP routing, and policy-based send rules.
03.01.04 *Access Control* Separation of Duties	A. Identify the duties of individuals requiring separation. B. Define system access authorizations to support separation of duties.	**Yes, supports compliance**	Kiteworks provides configurable administrator roles with granular separation of duties. Eight or more default admin roles ensure that compliance admins, security admins, and system admins have distinct, non-overlapping permissions. Admin role-based access to tracking data ensures that personnel who administer access controls cannot also administer audit functions.

Control	Requirement (ITSP.10.171)	Kiteworks Supports Compliance	Kiteworks Solution
03.01.05 *Access Control* Least Privilege	A. Allow only the authorized system access for users (or processes acting on behalf of users) that is necessary to accomplish assigned organizational tasks. B. Authorize access to [Assignment: organization-defined security functions] and [Assignment: organization-defined security-relevant information]. C. Review the privileges assigned to roles or classes of users [Assignment: organization-defined frequency] to validate the need for such privileges. D. Reassign or remove privileges, as necessary.	**Yes, supports compliance**	The platform defaults to least-privileged access. The Data Policy Engine enforces RBAC and ABAC policies, and folder roles (Owner, Manager, Collaborator, Downloader, Viewer, Uploader) enforce granular least privilege at the file and folder level. Offline RBAC policies and admin role hierarchies ensure that access privileges are scoped to each user's operational need.
03.01.06 *Access Control* Least Privilege - Privileged Accounts	A. Restrict privileged accounts on the system to [Assignment: organization-defined personnel or roles]. B. Require that users (or roles) with privileged accounts use non-privileged accounts when accessing non-security functions or non-security information. C. Require any administrative or superuser actions to be performed from a physical workstation which is dedicated to those specific tasks and isolated from all other functions and networks, especially any form of Internet access.	**Yes, supports compliance**	Configurable administrator roles restrict privileged functions to designated personnel. The platform prevents even Kiteworks staff from accessing customer data (No Kiteworks or Admin Access). Non-privileged users cannot execute admin functions, and all access to security functions is logged in the comprehensive audit log.
03.01.07 *Access Control* Least Privilege - Privileged Functions	A. Prevent non-privileged users from executing privileged functions. B. Log the execution of privileged functions.	**Yes, supports compliance**	The platform prevents non-privileged users from executing privileged functions through RBAC and ABAC governance controls. All privileged function execution is captured in comprehensive audit logs with real-time SIEM feed, enabling audit of every administrative action. Admin role-based access to tracking data restricts visibility of audit data to the Compliance admin role.

Control	Requirement (ITSP.10.171)	Kiteworks Supports Compliance	Kiteworks Solution
03.01.08 *Access Control* Unsuccessful Logon Attempts	A. Limit the number of consecutive invalid logon attempts to [Assignment: organization-defined number] in [Assignment: organization-defined time period]. B. Automatically [Selection (one or more): lock the account or node for an [Assignment: organization-defined time period]; lock the account or node until released by an administrator; delay next logon prompt; notify system administrator; take other action] when the maximum number of unsuccessful attempts is exceeded.	**Yes, supports compliance**	The platform enforces configurable lockout thresholds for failed login attempts via IP Address Blocking (Fail2Ban). When the defined limit is reached, the account can be locked and an alert sent to administrators. IP address controls provide additional protection against repeated unauthorized access attempts.
03.01.09 *Access Control* System Use Notification	Display a system use notification message with privacy and security notices consistent with applicable specified information rules before granting access to the system.	**Yes, supports compliance**	Terms of Service policies and platform branding controls allow administrators to configure system use notification banners that display privacy and security notices before users are granted access. These banners are fully customizable to meet organizational requirements.
03.01.10 *Access Control* Device Lock	A. Prevent access to the system by [Selection (one or more): initiating a device lock after [Assignment: organization-defined time period] of inactivity; requiring the user to initiate a device lock before leaving the system unattended]. B. Retain the device lock until the user re-establishes access using established identification and authentication procedures. C. Conceal, via the device lock, information previously visible on the display with a publicly viewable image.	**Yes, supports compliance**	The platform enforces session timeouts and requires re-authentication after inactivity, using the Time and expiration feature. Integration with identity management systems ensures re-authentication aligns with organizational policies. Note: OS-level device lock (screen lock) is outside the Kiteworks application scope.

Control	Requirement (ITSP.10.171)	Kiteworks Supports Compliance	Kiteworks Solution
03.01.11 *Access Control* Session Termination	Terminate a user session automatically after [Assignment: organization-defined conditions or trigger events requiring session disconnect].	**Yes, supports compliance**	The Time and expiration feature allows administrators to define policies that automatically terminate user sessions after a defined inactivity period. Session termination can also be triggered by IP address changes. Administrators can manually terminate active sessions at any time.
03.01.12 *Access Control* Remote Access	A. Establish usage restrictions, configuration requirements, and connection requirements for each type of allowable remote system access. B. Authorize each type of remote system access prior to establishing such connections. C. Route remote access to the system through authorized and managed access control points. D. Authorize remote execution of privileged commands and remote access to security-relevant information.	**Yes, supports compliance**	All Kiteworks remote access is encrypted in transit using TLS 1.3/1.2. The platform enforces authentication through its integration with a broad set of identity management and authentication systems including MFA, SAML 2.0, and Kerberos. The embedded network firewall and geofencing control access points. All remote sessions are captured in comprehensive audit logs.
03.01.16 *Access Control* Wireless Access	A. Establish usage restrictions, configuration requirements, and connection requirements for each type of wireless access to the system. B. Authorize each type of wireless access to the system prior to establishing such connections. C. Disable, when not intended for use, wireless networking capabilities prior to issuance and deployment. D. Protect wireless access to the system using authentication and encryption.	**Out of Scope**	Wireless infrastructure management is an endpoint and network-level control outside the Kiteworks application scope. Kiteworks encrypts all data in transit using TLS 1.3 regardless of the underlying network type, providing cryptographic protection over any wireless connection, but does not manage the wireless infrastructure itself.

