Kiteworks

GUIDE

Discover How Kiteworks Supports NIST 800-171 Compliance

Introduction

The U.S. government requires federal contractors to comply with the NIST 800-171 security standard to ensure the security of Controlled Unclassified Information (CUI) in non-federal systems and organizations.

In addition to general requirements for contractors to comply with NIST 800-171, the U.S. Department of Defense (DoD) mandates that all DOD contractors that process, store, or transmit CUI "meet the Defense Federal Acquisition Regulation Supplement (DFARS) minimum security standards by December 31, 2017, or risk losing their DoD contracts." Compliance with NIST 800-171 enables contractors to meet those minimum DFARS security standards.

What is CUI? According to NIST 800-171, it's "any information that law, regulation, or government-wide policy requires to have safeguarding or disseminating controls, with certain exemptions."[1] CUI includes 22 categories of information ranging from Personally Identifiable Information (PII) to critical infrastructure details to tax information. Within those 22 categories, the CUI Registry—the government service for tracking CUI—has identified 85 subcategories.[2]

[1] NIST 800-171, Revision 3, Draft 1, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations.

[2] Controlled Unclassified Information, Executive Order 13556.

It might be easiest to consider CUI to be any federal information that isn't classified but that needs to be secured.[3]

To ensure CUI remains secure, NIST 800-171 provides federal agencies with "a set of recommended security requirements for protecting the confidentiality of CUI when such information is resident in non-federal systems and organizations; when the non-federal organization is not collecting or maintaining information on behalf of a federal agency or using or operating a system on behalf of an agency; and where there are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or government-wide policy for the CUI category or subcategory listed in the CUI Registry."[4]

NIST 800-171 Organizes Its Security Requirements Into 17 Families:

- Access Control
- Awareness and Training
- Audit and Accountability
- Configuration Management
- Identification and Authentication

- Incident Response
- Maintenance
- Media Protection
- Personnel Security
- Physical Protection

- Risk Assessment
- Security Assessment
- System and Communications Protection
- System and Information Integrity

- Planning
- System and Services Acquisition
- Supply Chain Risk Management Plan

Together, these families cover a broad range of security concerns, ranging from screening and training personnel to providing physical safeguards that prevent the unauthorized disclosure of CUI.

This document describes NIST 800-171 requirements in detail and explains how the Kiteworks file sharing and governance platform helps commercial businesses who wish to work with the federal government, particularly the Department of Defense (DoD), comply with these requirements.

---

[3] An Introduction to NIST Special Publication 800-171 for Higher Education Institutions, October 2016.

[4] Ibid.

The Kiteworks Secure File Sharing and Governance Platform

Kiteworks' FedRAMP- and FIPS-140-2-compliant file sharing and governance platform enables enterprises to share sensitive information quickly and securely while maintaining full visibility and control over their file-sharing activities. The Kiteworks platform provides:

Secure File Sharing

Kiteworks enables government employees and federal contractors to access and share CUI securely, reducing the risk of data breaches, malware attacks, and data loss.

Governance and Compliance

Kiteworks supports NIST 800-171 compliance and provides comprehensive reports on file activity, access, and location.

Simplicity and Ease of Use

Kiteworks enables secure file sharing and collaboration from any device, among agency employees, contractors, and other trusted partners.

Automation

Kiteworks improves operational efficiency by automating information flows and data sharing with partners and remote locations to reduce manual steps and human error.

The Kiteworks Platform and NIST 800-171

The following tables describe how Kiteworks assists commercial businesses to comply with NIST 800-171.

3.1 Access Control

NIST SP 800-171 Requirement	Security Requirement Description	Kiteworks Supports Compliance	Kiteworks Solution

3.1.1 Account Management	a. Define and document the types of system accounts allowed and prohibited.
	b. Create, enable, modify, disable, and remove accounts in accordance with [Assignment: organization-defined policy, procedures, prerequisites, and criteria].
	c. Specify authorized users of the system, group and role membership, and access authorizations (i.e., privileges).
	d. Authorize access to the system based on a valid access authorization and intended system usage.
	e. Monitor the use of accounts.
	f. Disable accounts of individuals within [Assignment: organization-defined time period] when the accounts:
	  1. Have expired;
	  2. Are no longer associated with a user or individual;
	  3. Are in violation of organizational policy; or
	  4. Have been inactive for [Assignment: organization-defined time period]
	g. Disable accounts of individuals within [Assignment: organization-defined time period] of discovery of [Assignment: organization-defined significant risks].
	h. Notify [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period]:
	  1. When accounts are no longer required;
	  2. When users are terminated or transferred; and
	  3. When system usage or need-to-know changes for an individual.
		Yes, supports compliance	Kiteworks provides robust account management features, allowing administrators to easily manage users, groups, and permissions within the platform. Administrators can set up custom role-based access controls in Kiteworks for users and administrators, ensuring that users only have access to the data and features they need for their role, enhancing security and reducing the risk of unauthorized access, allowing organizations to protect all content, including CUI, under management. All user and admin actions are monitored in the centralized audit log. Accounts are automatically deactivated when they expire, when they have been inactive for a specified period, and can be deactivated manually by the admin or via API.

3.1.2 Access Enforcement	Enforce approved authorizations for logical access to CUI and system resources in accordance with applicable access control policies.	Yes, supports compliance	System administrators and content owners can control who receives which type of access: view and edit, view only, or access denied.

NIST SP 800-171 Requirement	Security Requirement Description	Kiteworks Supports Compliance	Kiteworks Solution
3.1.3 Flow Enforcement	Enforce approved authorizations for controlling the flow of CUI within the system and between connected systems.	Yes, supports compliance	Administrators and content owners can set permissions that ensure that nonauthorized users never gain access to CUI. Kiteworks Secure MFT and SMTP Gateway can be used to route content to approved destinations as part of workflows, ensuring that CUI is not accidentally distributed to unauthorized users.
3.1.4 Separation of Duties	a. Identify the duties of individuals requiring separation. b. Define system access authorizations to support separation of duties.	Yes, supports compliance	Administrators can define different roles and access levels for CUI, reducing the risk of collusion. The Kiteworks platform provides a set of standard admin roles and custom roles can be defined for each role/set of duties, e.g., help desk, application administration, system administration, etc.
3.1.5 Least Privilege	a. Allow only authorized system access for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks. b. Authorize access for [Assignment: organization-defined individuals or roles] to [Assignment: organization-defined security functions and security-relevant information]. c. Review [Assignment: organization-defined frequency] the privileges assigned to [Assignment: organization-defined roles or classes of users] to validate the need for such privileges. d. Reassign or remove privileges, as necessary.	Yes, supports compliance	The Kiteworks platform supports a range of user roles and access privileges. System administrators can define access policies that employ the principle of least privilege. All Kiteworks policies default to least privilege.
3.1.6 Least Privileged Accounts	a. Restrict privileged accounts on the system to [Assignment: organization-defined personnel or roles]. b. Require that users of system accounts (or roles) with access to [Assignment: organization-defined security functions or security-relevant information] use non-privileged accounts or roles when accessing nonsecurity functions.	Yes, supports compliance	The Kiteworks platform enables administrators to define different types of accounts and access privileges, ensuring that non-privileged users never access privileged content or controls.
3.1.7 Least Privilege – Privileged Functions	a. Prevent non-privileged users from executing privileged functions. b. Log the execution of privileged functions.	Yes, supports compliance	The Kiteworks platform prevents non-privileged users from executing administrative functions. The platform also logs all access to security functions, enabling the execution of those functions to be audited.

NIST SP 800-171 Requirement	Security Requirement Description	Kiteworks Supports Compliance	Kiteworks Solution
3.1.8 Unsuccessful Logon Attempts	Limit the number of consecutive invalid logon attempts by a user to [Assignment: organization-defined number] in [Assignment: organization-defined time period].	Yes, supports compliance	The Kiteworks platform enables system administrators to set a limit for unsuccessful logon attempts. When that limit is reached, that account can be locked, and an alert sent to administrators and security professionals.
3.1.9 System Use Notification	Display system use notification message or banner to users before granting access to the system that provides privacy and security notices consistent with applicable CUI rules.	Yes, supports compliance	The Kiteworks platform can be customized to display privacy and security notices required by an organization, with click-through if required. Different notices can be shown to different user roles, such as employees and external parties.
3.1.10 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 reestablishes 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 Kiteworks platform locks sessions after a configurable period of inactivity, and returns to the login screen.
3.1.11 Session Termination	Terminate a user session automatically after [Assignment: organization-defined conditions or trigger events].	Yes, supports compliance	The Kiteworks platform enables system administrators to define policies that automatically log users out after a set amount of idle time. System administrators can monitor and manually terminate active sessions.
3.1.12 Remote Access	(Now incorporates V2 3.1.13, 3.1.14, and 3.1.15) a. Establish, authorize, and document usage restrictions, configurations, and connections allowed for each type of permitted remote access. b. Monitor and control remote access methods. c. Route remote access to the system through managed access control points. d. Authorize remote execution of privileged commands and remote access to security-relevant information. e. Implement cryptographic mechanisms to protect the confidentiality of remote access sessions.	Yes, supports compliance	The Kiteworks platform monitors and logs all remote access to the system and to content, including CUI. All remote access is governed through strict access control policies through a single control point used by all clients. System administrators can monitor and manually terminate active sessions. The Kiteworks platform encrypts all transmission of content using Transport Layer Security (TLS) and encrypts content at rest using AES-256 encryption. A FIPS 140-2 validated module is also available. The Kiteworks platform enables system administrators to control which nodes (servers) are available for client access (HTTPS or SFTP) and provides a separate administrative interface that requires authentication and provides its own IP access restrictions. Access to privileged administrative commands can be limited to specific IP address ranges for known administrative users.

NIST SP 800-171 Requirement	Security Requirement Description	Kiteworks Supports Compliance	Kiteworks Solution
3.1.16 Wireless Access	(Now incorporates V2 3.1.17) a. Establish configuration requirements, connection requirements, and implementation guidance for wireless access to the system. b. Authorize wireless access to the system prior to allowing such connections. c. Protect wireless access to the system using authentication and encryption. d. Disable, when not intended for use, wireless networking capabilities embedded within the system prior to issuance and deployment.	Yes, supports compliance	The Kiteworks platform provides flexible deployment options with some or all of the Kiteworks servers behind the corporate firewall, plus uses authentication and encryption regardless of transport mechanism, protecting both wired and wireless access.
3.1.18 Access Control for Mobile Devices	(Now incorporates V2 3.1.19) a. Establish configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices. b. Authorize the connection of mobile devices to the system. c. Implement [Selection: full-device encryption; container-based encryption] to protect the confidentiality of CUI on mobile devices.	Yes, supports compliance	The Kiteworks platform enables and disables access from the Kiteworks mobile app. System administrators can also manage and terminate user sessions. If a mobile device is lost or stolen, system administrators can perform a remote wipe of all CUI in the Kiteworks secure container on the device. The Kiteworks platform encrypts CUI at rest on mobile devices and mobile computing platforms. In addition, it stores CUI in a secure container, protecting CUI on a mobile device from unauthorized access, data corruption, and malware.
3.1.20 Use of External Systems	a. [Selection (one or more): Establish [Assignment: organization-defined terms and conditions]; Identify [Assignment: organization-defined controls asserted to be implemented on external systems]], consistent with the trust relationships established with other organizations owning, operating, and/or maintaining external systems, allowing authorized individuals to: 1. Access the system from external systems; and 2. Process, store, or transmit CUI using external systems; or b. Prohibit the use of [Assignment: organization-defined types of external systems].	Yes, supports compliance	a. Kiteworks REST API can enable controlled access from external systems. Admins must grant access based on the client ID of the external system. The external system logs into Kiteworks as an authenticated user with access restrictions. b. The Kiteworks platform provides controlled access to cloud enterprise content management systems like Google Drive, Box, Dropbox, Microsoft OneDrive and Microsoft SharePoint Online.