Control	Requirement (ITSP.10.171)	Kiteworks Supports Compliance	Kiteworks Solution
03.01.18 *Access Control* Access Control for Mobile Devices	A. Establish usage restrictions, configuration requirements, and connection requirements for mobile devices. B. Authorize the connection of mobile devices to the system. C. Implement full-device or container-based encryption to protect the confidentiality of specified information on 26 ITSP.10.171 mobile devices.	**Yes, supports compliance**	The Kiteworks mobile app enforces encryption at rest and access controls, and supports remote wipe of CUI stored in the secure container on lost or stolen devices. Geofencing and IP address controls can restrict mobile access by location. Full mobile device management (MDM) policies are outside the Kiteworks application scope.
03.01.20 *Access Control* Use of External Systems	A. Prohibit the use of external systems unless they are specifically authorized. B. Establish the following terms, conditions, and security requirements to be satisfied on external systems prior to allowing use of or access to those systems by authorized individuals: [Assignment: organization-defined security requirements]. C. Permit authorized individuals to use an external system to access the organization's system or to process, store, or transmit specified information only after: 1. verifying that the security requirements on the external system as specified in the organization's system security and privacy plans have been satisfied 27 ITSP.10.171, 2. retaining approved system connection or processing agreements with the organizational entities hosting the external systems. D. Restrict the use of organization-controlled portable storage devices by authorized individuals on external systems.	**Yes, supports compliance**	Kiteworks controls access to and from external systems through domain allow/deny lists, geofencing, and geography-based policies. The Data Policy Engine restricts which external cloud content management systems (Google Drive, Box, Dropbox, OneDrive, SharePoint) can be accessed. Portable storage device restrictions on endpoints are outside the application scope.
03.01.22 *Access Control* Publicly Accessible Content	A. Train authorized individuals to ensure that publicly accessible information does not contain specified information. B. Review the content on publicly accessible systems for specified information periodically and remove such information, if discovered.	**Yes, supports compliance**	RBAC and ABAC governance controls determine who can share content externally. The Withdrawal feature allows removal of previously shared content. This control also addresses broader public-facing systems beyond the Kiteworks data exchange scope.

Awareness and Training

Control	Requirement (ITSP.10.171)	Kiteworks Supports Compliance	Kiteworks Solution
03.02.01 *Awareness and Training* Literacy Training and Awareness	A. Provide security and privacy literacy training to system users: 1. as part of initial training for new users and [Assignment: organization-defined frequency] thereafter, 2. when required by system changes or following [Assignment: organization-defined events], 3. on recognizing and reporting indicators of insider threat, social engineering, and social mining. B. Update security and privacy literacy training content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	**Out of Scope**	Security awareness training is an organizational process control outside the Kiteworks application scope. Kiteworks provides comprehensive audit logs and compliance reports that can support training program evidence and incident awareness programs, but does not deliver training content.
03.02.02 *Awareness and Training* Role-Based Training	A. Provide role-based security and privacy training to organizational personnel: 1. before authorizing access to the system or specified information, before performing assigned duties, and [Assignment: organization-defined frequency] thereafter, 2. when required by system changes or following [Assignment: organization-defined events]. B. Update role-based training content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	**Out of Scope**	Role-based security training is an organizational process control outside the Kiteworks application scope. Kiteworks provides role-specific admin interfaces and RBAC governance controls that reinforce role boundaries in practice, but training program delivery is the customer's responsibility.

Audit and Accountability

Control	Requirement (ITSP.10.171)	Kiteworks Supports Compliance	Kiteworks Solution
03.03.01 *Audit and Accountability* Event Logging	A. Specify the following event types selected for logging within the system: [Assignment: organization-defined event types]. B. Review and update the event types selected for logging [Assignment: organization-defined frequency].	**Yes, supports compliance**	Comprehensive audit logs capture every user, admin, and system event in real time with zero throttling—no gaps, no delays. Event types cover file operations, authentication attempts, policy enforcement, admin actions, and system events. Logs can be exported to SIEM systems via real-time SIEM feed and syslog.
03.03.02 *Audit and Accountability* Audit Record Content	A. Include the following content in audit records: 1. what type of event occurred, 2. when the event occurred, 3. where the event occurred, 4. source of the event, 5. outcome of the event, 6. identity of individuals, subjects, objects, or entities associated with the event. B. Provide additional information for audit records, as needed.	**Yes, supports compliance**	Every audit record includes event type, timestamp, source IP, user identity, action performed, object affected, outcome (success/failure), and policy evaluation results. The platform assigns unique user IDs to ensure all actions are traceable to individual users. Topics logged include all end-user actions and all admin changes.
03.03.03 *Audit and Accountability* Audit Record Generation	A. Generate audit records for the selected event types and audit record content specified in Event logging 03.03.01 and Audit record content 03.03.02. B. Retain audit records for a time period consistent with records retention policy.	**Yes, supports compliance**	Audit records are generated automatically for all system events with no time scope limit on retention. The expanded date range searches in the audit log and compliance reports support after-the-fact investigation. Log retention synchronization ensures records align with organizational retention policies.

Control	Requirement (ITSP.10.171)	Kiteworks Supports Compliance	Kiteworks Solution
03.03.04 *Audit and Accountability* Response to Audit Logging Process Failures	A. Alert organizational personnel or roles within [Assignment: organization-defined time period] in the event of an audit logging process failure. B. Take the following additional actions: [Assignment: organization-defined additional actions].	**Yes, supports compliance**	The real-time SIEM feed of the audit log enables alerting through external SIEM/SOAR systems when logging processes fail. The embedded managed detection and response (MDR) system can flag logging irregularities. Specific audit failure alert thresholds depend on the connected SIEM configuration.
03.03.05 *Audit and Accountability* Audit Record Review, Analysis, and Reporting	A. Review and analyze system audit records [Assignment: organization-defined frequency] for indications and potential impact of inappropriate or unusual activity. B. Report findings to organizational personnel or roles. C. Analyze and correlate audit records across different repositories to gain organization-wide situational awareness.	**Yes, supports compliance**	Security analytics and compliance reports (CMMC 2.0, GDPR, HIPAA) automate audit record analysis and reporting. The interactive audit log map enables geographic correlation of activity. Consolidated and normalized logs support SIEM integration for cross-repository correlation and threat hunting.
03.03.06 *Audit and Accountability* Audit Record Reduction and Report Generation	A. Implement an audit record reduction and report generation capability that supports audit record review, analysis, reporting requirements, and after-the-fact investigations of incidents. B. Preserve the original content and time ordering of audit records.	**Yes, supports compliance**	The platform provides audit record reduction through filtering, search, and on-demand report generation. Expanded date range searches support after-the-fact investigation. The Risk Policy audit log report and compliance summary reports reduce audit data to framework-specific evidence while preserving original log integrity.

Control	Requirement (ITSP.10.171)	Kiteworks Supports Compliance	Kiteworks Solution
03.03.07 *Audit and Accountability* Time Stamps	A. Use internal system clocks to generate time stamps for audit records. B. Record time stamps for audit records that meet [Assignment: organization-defined granularity of time measurement] and that use Coordinated Universal Time (UTC), have a fixed local time offset from UTC, or include the local time offset as part of the time stamp.	**Yes, supports compliance**	The platform integrates with Network Time Protocol (NTP) servers to provide authoritative timestamps for all audit records. Log timeliness ensures records are generated in real time, and detail fields include precise timestamps suitable for forensic analysis and event correlation.
03.03.08 *Audit and Accountability* Protection of Audit Information	A. Protect audit information and audit logging tools from unauthorized access, modification, and deletion. B. Authorize access to management of audit logging functionality to only a subset of privileged users or roles.	**Yes, supports compliance**	Audit data access is restricted to the Compliance admin role through admin role-based access to tracking data. Even Kiteworks staff cannot modify or delete audit records (No Kiteworks or Admin Access). The real-time SIEM feed of the audit log provides independent copies, and tamper-evident logging protects record integrity.