NIST SP 800-171 Requirement	Security Requirement Description	Kiteworks Supports Compliance	Kiteworks Solution
3.1.21 External Systems – Limits and Restrictions on Authorized Use	a. Permit authorized individuals to use an external system to access the system or to process, store, or transmit CUI only after: 1. Implemented controls on the external system as specified in the organization's security policies and security plans are verified; or 2. Approved system connection or processing agreements with the organizational entity hosting the external system are retained. b. Restrict the use of organization-controlled portable storage devices by authorized individuals on external systems as follows: [Assignment: organization-defined usage restrictions].	N/A	Out of Scope
3.1.22 Publicly Accessible Content	a. Train authorized individuals to ensure that publicly accessible information does not contain CUI. b. Review the content on publicly accessible systems for CUI [Assignment: organization-defined frequency] and remove such information, if discovered.	Yes, supports compliance	Kiteworks administrators set controls over which users have the ability to post information in publicly accessible places. All such posted information has least privilege access controls over the ability to list, view, or download it.
3.1.23 Account Management – Inactivity Logout	Require that users log out of the system [Selection (one or more): after [Assignment: 514 organization-defined time period] of expected inactivity; when [Assignment: organization-defined 515 circumstances occur]].	Yes, supports compliance	The Kiteworks platform enables system administrators to define policies that automatically log users out after a set amount of idle time. System administrators can monitor and manually terminate active sessions.

3.2 Awareness and Training

NIST SP 800-171 Requirement	Security Requirement Description	Kiteworks Supports Compliance	Kiteworks Solution
3.2.1 Literacy Training and Awareness	a. Provide security literacy training to system users: 1. As part of initial training for new users and [Assignment: organization-defined frequency] thereafter; and 2. When required by system changes or following [Assignment: organization-defined events]. b. Update training and awareness content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Yes, supports compliance	Kiteworks FedRAMP operations managers and administration personnel are trained in the security risks and applicable policies, standards, and procedures related to the platform. The system warns customer admins of potentially risky settings, such as access controls that fail to follow the principle of least privilege.
3.2.2 Role-Based Training	a. Provide role-based security training to organizational personnel: 1. Before authorizing access to the system, CUI, or performing assigned duties, and [Assignment: organization-defined frequency] thereafter; and 2. When required by system changes. b. Update role-based training content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Yes, supports compliance	Kiteworks FedRAMP operations personnel are trained in the security risks and applicable policies, standards, and procedures related to the platform.
3.2.3 Advanced Literacy Training	Provide literacy training on recognizing and reporting potential and actual indicators of insider threat, social engineering, and social mining.	Yes, supports compliance	Kiteworks FedRAMP operations personnel must regularly pass security awareness training.

3.3 Audit and Accountability

NIST SP 800-171 Requirement	Security Requirement Description	Kiteworks Supports Compliance	Kiteworks Solution
3.3.1 Event Logging	a. Specify the following event types 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	The Kiteworks platform logs all access to, and sharing of, content. It tracks end-user and administrative user activities, and system events. Administrators and managers can generate reports for use in security investigations.
3.3.2 Audit Record Content	Include the following content in audit records: what type of event occurred; when and where the event occurred; source and outcome of the event; identity of individuals, subjects, objects, or entities associated with the event; and [Assignment: organization-defined additional information].	Yes, supports compliance	The Kiteworks platform assigns each user a unique ID and tracks all activity on a per-user and per-file basis. Each log entry specifies a time, location (server node, client, etc.), and uses a standardized event list.
3.3.3 Audit Record Generation	a. Provide an audit record generation capability for the event types defined in 3.3.1a. b. Generate audit records for the event types defined in 3.3.1a. that include the audit record content defined in 3.3.2. c. Retain audit records for [Assignment: organization-defined time period consistent with records retention policy, applicable contract requirement, law, or regulation].	Yes, supports compliance	The Kiteworks platform logs all access to and sharing of content. It tracks end-user and administrative user activities, and system events. Administrators and managers can generate reports for use in security investigations. Logs can be fed to external archives via the syslog interface.
3.3.4 Response to Audit Logging Process Failures	a. Alert [Assignment: organization-defined 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 Kiteworks platform alerts administrators in the event of a logging process failure.
3.3.5 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 [Assignment: organization-defined personnel or roles]. c. Analyze and correlate audit records across different repositories to gain organization-wide 685 situational awareness.	Yes, supports compliance	Logs generated by the Kiteworks platform can be fed to SIEM systems and other security analysis platforms in real time for event correlation and threat hunting. The platform also inherently detects anomalous behavior and includes those alerts as a part of its audit log.
3.3.6 Audit Record Reduction and Report Generation	a. Implement an audit record reduction and report generation capability that supports on-demand 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 Kiteworks platform provides comprehensive audit logs that can be exported to a SIEM system and analyzed in on-demand reports. Logs include content-specific audit record fields such as username, email addresses, IP address, file or folder names, and event type. Kiteworks also provides a CISO Dashboard, highlighting system issues of interest to CISOs and other security stakeholders and providing an easily readable, visual presentation of activity and anomalous behavior, and both scheduled and ad hoc reporting on user and file activities.

NIST SP 800-171 Requirement	Security Requirement Description	Kiteworks Supports Compliance	Kiteworks Solution
3.3.7 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: 1. Use Coordinated Universal Time (UTC); 2. Have a fixed local time offset from UTC; or 3. Include the local time offset as part of the time stamp	Yes, supports compliance	The Kiteworks platform integrates with Network Time Protocol (NTP) servers to provide authoritative time stamps for audit records, and marks every record with a time stamp.
3.3.8 Protection of Audit Information	Protect audit information and audit logging tools from unauthorized access, modification, and deletion.	Yes, supports compliance	Logs in the Kiteworks platform are protected from editing and deletion. Only specified system administrative users have access to syslog integration settings and Splunk Universal Forwarder settings. Only specified application administrative users have access to log-based reporting. End-users can have access to tracking information as it applies to specific content to which they have ownership or sufficient access rights. Logs generated by the Kiteworks platform can be exported to SIEM systems and other security analysis platforms for event correlation and threat hunting. The platform also inherently detects anomalous behavior and includes those alerts as a part of its audit log.
3.3.9 Audit Information Access	Authorize access to management of audit logging functionality to a subset of privileged users or roles.	Yes, supports compliance	Logs in the Kiteworks platform are protected from editing and deletion. Only specified system administrative users have access to syslog integration settings and Splunk Universal Forwarder settings. No personnel have access to the log repository itself, except for Kiteworks support engineers with temporary permission from the customer and with full logging of all activities.

3.4 Configuration Management

NIST SP 800-171 Requirement	Security Requirement Description	Kiteworks Supports Compliance	Kiteworks Solution
3.4.1 Baseline Configuration	a. Develop, document, 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 upgraded.	Yes, supports compliance	The Kiteworks platform provides one-click compliance reports that can be used to track the baseline configuration of the Kiteworks system. All changes to the system configuration are recorded in the audit log.
3.4.2 Configuration Settings	a. Establish, document, and implement configuration settings for the system that reflect the most restrictive mode consistent with operational requirements using [Assignment: organization-defined common secure configurations]. b. Identify, document, and approve any deviations from established configuration settings. c. Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.	Yes, supports compliance	System administrators on the Kiteworks platform can configure security settings for the platform. Administrators can also configure security settings for users and their mobile devices when those users access CUI under the platform's management. The system defaults to least privilege settings, and warns administrative users when possibly risky settings are used. The system logs all configuration changes.
3.4.3 Configuration Change Control	a. Determine 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	The Kiteworks platform enables system administrators to track, review, and control all changes made to the platform.
3.4.4 Impact Analyses	a. Analyze the security impact of changes to the system prior to implementation. b. After system changes, verify that the impacted controls are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting specified security requirements.	Yes, supports compliance	The Kiteworks platform provides compliance warnings that report configuration changes that degrade security below recommended levels.
3.4.5 Access Restrictions for Change	Define, document, approve, and enforce physical and logical access restrictions associated with changes to the system.	Yes, supports compliance	The Kiteworks platform enforces and logs all logical access restrictions applied to CUI under management.

NIST SP 800-171 Requirement	Security Requirement Description	Kiteworks Supports Compliance	Kiteworks Solution
3.4.6 Least Functionality	(Now incorporates V2 3.4.7) a. Configure the system to provide only mission-essential capabilities. b. Prohibit or restrict use of the following functions, ports, protocols, software, and/or services: [Assignment: organization-defined prohibited or restricted functions, system ports, protocols, software, and/or services]. c. Prevent program execution in accordance with [Selection (one or more): [Assignment: organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions]; rules authorizing the terms and conditions of software program usage]]. d. Review the system [Assignment: organization-defined frequency] to identify and disable/remove functions, ports, protocols, software, and/or services identified in 3.4.6b.	Yes, supports compliance	a. Non-mission-essential capabilities be disabled on a system and/or user role basis. These can be at a coarse level, such as all secure email, or more fine-grained such as mobile device usage. b. The Kiteworks hardened appliance exposes only a few essential ports and services. The system provides no operating system access for users or administrators. The Kiteworks platform ships as a hardened appliance with nonessential services disabled. All unused ports are blocked. Also provided is the ability to enable/disable SFTP/SSH access, to change its port, or to move SFTP and SSH to separate ports. c. Programs cannot be installed in the Kiteworks hardened virtual appliance. Administrators and users have no access to the operating system. Any attempt to install or run an unexpected program is designed to be detected by intrusion detection systems, shut down, and an alert sent to the admin.
3.4.8 Authorized Software – Allow by Exception	a. Identify software programs authorized to execute on the system. b. Implement a deny-all, allow-by-exception policy to allow the execution of authorized software programs on the system. c. Review and update the list of authorized software programs [Assignment: organization-defined frequency].	Yes, supports compliance	Programs cannot be installed in the Kiteworks hardened virtual appliance. Administrators and users have no access to the operating system. Any attempt to install or run an unexpected program is designed to be detected by intrusion detection systems, shut down, and an alert sent to the admin.
3.4.9 User-Installed Software	a. Establish policies governing the installation of software by users. b. Enforce software installation policies through the following methods: [Assignment: organization-defined methods]. c. Monitor policy compliance [Assignment: organization-defined frequency].	Yes, supports compliance	Programs cannot be installed in the Kiteworks hardened virtual appliance. Administrators and users have no access to the operating system. Any attempt to install or run an unexpected program is designed to be detected by intrusion detection systems, shut down, and an alert sent to the admin.

NIST SP 800-171 Requirement	Security Requirement Description	Kiteworks Supports Compliance	Kiteworks Solution
3.4.10 System Component Inventory	a. Develop and document an inventory of system components. b. Review and update the system component inventory [Assignment: organization-defined frequency] and as part of component installations, removals, and system updates.	Yes, supports compliance	The admin console retains up-to-date records of software updates and other network settings.
3.4.11 Information Location	a. Identify and document the location within the system where CUI is processed and stored. b. Identify and document the users who have access to the system where CUI is processed and stored. c. Document changes to the location where CUI is processed and stored.	Yes, supports compliance	All processing happens within the Kiteworks hardened virtual appliance where no users or admins have access. Any content stored on external media, such as NFS, is encrypted and decrypted within the Kiteworks system using keys not accessible to personnel.
3.4.12 System and Component Configuration for High-Risk Areas	a. Issue [Assignment: organization-defined system] with [Assignment: organization-defined system configurations] to individuals traveling to locations that the organization deems to be of significant risk. b. Apply the following controls to the system when the individuals return from travel: [Assignment: organization-defined controls].	Yes, supports compliance	The Kiteworks platform protects CUI at all locations. Remote access to CUI is secured with authentication controls along with other best practices, including the use of secure containers on mobile devices and encryption of all CUI in transit and at rest. Location and IP Range blacklisting can be used to prevent the downloading of CUI in high-risk areas.