Configuration Management

Control	Requirement (ITSP.10.171)	Kiteworks Supports Compliance	Kiteworks Solution
03.04.01 *Configuration Management* Baseline Configuration	A. Develop and maintain under configuration control, a current baseline configuration of the system. B. Review and update the baseline configuration of the system [Assignment: organization-defined frequency] and when system components are installed or modified.	**Yes, supports compliance**	Kiteworks ships as a hardened virtual appliance with a documented baseline (stripped-down Rocky Linux 8.10). The embedded operating system removes unnecessary services. Compliance reports and one-click system updates maintain the baseline. Broader system baseline documentation for the customer's full environment is an organizational responsibility.
03.04.02 *Configuration Management* Configuration Settings	A. Establish, document, and implement the following configuration settings for the system that reflect the most restrictive mode consistent with operational requirements: [Assignment: organization-defined configuration settings]. B. Identify, document, and approve any deviations from established configuration settings.	**Yes, supports compliance**	The hardened virtual appliance ships with secure defaults. Risky settings detection alerts administrators when configurations fall below recommended security levels. Admin settings are captured in comprehensive audit logs. Documenting deviations in the system security plan is an organizational responsibility.
03.04.03 *Configuration Management* Configuration Change Control	A. Define the types of changes to the system that are configuration-controlled. B. Review proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security impacts. C. Implement and document approved configuration-controlled changes to the system. D. Monitor and review activities associated with configuration-controlled changes to the system.	**Yes, supports compliance**	All admin configuration changes are logged with full attribution in comprehensive audit logs with real-time SIEM feed. Topics logged include system setup activities. Formal change management processes (CAB review, approval workflows) are organizational responsibilities.

Control	Requirement (ITSP.10.171)	Kiteworks Supports Compliance	Kiteworks Solution
03.04.04 *Configuration Management* Impact Analyses	A. Analyze the security and privacy impacts of changes to the system prior to implementation. B. Verify that the security requirements for the system continue to be satisfied after the system changes have been implemented.	**Out of scope**	Impact analysis is an organizational process control outside the Kiteworks application scope. Kiteworks provides automatic security-tested updates and compliance reports that highlight configuration changes degrading security below recommended levels.
03.04.05 *Configuration Management* Access Restrictions for Change	Define, document, approve, and enforce physical and logical access restrictions associated with changes to the system.	**Yes, supports compliance**	System changes are restricted to authorized admin roles through RBAC governance controls and the hardened virtual appliance architecture. The No Kiteworks or Admin Access feature prevents unauthorized access. All access restrictions and changes are logged with full attribution.
03.04.06 *Configuration Management* Least Functionality	A. Configure the system to provide only mission-essential capabilities. B. Prohibit or restrict use of the following functions, ports, protocols, connections, and services: [Assignment: organization-defined functions, ports, protocols, connections, and services]. C. Review the system [Assignment: organization-defined frequency] to identify unnecessary or nonsecure functions, ports, protocols, connections, and services. D. Disable or remove functions, ports, protocols, connections, and services that are unnecessary or nonsecure.	**Yes, supports compliance**	The embedded network firewall implements deny-by-default architecture, blocking all unused ports. The hardened virtual appliance and embedded operating system remove unnecessary services. Zero-trust mode for intrusion detection prevents unauthorized connections. Deny-by-default and least functionality are enforced at the infrastructure level.

Control	Requirement (ITSP.10.171)	Kiteworks Supports Compliance	Kiteworks Solution
03.04.08 *Configuration Management* Authorized Software - Allow by Exception	A. Identify software programs authorized to execute on the system. B. Implement a deny-all, allow-by-exception policy for the execution of software programs on the system. C. Review and update the list of authorized software programs [Assignment: organization-defined frequency].	**Yes, supports compliance**	The hardened virtual appliance enforces a deny-all, allow-by-exception policy for software execution. Open-source library sandboxing isolates external code. The platform enforces app whitelisting on mobile devices. Broader endpoint software management is outside the Kiteworks application scope.
03.04.10 *Configuration Management* System Component Inventory	A. Develop and document an inventory of system components. B. Review and update the system component inventory [Assignment: organization-defined frequency]. C. Update the system component inventory as part of installations, removals, and system updates.	**Yes, supports compliance**	The hardened virtual appliance maintains a defined component inventory for the Kiteworks system (OS, application, dependencies). System component inventory across the customer's full environment is an organizational responsibility.
03.04.11 *Configuration Management* Information Location	A. Identify and document the location of specified information and the system components on which the information is processed and stored. B. Document changes to the system or system component location where specified information is processed and stored.	**Yes, supports compliance**	Data sovereignty and geofencing controls track and enforce the location of specified information. The interactive audit log map visualizes where data is accessed geographically. Documenting changes to system component locations is an organizational responsibility.
03.04.12 *Configuration Management* System and Component Configuration for High-Risk Areas	A. Issue systems or system components with the following configurations to individuals traveling to high-risk locations: [Assignment: organization-defined system configurations]. B. Apply the following security requirements to the system or system components when the individuals return from 39 ITSP.10.171 travel: [Assignment: organization-defined security requirements].	**Out of Scope**	Physical device provisioning for high-risk travel is an organizational and physical security control outside the Kiteworks application scope. Geofencing can restrict access from high-risk geographic locations at the platform level.

Identification and Authentication

Control	Requirement (ITSP.10.171)	Kiteworks Supports Compliance	Kiteworks Solution
03.05.01 *Identification and Authentication* User Identification, Authentication, and Re-authentication	A. Uniquely identify and authenticate system users and associate that unique identification with processes acting on behalf of those users. B. Re-authenticate users when [Assignment: organization-defined circumstances or situations requiring reauthentication].	**Yes, supports compliance**	The platform assigns unique IDs to all users and requires authentication before granting access. Integration with a broad set of identity management and authentication systems (LDAP/Active Directory, SAML 2.0, Kerberos, OAuth) provides centralized identity management with automatic provisioning. Re-authentication is enforced on session timeout and configurable trigger events.
03.05.02 *Identification and Authentication* Device Identification and Authentication	Uniquely identify and authenticate [Assignment: organization-defined devices or types of devices] before establishing a system connection.	**Yes, supports compliance**	Device authentication is supported through TLS certificate validation, PIV/CAC card support, and IP address controls for consistency checking. Geofencing provides location-based device validation. Full device certificate-based authentication depends on integration with enterprise MDM/NAC solutions.
03.05.03 *Identification and Authentication* Multi-Factor Authentication	Implement strong multi-factor authentication (MFA) for access to privileged and non-privileged accounts.	**Yes, supports compliance**	The platform supports and enforces multi-factor authentication for both privileged and non-privileged accounts through integration with a broad set of identity management and authentication systems. Supported MFA methods include RADIUS protocol, PIV/CAC cards, time-based OTP (RFC 6238), native email-based OTP, and authenticator apps (Google Authenticator, Microsoft Authenticator, Duo).

Control	Requirement (ITSP.10.171)	Kiteworks Supports Compliance	Kiteworks Solution
03.05.04 *Identification and Authentication* Replay-Resistant Authentication	Implement replay-resistant authentication mechanisms for access to privileged and non-privileged accounts.	**Yes, supports compliance**	OAuth 2.0 authentication with refresh token support provides replay-resistant authentication for API and MCP integrations. Time-based OTP (RFC 6238) is inherently replay-resistant. TLS certificate validation prevents session hijacking. PIV/CAC cards use certificate-based authentication not susceptible to credential replay.
03.05.05 *Identification and Authentication* Identifier Management	A. Receive authorization from organizational personnel or roles to assign an individual, group, role, service, or device identifier. B. Select and assign an identifier that identifies an individual, group, role, service, or device. C. Prevent reuse of identifiers for [Assignment: organization-defined time period]. D. Manage individual identifiers by uniquely identifying each individual as [Assignment: organization-defined characteristic identifying individual status].	**Yes, supports compliance**	LDAP/Active Directory integration provides an authoritative identity source with unique email-based identification. The Time and expiration feature automatically disables inactive accounts per configurable timeouts. Domain controls enforce user assignment to allowed domains.
03.05.07 *Identification and Authentication* Password Management	A. Maintain a list of commonly used, expected, or compromised passwords and update the list [Assignment: organization-defined frequency] and when organizational passwords are suspected to have been compromised. B. Verify that passwords are not found on the list of commonly used, expected, or compromised passwords when users create or update passwords. C. Transmit passwords only over cryptographically protected channels. D. Store passwords in a cryptographically protected form. E. Select a new password upon first use after account recovery. F. Enforce the following composition and complexity rules for passwords: [Assignment: organization-defined composition and complexity rules].	**Yes, supports compliance**	The platform enforces configurable password complexity requirements through integration with identity management systems. Passwords are stored as salted cryptographic hashes and transmitted only over encrypted connections (Encryption in Transit, TLS 1.3). Enterprise SSO/IdP integration delegates password policy to the organization's identity system.

Control	Requirement (ITSP.10.171)	Kiteworks Supports Compliance	Kiteworks Solution
03.05.11 *Identification and Authentication* Authentication Feedback	Obscure feedback of authentication information during the authentication process.	**Yes, supports compliance**	The platform obscures password input during authentication—passwords are not displayed in plain text on screens. Error messages do not reveal whether the username or password was incorrect, preventing enumeration attacks. All authentication information is transmitted over secure TLS connections.
03.05.12 *Identification and Authentication* Authenticator Management	A. Verify the identity of the individual, group, role, service, or device receiving the authenticator as part of the initial authenticator distribution. B. Establish initial authenticator content for any authenticators issued by the organization. C. Establish and implement administrative procedures for initial authenticator distribution, for lost, compromised, or damaged authenticators, and for revoking authenticators. D. Change default authenticators at first use. E. Change or refresh authenticators [Assignment: organization-defined frequency] or when the following events occur: [Assignment: organization-defined events]. F. Protect authenticator content from unauthorized disclosure and modification.	**Yes, supports compliance**	The platform manages authenticators through enterprise IdP integration. MFA authenticator enrollment requires verified identity. Token lifetimes are configurable through the Time and expiration feature. Secure credential management stores credentials in OS-level secure keystores for MCP integrations.

Incident Response

Control	Requirement (ITSP.10.171)	Kiteworks Supports Compliance	Kiteworks Solution
03.06.01 *Incident Response* Incident Handling	Implement an incident-handling capability that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery.	**Yes, supports compliance**	Kiteworks supports detection and analysis through real-time audit logging, comprehensive SIEM feeds, and the embedded managed detection and response (MDR) system. Security analytics and anomaly detection support incident identification. Containment actions (account disabling, session termination, content withdrawal) are available. Full incident handling procedures are an organizational responsibility.
03.06.02 *Incident Response* Incident Monitoring, Reporting, and Response Assistance	A. Track and document system security incidents. B. Report suspected incidents to the organizational incident response capability within [Assignment: organization-defined time period]. C. Report incident information to [Assignment: organization-defined authorities]. D. Provide an incident response support resource that offers advice and assistance to system users for the handling and reporting of incidents.	**Yes, supports compliance**	Compliance reports for insider threats and outsider threats, combined with real-time SIEM feeds and security analytics, support incident tracking and reporting. Topics logged include intrusion and anomaly alerts. Formal incident reporting to designated authorities is an organizational process responsibility.
03.06.03 *Incident Response* Incident Response Testing	Test the effectiveness of the incident response capability [Assignment: organization-defined frequency].	**Out of Scope**	Incident response testing (tabletop exercises, simulations, drills) is an organizational process control outside the Kiteworks application scope. Kiteworks audit data and compliance reports can inform test scenarios.

Control	Requirement (ITSP.10.171)	Kiteworks Supports Compliance	Kiteworks Solution
03.06.04 *Incident Response* Incident Response Training	A. Provide incident response training to system users consistent with assigned roles and responsibilities: 1. within [Assignment: organization-defined time period] of assuming an incident response role or responsibility or acquiring system access, 2. when required by system changes, 3. [Assignment: organization-defined frequency] thereafter. B. Review and update incident response training content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	**Out of Scope**	Incident response training is an organizational process control outside the Kiteworks application scope. Kiteworks platform activity logs provide context for security-aware training program development.
03.06.05 *Incident Response* Incident Response Plan	A. Develop an incident response plan that: 1. provides the organization with a roadmap for implementing its incident response capability, 2. describes the structure and organization of the incident response capability, 3. provides a high-level approach for how the incident response capability fits into the overall organization, 4. defines reportable incidents, 5. addresses the sharing of incident information, 6. designates responsibilities to organizational entities, personnel, or roles. B. Distribute copies of the incident response plan to designated incident response personnel (identified by name and/or by role) and organizational elements. C. Update the incident response plan to address system and organizational changes or problems encountered during plan implementation, execution, or testing. D. Protect the incident response plan from unauthorized disclosure.	**Yes, supports compliance**	Kiteworks supports protection of the incident response plan document (sub-req D) through RBAC and ABAC access controls, encryption at rest, customer-owned keys, and the “SafeVIEW” file viewer for view-only access. Plan development, distribution, and update (sub-reqs A–C) are organizational process responsibilities.