3.5 Identification and Authentication

NIST SP 800-171 Requirement	Security Requirement Description	Kiteworks Supports Compliance	Kiteworks Solution
3.5.1 User Identification, Authentication, and Re-Authentication	a. Uniquely identify and authenticate system user, 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 re-authentication].	Yes, supports compliance	The Kiteworks platform assigns individual users unique IDs and uses those IDs to track user activity on the platform across all devices. Users must authenticate to begin a session, and their unique ID ties to access controls for any resource, including access to CUI. Users must reauthenticate after idle timeouts or other events that log them out of the system.
3.5.2 Device Identification and Authentication	Uniquely identify and authenticate [Assignment: organization-defined devices and/or types of devices] before establishing a system or network connection.	Yes, supports compliance	Users must authenticate to begin a session.
3.5.3 Multi-Factor Authentication	Implement multi-factor authentication for access to system accounts.	Yes, supports compliance	The Kiteworks platform can be configured to require multi-factor authentication for any administrative or end-user session. Multi-factor authentication is also enforced through one-time passcodes via email. Alternatively, multi-factor authentication is enforced through integration with third-party authentication solutions that support SMS-based passcodes or the RADIUS protocol. It can also be configured to time out those sessions after a threshold of idle time has been reached.
3.5.4 Replay-Resistant Authentication	Implement replay-resistant authentication mechanisms for access to system accounts.	Yes, supports compliance	The Kiteworks platform can be configured to require multi-factor authentication for any administrative session. Multi-factor authentication is also enforced through one-time passcodes via email. Alternatively, multi-factor authentication is enforced through integration with third-party authentication solutions that support SMS-based passcodes or the RADIUS protocol. It can also be configured to time out those sessions after a threshold of idle time has been reached. This prevents old credential replay. Kiteworks also supports PIV/CAC cards, which use no credentials and are therefore not susceptible to replay.
3.5.5 Identifier Management	a. Receive authorization from [Assignment: organization-defined 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. Identify the status of each individual with the following characteristic: [Assignment: organization-defined characteristic].	Yes, supports compliance	The Kiteworks platform assigns each user a unique ID and tracks all activity on a per-user and per-file basis.

NIST SP 800-171 Requirement	Security Requirement Description	Kiteworks Supports Compliance	Kiteworks Solution
3.5.7 Password Management	(Now contains V2 3.5.9 and 3.5.10) a. Enforce the following password composition and complexity rules: [Assignment: organization-defined composition and complexity rules]. b. Allow user selection of long passwords and passphrases, including spaces and all printable characters. c. Verify, when users create or update passwords, that the passwords are not found on the list of commonly used, expected, or compromised passwords. d. Transmit passwords only over cryptographically protected channels. e. Store passwords using an approved salted key derivation function, preferably using a keyed hash. f. Select a new password immediately upon account recovery. g. Allow the use of a temporary password for system logons with an immediate change to a permanent password.	Yes, supports compliance	The platform enables managers and system administrators to define password configuration requirements, including requirements for password complexity. The Kiteworks platform enables system administrators to reset user passwords and enforce password change upon next logon. Otherwise, users follow an account verification link or password reset link to set or reset their passwords. The Kiteworks platform encrypts passwords in transit and at rest. Passwords at rest are stored as salted hashes. Passwords are never stored or transmitted insecurely.
3.5.11 Authentication Feedback	Obscure feedback of authentication information.	Yes, supports compliance	The Kiteworks platform transmits all authentication information via secure Transport Layer Security (TLS) connections. By default, passwords are not displayed in plain text on screens.
3.5.12 Authenticator Management	a. Establish initial authenticator content for any authenticators issued by the organization. b. Verify the identity of the individual, group, role, service, or device receiving the authenticator as part of the initial authenticator distribution. c. Establish and implement administrative procedures for initial authenticator distribution, for lost, compromised, or damaged authenticators, and for revoking authenticators. d. Protect authenticator content from unauthorized disclosure and modification. e. Change default authenticators prior to first use. f. Change or refresh authenticators [Assignment: organization-defined time period by authenticator type] or when [Assignment: organization-defined events]. g. Change authenticators for group or role accounts when membership to those accounts changes.	Yes, supports compliance	The Kiteworks platform supports the use of external authenticators such as Google Authenticator.

3.6 Incident Response

NIST SP 800-171 Requirement	Security Requirement Description	Kiteworks Supports Compliance	Kiteworks Solution
3.6.1 Incident Response Plan and Handling	a. Develop an incident response plan that provides the organization with a roadmap for implementing its incident response capability. b. Implement an incident-handling capability for incidents that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery. c. Update the incident response plan to address system and organizational changes or problems encountered during plan implementation, execution, or testing.	Yes, supports compliance	Logs generated by the Kiteworks platform can be exported to SIEM systems and other security analysis platforms for event correlation and threat hunting. The platform also inherently detects anomalous behavior and includes those alerts as a part of its audit log.
3.6.2 Incident Monitoring, Reporting, and Response Assistance	a. Track and document system security incidents. b. Report incident information to [Assignment: organization-defined authorities]. c. Provide an incident response support resource that offers advice and assistance to users of the system for the handling and reporting of incidents.	Yes, supports compliance	Logs generated by the Kiteworks platform can be exported to SIEM systems and other security analysis platforms for event correlation and threat hunting. The platform also inherently detects anomalous behavior and includes those alerts as a part of its audit log.
3.6.3 Incident Response Testing	Test the effectiveness of the incident response capability [Assignment: organization-defined frequency].	Out of Scope	N/A
3.6.4 Incident Response Training	a. Provide incident response training to system users consistent with assigned roles and responsibilities. b. Review and update incident response training content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Out of Scope	N/A

3.7 Maintenance

NIST SP 800-171 Requirement	Security Requirement Description	Kiteworks Supports Compliance	Kiteworks Solution

3.7.4 Maintenance Tools	(Now incorporates V2 3.7.2)
	
	a. Approve, control, and monitor the use of system maintenance tools.
	
	b. Inspect maintenance tools and media containing diagnostic and test programs for malicious code before the media and tools are used in the system.
	
	c. Prevent the removal of maintenance equipment containing CUI by:
	
	  1. Verifying that there is no CUI on the equipment;
	
	  2. Sanitizing or destroying the equipment; or
	
	  3. Obtaining an exemption from [Assignment: organization-defined officials] explicitly authorizing removal of the equipment from the facility.
		Yes, supports compliance	The Kiteworks system is a hardened appliance that normally does not facilitate the use of maintenance tools. External drives containing CUI are encrypted with keys not available to administrative users.

3.7.5 Nonlocal Maintenance	a. Approve and monitor nonlocal maintenance and diagnostic activities. b. Implement multi-factor authentication and replay resistance in the establishment of nonlocal maintenance and diagnostic sessions. c. Terminate session and network connections when nonlocal maintenance is completed.	Yes, supports compliance	The Kiteworks platform can be configured to require multi-factor authentication for any administrative session. Multi-factor authentication is also enforced through one-time passcodes via email. Alternatively, multi-factor authentication is enforced through integration with third-party authentication solutions that support SMS-based passcodes or the RADIUS protocol. It can also be configured to time out those sessions after a threshold of idle time has been reached.
3.7.6 Maintenance Personnel	(Now incorporates V2 3.7.2) a. Establish a process for maintenance personnel authorization, and maintain a list of authorized maintenance organizations or personnel. b. Verify that non-escorted personnel who perform maintenance on the system possess the required access authorizations. c. 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	Only privileged users can authenticate and perform maintenance on the system. The Kiteworks platform logs the activities of all users, including maintenance activities of users with varying degrees of privilege.

3.8 Media Protection

NIST SP 800-171 Requirement	Security Requirement Description	Kiteworks Supports Compliance	Kiteworks Solution
3.8.1 Media Storage	Physically control and securely store digital and non-digital media containing CUI until the media are destroyed or sanitized using approved equipment, techniques, and procedures.	Yes, supports compliance	Kiteworks FedRAMP systems encrypt all CUI when stored on media, and physical media is procedurally controlled and audited in data centers used by Kiteworks.
3.8.2 Media Access	Restrict access to CUI on digital and non-digital media to [Assignment: organization-defined personnel or roles].	Yes, supports compliance	The Kiteworks platform protects CUI by encrypting content and enforcing access controls.
3.8.3 Media Sanitization	(Now incorporates V2 3.7.3) Sanitize system media containing CUI prior to maintenance, disposal, release out of organizational control, or release for reuse.	Yes, supports compliance	The Kiteworks platform can perform a remote wipe of CUI in the secure containers on mobile devices that have been lost, stolen, or decommissioned.
3.8.4 Media Marking	a. Mark system media containing CUI indicating distribution limitations, handling caveats, and security markings. b. Exempt [Assignment: organization-defined types of system media containing CUI] from marking if the media remain within [Assignment: organization-defined controlled areas].	Out of Scope	N/A
3.8.5 Media Transport	(Now incorporates V2 3.8.6) a. Protect, control, and maintain accountability for system media containing CUI and during transport outside of controlled areas. b. Implement cryptographic mechanisms to prevent the unauthorized disclosure of CUI stored on digital media during transport.	Yes, supports compliance	The Kiteworks platform enforces access controls on mobile devices regardless of their location and encrypts all CUI at rest with AES-256 encryption twice, once at the file level and again at the disk level.
3.8.7 Media Use	(Now incorporates V2 3.8.8) a. [Selection: Restrict; Prohibit] the use of [Assignment: organization-defined removable system media]. b. Prohibit the use of portable storage devices when such devices have no identifiable owner	Out of Scope	N/A
3.8.9 System Backup – Cryptographic Protection	Implement cryptographic mechanisms to prevent the unauthorized disclosure of CUI at backup storage locations.	Yes, supports compliance	Kiteworks protects the confidentiality of FedRAMP system backups per documented and audited procedures. All CUI is encrypted with a key owned by the customer.

3.9 Personnel Security

NIST SP 800-171 Requirement	Security Requirement Description	Kiteworks Supports Compliance	Kiteworks Solution
3.9.1 Personnel Screening	a. Screen individuals prior to authorizing access to the system. b. Rescreen individuals in accordance with [Assignment: organization-defined conditions requiring rescreening].	Yes, supports compliance	Kiteworks FedRAMP personnel are screened U.S. citizens.

3.9.2 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; and
	
	  3. Retrieve all security-related system property.
	
	b. When individuals are reassigned or transferred to other positions within the organization:
	
	  1. Review and confirm the ongoing operational need for current logical and physical access authorizations to the system and facility;
	
	  2. Initiate [Assignment: organization-defined transfer or reassignment actions] within [Assignment: organization-defined time period following the formal transfer action]; and
	
	  3. Modify access authorization as needed to correspond with any changes in operational need due to reassignment or transfer.
		Yes, supports compliance	The Kiteworks platform protects CUI even when employees or contractors are terminated or transferred. CUI can be remotely wiped from mobile devices, and access to private- or public-cloud repositories can be blocked. Administrators can delete users or change their access control roles (profiles) at the time their responsibilities change.

3.9.3 External Personnel Security	a. Establish and document personnel security requirements, including security roles and responsibilities for external providers. b. Require external providers to comply with the personnel security policies and procedures established by the organization. c. Monitor provider compliance with personnel security requirements.	Out of Scope	N/A

3.10 Physical Protection

NIST SP 800-171 Requirement	Security Requirement Description	Kiteworks Supports Compliance	Kiteworks Solution
3.10.1 Physical Protection	a. Develop, approve, and maintain a list of individuals with authorized access to the facility where the system resides. b. Issue authorization credentials for facility access. c. Review the access list detailing authorized facility access by individuals [Assignment: organization-defined frequency]. d. Remove individuals from the facility access list when access is no longer required.	Yes, supports compliance	Kiteworks FedRAMP systems are deployed in controlled environments with strict, audited procedures that limit physical access.
3.10.2 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]. c. Coordinate the results of reviews and investigations with the organizational incident response capability.	Yes, supports compliance	Kiteworks FedRAMP systems are deployed in controlled environments with strict, audited protection and monitoring.
3.10.6 Alternate Work Site	a. Determine and document alternate work sites allowed for use by employees. b. Employ the following controls at alternate work sites: [Assignment: organization-defined controls].	Yes, supports compliance	The Kiteworks platform protects CUI at all locations. Remote access to CUI is secured with authentication controls along with other best practices, including the use of secure containers on mobile devices and encryption of all CUI in transit and at rest.
3.10.7 Physical Access Control	(Now incorporates V2 3.10.3, 3.10.4, and 3.10.5) a. Enforce physical access authorizations at [Assignment: organization-defined entry and exit points to the facility where the system resides] by: 1. Verifying individual access authorizations before granting access to the facility; and 2. Controlling ingress and egress to the facility using [Selection (one or more): [Assignment: organization-defined physical access control systems or devices]; guards]. b. Maintain physical access audit logs for [Assignment: organization-defined entry or exit points]. c. Escort visitors and control visitor activity [Assignment: organization-defined circumstances requiring visitor escorts and control of visitor activity]. d. Secure keys, combinations, and other physical access devices.	Yes, supports compliance	Kiteworks maintains audit logs of all physical access of FedRAMP systems. Kiteworks FedRAMP systems are deployed and managed in controlled environments with strict, audited procedures that control card readers, access cards, and other access devices.
3.10.8 Access Control for Transmission and Output Devices	a. Control physical access to system distribution and transmission lines within organizational facilities. b. Control physical access to output from [Assignment: organization-defined output devices] to prevent unauthorized individuals from obtaining the output.	Yes, supports compliance	Kiteworks FedRAMP systems are deployed in controlled environments with strict, audited procedures that limit physical access.