Maintenance

Control	Requirement (ITSP.10.171)	Kiteworks Supports Compliance	Kiteworks Solution
03.07.04 *Maintenance* Maintenance Tools	A. Approve, control, and monitor the use of system maintenance tools. B. Check media containing diagnostic and test programs for malicious code before the media are used in the system. C. Prevent the removal of system maintenance equipment containing specified information by verifying that there is no specified information on the equipment, sanitizing or destroying the equipment, or retaining the equipment within the facility.	**Yes, supports compliance**	The hardened virtual appliance architecture prevents direct OS or database access by customers or Kiteworks staff (No Kiteworks or Admin Access). System updates are delivered through controlled, security-tested channels. Advanced threat prevention integrations scan content. Broader maintenance tool controls for non-Kiteworks infrastructure are organizational responsibilities.
03.07.05 *Maintenance* Non-Local Maintenance	49 ITSP.10.171 A. Approve and monitor non-local maintenance and diagnostic activities. B. Implement multi-factor authentication and replay resistance in the establishment of non-local maintenance and diagnostic sessions. C. Terminate session and network connections when non-local maintenance is completed.	**Yes, supports compliance**	All Kiteworks admin sessions use encryption in transit (TLS 1.3), require authenticated access through the integration with a broad set of identity management and authentication systems including MFA, and are captured in comprehensive audit logs. Sessions terminate on inactivity via the Time and expiration feature. No Kiteworks or Admin Access ensures no unauthorized maintenance access.
03.07.06 *Maintenance* Maintenance Personnel	A. Establish a process for maintenance personnel authorization. B. Maintain a list of authorized maintenance organizations or personnel. C. Verify that non-escorted personnel who perform maintenance on the system possess the required access authorizations. D. Designate organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.	**Yes, supports compliance**	Admin roles restrict maintenance activities to authorized personnel. All user activity including maintenance is captured in comprehensive audit logs. Formal maintenance personnel authorization lists and supervision requirements are organizational responsibilities.

Media Protection

Control	Requirement (ITSP.10.171)	Kiteworks Supports Compliance	Kiteworks Solution
03.08.01 *Media Protection* Media Storage	Physically control and securely store system media containing specified information.	**Yes, supports compliance**	Digital media is protected through AES-256 double encryption at rest (file and disk levels) and single-tenant isolation. The on-premises and self-hosted private cloud deployment option ensures data sovereignty. Physical media storage controls for non-digital media (tapes, paper) are outside the application scope.
03.08.02 *Media Protection* Media Access	Restrict access to specified information on system media to authorized personnel or roles.	**Yes, supports compliance**	RBAC and ABAC governance controls restrict access to data on system media to authorized users and roles. Encryption at rest with customer-owned keys ensures only authorized parties can decrypt stored data. Admin role separation prevents unauthorized access to media.
03.08.03 *Media Protection* Media Sanitization	Sanitize system media containing specified information prior to disposal, release out of organizational control, or release for reuse.	**Yes, supports compliance**	The Time and expiration feature enforces configurable data expiration and deletion policies for files and folders. Single-tenant architecture ensures data isolation on disposal. Physical media sanitization (degaussing, destruction) for hardware is outside the application scope.
03.08.04 *Media Protection* Media Marking	Mark system media containing specified information to indicate distribution limitations, handling caveats, and applicable specified information markings.	**Yes, supports compliance**	Kiteworks Tags support data classification and marking of digital media. Automated policies based on Microsoft MIP sensitivity labels mark CUI according to distribution limitations. Physical media marking (labels on drives, tapes) is outside the application scope.

Control	Requirement (ITSP.10.171)	Kiteworks Supports Compliance	Kiteworks Solution
03.08.05 *Media Protection* Media Transport	A. Protect and control system media that contain specified information during transport outside of controlled areas. B. Maintain accountability of system media that contain specified information during transport outside of controlled areas. C. Document activities associated with the transport of system media that contain specified information.	**Yes, supports compliance**	All data exchanged through Kiteworks is encrypted in transit using TLS 1.3 and protected at rest with AES-256 double encryption with FIPS 140-3 validated modules. The FIPS 140-3 validate encryption option is available. This cryptographic protection is a core Kiteworks capability.
03.08.07 *Media Protection* Media Use	A. Restrict or prohibit the use of [Assignment: organization-defined types of system media]. B. Prohibit the use of removable system media without an identifiable owner.	**Yes, supports compliance**	ABAC runtime policies and directives supported by ABAC data policies can restrict file types, sizes, and sources for data exchange. Physical media use restrictions (USB drives, removable storage) on endpoints are outside the Kiteworks application scope.
03.08.09 *Media Protection* System Backup - Cryptographic Protection	A. Protect the confidentiality of backup information. B. Implement cryptographic mechanisms to prevent the unauthorized disclosure of specified information at backup storage locations.	**Yes, supports compliance**	Backup data is protected through AES-256 double encryption with customer-owned keys, ensuring only the customer can decrypt backup data. The hardware security module (HSM) integration supports key management for backup encryption. The FIPS 140-3 validate encryption option is available.

Personnel Security

Control	Requirement (ITSP.10.171)	Kiteworks Supports Compliance	Kiteworks Solution
03.09.01 *Personnel Security* Personnel Screening	A. Screen individuals prior to authorizing access to the system. B. Rescreen individuals in accordance with [Assignment: organization-defined conditions requiring rescreening].	**Out of Scope**	Personnel screening (background checks, security clearances) is an HR and organizational process control outside the Kiteworks application scope.
03.09.02 *Personnel Security* Personnel Termination and Transfer	A. When individual employment is terminated: 1. disable system access within [Assignment: organization-defined time period], 2. terminate or revoke authenticators and credentials associated with the individual, 3. retrieve security-related system property. B. When individuals are reassigned or transferred to other positions in the organization: 1. review and confirm the ongoing operational need for current logical and physical access authorizations to the system and facility, 2. modify access authorization to correspond with any changes in operational need.	**Yes, supports compliance**	LDAP/Active Directory integration enables automatic deprovisioning when employees are terminated in the directory. The Withdrawal feature allows removal of previously shared content. Authentication certificate expiration notifications support credential revocation. Physical property retrieval is outside the application scope.

Physical Protection

Control	Requirement (ITSP.10.171)	Kiteworks Supports Compliance	Kiteworks Solution
03.10.01 *Physical Protection* Physical Access Authorizations	A. Develop, approve, and maintain a list of individuals with authorized access to the physical location where the system resides. B. Issue authorization credentials for physical access. C. Review the physical access list [Assignment: organization-defined frequency]. D. Remove individuals from the facility access list when access is no longer required.	**Out of Scope**	Physical access authorization lists are a facilities and physical security control outside the Kiteworks application scope.
03.10.02 *Physical Protection* Monitoring Physical Access	A. Monitor physical access to the facility where the system resides to detect and respond to physical security incidents. B. Review physical access logs [Assignment: organization-defined frequency] and upon occurrence of [Assignment: organization-defined events or potential indications of events].	**Out of Scope**	Physical access monitoring (cameras, badge readers, physical access logs) is a facilities control outside the Kiteworks application scope.
03.10.06 *Physical Protection* Alternate Work Site	A. Determine alternate work sites allowed for use by employees. B. Employ the following security requirements at alternate work sites: [Assignment: organization-defined security requirements].	**Yes, supports compliance**	Kiteworks protects CUI at all locations through encryption in transit, encryption at rest, and authentication controls. Geofencing and data sovereignty controls restrict access by geographic location. Physical security requirements at alternate work sites (locks, screens) are outside the application scope.