3.11 Risk Assessment

NIST SP 800-171 Requirement	Security Requirement Description	Kiteworks Supports Compliance	Kiteworks Solution
3.11.1 Risk Assessment	a. Assess the risk (including supply chain risk) of unauthorized disclosure resulting from the processing, storage, or transmission of CUI. b. Update risk assessments (including supply chain risk) [Assignment: organization-defined frequency].	Out of Scope	N/A
3.11.2 Vulnerability Monitoring and Scanning	(Now incorporates V2 3.11.3) a. Monitor and scan for vulnerabilities in the system [Assignment: organization-defined frequency] and when new vulnerabilities affecting the system are identified. b. Remediate vulnerabilities [Assignment: organization-defined response times] in accordance with an organizational assessment of risk. c. Update vulnerabilities to be scanned [Assignment: organization-defined frequency]. d. Implement privileged access authorization to the system for vulnerability scanning activities.	Yes, supports compliance	Kiteworks security engineers regularly scan the code base to discover new vulnerabilities. Kiteworks security engineers prioritize and release fixes per a documented secure software development life cycle. Kiteworks products, whether hosted or deployed on the customer's premises, can detect the availability of new updates and apply them with a click. The Kiteworks organization offers updates as a service as part of the Premium Support package.
3.11.4 Risk Response	Respond to findings from security assessments, monitoring, and audits.	Yes, supports compliance	Kiteworks engineering responds to findings from penetration tests, bounty programs, and other methods. Kiteworks provides timely patches and updates as appropriate when vulnerabilities are discovered.

3.12 Security Assessment

NIST SP 800-171 Requirement	Security Requirement Description	Kiteworks Supports Compliance	Kiteworks Solution
3.12.1 Control Assessments	Assess the controls in the system and its environment of operation [Assignment: organization-defined frequency] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting specified security requirements.	Yes, supports compliance	Kiteworks is SOC 2 certified, FedRAMP Authorized, and FIPS 140-2 compliant, following all of the guidelines and reviews therein. The system produces warnings when admins select potentially risky settings.
3.12.2 Plan of Action and Milestones	(Now incorporates V2 3.12.4) a. Develop a plan of action and milestones for the system: 1. To document the planned remediation actions to correct weaknesses or deficiencies noted during control assessments; and 2. To reduce or eliminate known vulnerabilities in the system. b. Update the existing plan of action and milestones [Assignment: organization-defined frequency] based on the findings from control assessments, independent audits or reviews, and continuous monitoring activities.	Yes, supports compliance	Kiteworks is SOC 2 certified, FedRAMP Authorized, and FIPS 140-2 compliant, following all of the guidelines and reviews therein.
3.12.3 Continuous Monitoring	Develop and implement a system-level continuous monitoring strategy that includes ongoing monitoring and assessment of control effectiveness.	Yes, supports compliance	Kiteworks FedRAMP security controls and incidents are audited yearly by the Third Party Assessor Organization (3PAO).
3.12.5 Independent Assessment	Use independent assessors or assessment teams to assess controls.	Yes, supports compliance	Kiteworks FedRAMP security controls and incidents are audited yearly by the Third Party Assessor Organization (3PAO).
3.12.6 Information Exchange	a. Approve, document, and manage the exchange of CUI between the system and other systems using [Assignment: organization-defined agreements]. b. Review and update the agreements [Assignment: organization-defined frequency].	Out of Scope	N/A
3.12.7 Internal System Connections	a. Authorize internal system connections of [Assignment: organization-defined system components or classes of components]. b. Review the continued need for each internal system connection [Assignment: organization-defined frequency].	Out of Scope	N/A

3.13 System and Communications Protection

NIST SP 800-171 Requirement	Security Requirement Description	Kiteworks Supports Compliance	Kiteworks Solution
3.13.1 Boundary Protection	(Now incorporates V2 3.13.5) a. Monitor and control communications at the external managed interfaces to the system and at 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 networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.	Yes, supports compliance	The Kiteworks platform monitors, controls, and protects CUI at rest as well as when shared with internal or external users. The platform ensures the security of CUI shared across organizational boundaries. The Kiteworks platform tiered architecture allows web interfaces and other system functions to be deployed in network DMZs for public access, while ensuring that application logic and CUI storage remain on internal networks, and can connect to multiple network segments to access resources such as file repositories.
3.13.3 Separation of System and User Functionality	Separate user functionality from system management functionality.	Yes, supports compliance	The Kiteworks platform enforces security controls specific to user roles, including system administrators, CUI managers, and end-users. Unprivileged users never gain access to system management functionality. The Kiteworks platform prevents unauthorized access or sharing of CUI.
3.13.4 Information in Shared System Resources	Prevent unauthorized and unintended information transfer via shared system resources.	Yes, supports compliance	Only authorized users and processes can access and share CUI
3.13.6 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 Kiteworks platform supports the whitelisting and blacklisting of IP addresses and can be configured to deny network traffic by default. Only authenticated sessions can transfer files, and only within limits of access controls.
3.13.7 Split Tunneling	Prevent split tunneling for remote devices unless the split tunnel is securely provisioned using [Assignment: organization-defined safeguards].	Out of Scope	N/A
3.13.8 Transmission and Storage Confidentiality	(Now incorporates V2 3.13.16) Implement cryptographic mechanisms to prevent the unauthorized disclosure of CUI during transmission and while in storage.	Yes, supports compliance	The Kiteworks platform encrypts CUI in transit using Transport Layer Security, TLS 1.3 or above only. The Kiteworks platform protects the confidentiality of CUI at rest through the enforcement of strict access controls and the use of AES-256 encryption. In addition, CUI at rest on mobile devices is stored in an encrypted secure container that shields the CUI from access from other applications and processes.
3.13.9 Network Disconnect	Terminate network connections associated with communications sessions at the end of the sessions or after [Assignment: organization-defined time period] of inactivity.	Yes, supports compliance	The Kiteworks platform enables system administrators to set session timeout policies, disconnecting users after a defined period of inactivity.