Control	Requirement (ITSP.10.171)	Kiteworks Supports Compliance	Kiteworks Solution
03.10.07 *Physical Protection* Physical Access Control	Enforce physical access authorizations at entry and exit points to the facility where the system resides by: 1. verifying individual physical access authorizations before granting access to the facility, 2. controlling ingress and egress with physical access control systems, devices or guards. B. Maintain physical access audit logs for entry or exit points. C. Escort visitors and control visitor activity. D. Secure keys, combinations, and other physical access devices. E. Control physical access to output devices to prevent unauthorized individuals from obtaining access to specified information. 58 ITSP.10.171	**Out of Scope**	Physical access control (locks, guards, mantraps, card readers) is a facilities control outside the Kiteworks application scope.
03.10.08 *Physical Protection* Access Control for Transmission	Control physical access to system distribution and transmission lines in organizational facilities.	**Out of Scope**	Physical protection of transmission lines (wiring closets, cable runs) is a facilities control outside the Kiteworks application scope. Kiteworks provides cryptographic protection of data in transit regardless of physical line security.

Risk Assessment

Control	Requirement (ITSP.10.171)	Kiteworks Supports Compliance	Kiteworks Solution
03.11.01 *Risk Assessment* Risk Assessment	A. Assess the risk (including supply chain risk) of unauthorized disclosure resulting from the handling, processing, storage, or transmission of specified information. B. Update risk assessments [Assignment: organization-defined frequency].	**Out of Scope**	Risk assessment methodology is an organizational process outside the Kiteworks application scope. Kiteworks provides comprehensive audit logs, security analytics, and compliance reports that inform organizational risk assessments.
03.11.02 *Risk Assessment* Vulnerability Monitoring and Scanning	A. Monitor and scan for vulnerabilities in the system [Assignment: organization-defined frequency] and when new vulnerabilities affecting the system are identified. B. Remediate system vulnerabilities within [Assignment: organization-defined response times]. C. Update system vulnerabilities to be scanned [Assignment: organization-defined frequency] and when new vulnerabilities are identified and reported.	**Yes, supports compliance**	Kiteworks manages vulnerability scanning and remediation for its own platform through automated and manual penetration testing, the comprehensive DevSecOps "shift left" approach, and the embedded managed detection and response system. The platform supports one-click updates to remediate identified vulnerabilities. Customer-side scanning of the broader environment is an organizational responsibility.
03.11.04 *Risk Assessment* Risk Response	Respond to findings from security assessments, monitoring, and audits.	**Out of Scope**	Risk response strategy is an organizational management decision outside the Kiteworks application scope. Kiteworks provides security controls, compliance reports, and audit data that support risk mitigation responses.

Security Assessment and Monitoring

Control	Requirement (ITSP.10.171)	Kiteworks Supports Compliance	Kiteworks Solution
03.12.01 *Security Assessment and Monitoring* Security Assessment	Assess the security and privacy requirements for the system and its environment of operation [Assignment: organization-defined frequency] to determine if the requirements have been satisfied.	**Yes, supports compliance**	Compliance reports (CMMC 2.0, GDPR, HIPAA) automatically assess control effectiveness. Kiteworks is SOC 2 certified and FedRAMP Authorized, with annual third-party assessments. The CMMC 2.0 report with controls addendum documents control implementation. The broader organizational security assessment program is customer-led.
03.12.02 *Security Assessment and Monitoring* Plan of Action and Milestones	A. Develop a plan of action and milestones (POAMs) for the system to: 1. document the planned remediation actions to correct weaknesses or deficiencies noted during security assessments, 2. reduce or eliminate known system vulnerabilities. B. Update the existing POAMs based on the findings from: 1. security assessments, 2. audits or reviews, 3. continuous monitoring activities.	**Out of Scope**	POA&M development is an organizational documentation process outside the Kiteworks application scope. Compliance reports identify control gaps that inform POA&M development.
03.12.03 *Security Assessment and Monitoring* Continuous Monitoring	Develop and implement a system-level continuous monitoring strategy that includes ongoing monitoring and security assessments.	**Yes, supports compliance**	Real-time audit logging, real-time SIEM feed, the embedded managed detection and response (MDR) system, and security analytics provide continuous monitoring of the Kiteworks platform. The CISO Dashboard visualizes security posture and anomalous activity continuously.
03.12.05 *Security Assessment and Monitoring* Information Exchange	A. Approve and manage the exchange of specified information between the system and other systems using [Selection (one or more): interconnection security agreements; information exchange security agreements; memoranda of understanding or agreement; information sharing arrangements; service level agreements; user agreements; nondisclosure agreements]. B. Document, as part of the exchange agreements, interface characteristics, security and privacy requirements, and responsibilities for each system. C. Review and update the exchange agreements [Assignment: organization-defined frequency].	**Yes, supports compliance**	RBAC and ABAC governance controls, domain allow/deny lists, and data policies for folder invitations enforce data exchange agreements at the technical level. Formal agreement documentation (ISAs, MOUs) is an organizational process responsibility.

System and Communications Protection

Control	Requirement (ITSP.10.171)	Kiteworks Supports Compliance	Kiteworks Solution
03.13.01 *System and Communications Protection* Boundary Protection	A. Monitor and control communications at the external managed interfaces to the system and key internal managed interfaces within the system. B. Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks. C. Connect to external systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.	**Yes, supports compliance**	The embedded network firewall implements deny-by-default architecture blocking all unused ports. The embedded web application firewall (WAF) detects and blocks web and API attacks. The embedded managed detection and response (MDR) system and AI-based intrusion and anomaly detection provide threat monitoring. Tiered internal services with zero-trust principles enforce internal boundaries.
03.13.04 *System and Communications Protection* Information in Shared System Resources	Prevent unauthorized and unintended information transfer via shared system resources.	**Yes, supports compliance**	Single-tenant private cloud architecture eliminates cross-tenant data exposure. Tiered internal services with zero-trust principles prevent cross-component information leakage. Open-source library sandboxing isolates external code from application data.
03.13.06 *System and Communications Protection* Network Communications - Deny by Default - Allow by Exception	Deny network communications traffic by default and allow network communications traffic by exception.	**Yes, supports compliance**	The embedded network firewall implements deny-all, permit-by-exception network communications. Only essential ports and services are exposed. The hardened virtual appliance enforces this deny-by-default policy at the infrastructure level. IP address controls support whitelisting and blacklisting.

Control	Requirement (ITSP.10.171)	Kiteworks Supports Compliance	Kiteworks Solution
03.13.08 *System and Communications Protection* Transmission and Storage Confidentiality	Implement cryptographic mechanisms to prevent the unauthorized disclosure of specified information during transmission and while in storage.	**Yes, supports compliance**	The platform encrypts specified information in transit using TLS 1.3 and protects data at rest with AES-256 double encryption (file and disk levels). Customer-owned keys ensure only authorized parties can decrypt data. The FIPS 140-3 validate encryption option is available for both transit and storage.
03.13.09 *System and Communications Protection* Network Disconnect	Terminate network connections associated with communications sessions at the end of the sessions or after [Assignment: organization-defined time period] of inactivity. 67 ITSP.10.171	**Yes, supports compliance**	The Time and expiration feature allows administrators to configure session timeout policies, automatically disconnecting users after a defined inactivity period. TCP/IP sessions are terminated at both the application and network levels.
03.13.10 *System and Communications Protection* Cryptographic Key Establishment and Management	Establish and manage cryptographic keys in the system in accordance with the following key management requirements: [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction].	**Yes, supports compliance**	Kiteworks customers have full ownership of their cryptographic keys through customer-owned keys. Keys can be managed within the platform or stored in an external hardware security module (HSM) integration. The FIPS 140-3 validate encryption option is available. The Trusted Data Format (TDF) provides standards-based key management.

Control	Requirement (ITSP.10.171)	Kiteworks Supports Compliance	Kiteworks Solution
03.13.11 *System and Communications Protection* Cryptographic Protection	Implement the following types of cryptography when used to protect the confidentiality of specified information: [Assignment: organization-defined types of cryptography].	**Yes, supports compliance**	The FIPS 140-3 validate encryption option provides validated cryptography for the protection of specified information. AES-256 is used for data at rest, TLS 1.3 for data in transit. Encryption standards align with applicable laws, directives, and policies.
03.13.12 *System and Communications Protection* Collaborative Computing Devices and Applications	A. Prohibit remote activation of collaborative computing devices and applications with the following exceptions: [Assignment: organization-defined exceptions where remote activation is to be allowed]. B. Provide an explicit indication of use to users physically present at the devices.	**Yes, supports compliance**	Kiteworks collaboration features (File Share, Transfer, and Collaboration) require explicit user activation and authenticated access. Broader collaborative device controls (cameras, microphones, videoconferencing) are endpoint and OS-level controls outside the Kiteworks application scope.
03.13.13 *System and Communications Protection* Mobile Code	A. Define acceptable mobile code and mobile code technologies. B. Authorize, monitor, and control the use of mobile code.	**Yes, supports compliance**	The embedded web application firewall (WAF) controls mobile code execution at the application layer. Open-source library sandboxing isolates external code. Kiteworks uses secure coding practices aligned with OWASP Top 10, verified through SOC 2, FedRAMP, and FIPS 140-3 audits. Endpoint browser policies are an organizational responsibility.
03.13.15 *System and Communications Protection* Session Authenticity	Protect the authenticity of communications sessions.	**Yes, supports compliance**	TLS certificate validation establishes session authenticity. SAML 2.0 assertions are cryptographically signed. OAuth 2.0 authentication with refresh token support provides cryptographically bound session tokens. The platform invalidates session identifiers upon logout and generates unique session identifiers with predefined randomness requirements.

System and Information Integrity

Control	Requirement (ITSP.10.171)	Kiteworks Supports Compliance	Kiteworks Solution
03.14.01 *System and Information Integrity* Flaw Remediation	A. Identify, report, and correct system flaws. B. Install security-relevant software and firmware updates within [Assignment: organization-defined time period] of the release of the updates.	**Yes, supports compliance**	Kiteworks monitors and reviews vulnerabilities in its platform through automated and manual penetration testing, white and black box bounty programs, and the embedded managed detection and response (MDR) system. One-click updates enable prompt flaw remediation. The hardened virtual appliance reduces the attack surface.
03.14.02 *System and Information Integrity* Malicious Code Protection	A. Implement malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code. B. Update malicious code protection mechanisms as new releases are available in accordance with configuration management policies and procedures. C. Configure malicious code protection mechanisms to: 1. perform scans of the system [assignment: organization-defined frequency] and real-time scans of files from external sources at endpoints or system entry and exit points as the files are downloaded, opened, or executed, 2. block or quarantine malicious code, or take other mitigation actions in response to malicious code detection.	**Yes, supports compliance**	The embedded WAF detects and blocks malicious code at the application layer. AI-based intrusion and anomaly detection identifies suspicious patterns. Open-source library sandboxing isolates external code. Advanced threat prevention (ATP) integration and antivirus scanning scan uploaded files for malware and zero-day threats. WAF rules are automatically updated.
03.14.03 *System and Information Integrity* Security Alerts, Advisories, and Directives	A. Receive system security alerts, advisories, and directives from external organizations on an ongoing basis. B. Generate and disseminate internal system security alerts, advisories, and directives, as necessary.	**Yes, supports compliance**	The platform can be configured to export logs to SIEM systems via real-time SIEM feed for security monitoring and alerts. The embedded managed detection and response (MDR) system monitors external security advisories and incorporates them into the update cycle.

Control	Requirement (ITSP.10.171)	Kiteworks Supports Compliance	Kiteworks Solution
03.14.06 *System and Information Integrity* System Monitoring	A. Monitor the system to detect: 1. attacks and indicators of potential attacks, 2. unauthorized connections. B. Identify unauthorized use of the system. C. Monitor inbound and outbound communications traffic to detect unusual or unauthorized activities or conditions.	**Yes, supports compliance**	Real-time audit logging and comprehensive SIEM feeds monitor all inbound and outbound communications. AI-based intrusion and anomaly detection identifies attacks and unauthorized connections. The embedded WAF monitors web and API traffic. Security analytics identifies unauthorized use patterns.
03.14.08 *System and Information Integrity* Information Management and Retention	Manage and retain specified information within the system and specified information output from the system in accordance with applicable laws, Orders in Council, directives, regulations, policies, standards, guidelines, and operational requirements.	**Yes, supports compliance**	The Time and expiration feature enforces configurable retention policies for files, folders, and audit data. Legal hold and eDiscovery access controls preserve specified information. Audit logs have no time scope limit for retention.
03.14.09 *System and Information Integrity* Dedicated Administration Workstation	A. Require any administrative or superuser actions to be performed from a physical workstation which is dedicated to those specific tasks and isolated from all other functions and networks, and especially from any form of internet access. B. Remote connection of a DAW to a target network is to use carrier private networks (e.g., virtual private LAN service (VPLS) or multiprotocol label switching (MPLS)) with VPN encryption. C. Use a dedicated and hardened single-purpose physical workstation or thin client as the DAW, that is not shared between security realms.	**Out of Scope**	Dedicated administration workstations are a physical and endpoint control outside the Kiteworks application scope. The Kiteworks admin console can be accessed from any authenticated, authorized system. Encrypting remote admin connections via VPN is an infrastructure-level control.

Planning

Control	Requirement (ITSP.10.171)	Kiteworks Supports Compliance	Kiteworks Solution
03.15.01 *Planning* Policy and Procedures	A. Develop, document, and disseminate to organizational personnel or roles, policies and procedures needed to satisfy the security requirements for the protection of specified information. B. Review and update policies and procedures [Assignment: organization-defined frequency].	**Out of Scope**	Policy and procedure documentation is an organizational governance responsibility outside the Kiteworks application scope. Kiteworks provides the technical controls these policies reference.
03.15.02 *Planning* System Security Plan	A. Develop a system security and privacy plan that: 1. defines the constituent system components, 2. identifies the information types processed, stored, and transmitted by the system, 3. describes specific threats to the system that are of concern to the organization, 4. describes the operational environment for the system and any dependencies on or connections to other systems or system components, 5. provides an overview of the security requirements for the system, 6. describes the safeguards in place or planned for meeting the security requirements, 7. identifies individuals that fulfill system roles and responsibilities, 8. includes other relevant information necessary for the protection of specified information. B. Review and update the system security plan [Assignment: organization-defined frequency]. C. Protect the system security plan from unauthorized disclosure.	**Yes, supports compliance**	The CMMC 2.0 report with controls addendum documents Kiteworks control implementation and supports system security plan development. Compliance summary reports provide evidence for SSP documentation. The SSP itself and broader plan development are organizational responsibilities. The "SafeVIEW" file viewer protects the SSP document from unauthorized modification.
03.15.03 *Planning* Rules of Behaviour	A. Establish rules that describe the responsibilities and expected behaviour for system usage and protecting specified information. B. Provide rules to individuals who require access to the system. C. Receive a documented acknowledgement from individuals indicating that they have read, understand, and agree to abide by the rules of behaviour before authorizing access to specified information and the system. D. Review and update the rules of behaviour [Assignment: organization-defined frequency].	**Out of Scope**	Rules of behaviour documentation is an organizational HR and governance control outside the Kiteworks application scope. Terms of Service policies can display rules at login, but rules development is the customer's responsibility.

System and Services Acquisition

Control	Requirement (ITSP.10.171)	Kiteworks Supports Compliance	Kiteworks Solution
03.16.01 *System and Services Acquisition* Security Engineering Principles	Apply the following systems security engineering principles to the development or modification of the system and system components: [Assignment: organization-defined systems security engineering principles].	**Yes, supports compliance**	Kiteworks is architected with security engineering principles: defense-in-depth through tiered internal services with zero-trust principles, least privilege via RBAC and ABAC governance controls, the hardened virtual appliance, embedded operating system, and open-source library sandboxing. Customer-side application of security engineering principles to their own systems is an organizational responsibility.
03.16.02 *System and Services Acquisition* Unsupported System Components	A. Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer. B. Provide options for risk mitigation or alternative sources for continued support for unsupported components if components cannot be replaced.	**Yes, supports compliance**	The hardened virtual appliance and embedded operating system manage the Kiteworks component life cycle, replacing unsupported components through controlled updates. Customer responsibility extends to ensuring the host infrastructure (hypervisor, operating system) remains supported.
03.16.03 *System and Services Acquisition* External System Services	A. Require the providers of external system services used for the processing, storage, or transmission of specified information, to comply with the following security requirements: [Assignment: organization-defined security requirements]. B. Define and document user roles and responsibilities with regard to external system services including shared responsibilities with external service providers. C. Implement processes, methods, and techniques to monitor security requirement compliance by external service providers on an ongoing basis.	**Yes, supports compliance**	Kiteworks as a service provider offers single-tenant private cloud isolation, customer-owned keys, and documented security controls verified through FedRAMP authorization and SOC 2 certification. Compliance summary reports and the CMMC 2.0 report document Kiteworks compliance posture. Governing other external services in the customer environment is an organizational responsibility.

Supply Chain Risk Management

Control	Requirement (ITSP.10.171)	Kiteworks Supports Compliance	Kiteworks Solution
03.17.01 *Supply Chain Risk Management* Supply Chain Risk Management Plan	A. Develop a plan for managing supply chain risks associated with the research, development, design, manufacturing, acquisition, delivery, integration, operations, maintenance, and disposal of the system, system components, or system services. B. Review and update the supply chain risk management plan [Assignment: organization-defined frequency]. C. Protect the supply chain risk management plan from unauthorized disclosure.	**Yes, supports compliance**	Kiteworks supports protection of the SCRM plan document (sub-req C) through RBAC and ABAC access controls, customer-owned encryption keys, double encryption at rest, and the "SafeVIEW" file viewer for controlled access. Supply chain risk management plan development and review (sub-reqs A–B) are organizational process responsibilities.
03.17.02 *Supply Chain Risk Management* Acquisition Strategies, Tools, and Methods	Develop and implement acquisition strategies, contract tools, and procurement methods to identify, protect against, and mitigate supply chain risks.	**Out of Scope**	Acquisition strategies, contract tools, and procurement methods are organizational procurement controls outside the Kiteworks application scope.
03.17.03 *Supply Chain Risk Management* Supply Chain Requirements and Processes	A. Establish a process for identifying and addressing weaknesses or deficiencies in the supply chain elements and processes. B. Enforce the following security requirements to protect against supply chain risks to the system, system components, or system services and to limit the harm or consequences from supply chain-related events: [Assignment: organization-defined security requirements].	**Yes, supports compliance**	Kiteworks manages its own supply chain security through the hardened virtual appliance, open-source library sandboxing, and single-tenant private cloud architecture. Customer responsibility extends to governing the broader supply chain environment.

Coverage Summary

The following analysis of ITSP.10.171 reveals that Kiteworks supports 80% of Level 2 requirements. The table below shows Kiteworks alignment by control family.

Practice Area	Kiteworks Supports	Out of Scope	Total
Access Control	15	1	16
Awareness and Training		2	2
Audit and Accountability	8		8
Configuration Management	8	2	10
Identification and Authentication	8		8
Incident Response	3	2	5
Maintenance	3		3
Media Protection	7		7
Personnel Security	1	1	2
Physical Protection	1	4	5
Risk Assessment	1	2	3
Security Assessment and Monitoring	3	1	4
System and Communications Protection	10		10
System and Information Integrity	5	1	6
Planning	1	2	3
System and Services Acquisition	3		3
Supply Chain Risk Management	2	1	3
Total	**79**	**19**	**98**

Kiteworks

April 2026

www.kiteworks.com