NIST SP 800-171 Requirement	Security Requirement Description	Kiteworks Supports Compliance	Kiteworks Solution
3.13.10 Cryptographic Key Establishment and Management	Establish and manage cryptographic keys when cryptography is implemented 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	The Kiteworks platform uses keys to encrypt content in transit and at rest. Kiteworks customers have full ownership of their cryptographic keys. Keys can be managed directly within the Kiteworks platform or stored in a Hardware Security Module. Administrators have the ability to rotate keys.
3.13.11 Cryptographic Protection	Implement the following types of cryptography when used to protect the confidentiality of CUI: [Assignment: organization-defined types of cryptography].	Yes, supports compliance	The Kiteworks platform is available in a FIPS 140-2 configuration. See the Security Architecture White Paper for a list of encryption methods and ciphers.
3.13.12 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.	Out of Scope	N/A
3.13.13 Mobile Code	a. Define acceptable and unacceptable mobile code and mobile code technologies. b. Authorize, control, and monitor the use of mobile code.	Yes, supports compliance	Kiteworks uses secure coding practices and abides by OWASP Top 10 mitigation strategies. Our SDLC is rigorously reviewed and tested, as attested and verified through our SOC 2, FedRAMP, IRAP, and FIPS-140 certifications/audits. Admins can enable/disable the use of mobile clients with Kiteworks.
3.13.15 Session Authenticity	Protect the authenticity of communications sessions.	Yes, supports compliance	The Kiteworks platform protects the authenticity of communications sessions in compliance with NIST 800-53, SC-23. Specifically, the platform invalidates session identifiers upon user logout or other session termination, generates a unique session identifier for each session with predefined randomness requirements and recognizes only session identifiers that are system generated, and uses only predefined certificate authorities for verification of the establishment of protected sessions.
3.13.17 Internal Network Communications Traffic	Route internal network communications traffic to external networks through an authenticated proxy server.	Yes, supports compliance	Kiteworks supports the use of proxy servers, providing an additional layer of security and control for organizations. The platform's support for proxy servers allows organizations to control and monitor their network traffic, enhancing visibility and aiding in threat detection and prevention.
3.13.18 System Access Points	Limit the number of external network connections to the system.	Yes, supports compliance	The Kiteworks architecture allows customers to limit external network connections. Content communications use a limited set of protocols such as HTTPS, SFTP, and FTPS. Special protocols are used for optionally accessing the Kiteworks update server for uploading telemetry and downloading software updates. Customers have the option of running "air gapped" with no internet access whatsoever; Kiteworks Support provides offline update packages for these customers.

3.14 System and Information Integrity

NIST SP 800-171 Requirement	Security Requirement Description	Kiteworks Supports Compliance	Kiteworks Solution
3.14.1 Flaw Remediation	a. Identify, report, and correct system flaws. b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation. c. 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 the Kiteworks platform and prioritizes and resolves these vulnerabilities based on impact and severity. Kiteworks provides updates that work like a smartphone: the admin checks for an update and then clicks a button to apply it to each server in the system. Offline updates work in a similar manner against an update file.
3.14.2 Malicious Code Protection	(Now incorporates V2 3.14.4 and 3.14.5) a. Implement malicious code protection mechanisms at designated locations within the system to detect and eradicate malicious code. b. Update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures.	Yes, supports compliance	The Kiteworks development organization guards against malicious code in its formal secure software development process. It also runs open source code in a sandbox so any malware or vulnerability in the code will not be able to infect the system. The Kiteworks software distribution process uses encryption and other protections to ensure malware has not been introduced.
3.14.3 Security Alerts, Advisories, and Directives	a. Receive security alerts, advisories, and directives from external organizations. b. Generate internal security alerts, advisories, and directives, as necessary.	Yes, supports compliance	The Kiteworks organization carefully tracks and maintains contact information for delivering alerts, advisories, and directives to your organization, and the product also alerts admins to update this information quarterly.

3.14.6 System Monitoring	a. Monitor the system, including inbound and outbound communications traffic, to detect:
	   1. Attacks and indicators of potential attacks;
	   2. Unusual or unauthorized activities or conditions; and
	   3. Unauthorized connections.
	
	b. Identify unauthorized use of the system.
		Yes, supports compliance	The Kiteworks platform monitors all communications under management for signs of failed login attempts, internal intrusions, attempts to alter or run code unexpectedly, malware, and other security anomalies that could signal the presence of an attack. Its comprehensive audit log tracks all use of the system, and feeds it to external SIEMs and other security systems via syslogs and the Splunk Universal Forwarder.

3.14.8 Spam Protection	a. Implement spam protection mechanisms at designated locations within the system to detect and act on unsolicited messages. b. Update spam protection mechanisms [Assignment: organization-defined frequency].	Out of Scope	N/A

3.15 Planning

NIST SP 800-171 Requirement	Security Requirement Description	Kiteworks Supports Compliance	Kiteworks Solution
3.15.1 Policy and Procedures	a. Develop, document, and disseminate to organizational personnel or roles, policies and procedures needed to implement security requirements. b. Review and update policies and procedures [Assignment: organization-defined frequency].	Out of Scope	N/A

3.15.2 System Security Plan	a. Develop and document a system security plan that describes:
	
	  1. System boundary and operating environment;
	
	  2. Security requirements, tailoring actions, and implementation; and
	
	  3. Connections to other systems.
	
	b. Review and update the plan at [Assignment: organization-defined frequency].
		Out of Scope	N/A

3.15.3 Rules of Behavior	a. Establish and provide to individuals requiring access to the system, the rules that describe their responsibilities and expected behavior for handling CUI and system usage. b. Review and update the rules of behavior [Assignment: organization-defined frequency].	Yes, supports compliance	The Kiteworks platform can be customized to display privacy and security notices required by an organization.

3.16 System and Services Acquisition

NIST SP 800-171 Requirement	Security Requirement Description	Kiteworks Supports Compliance	Kiteworks Solution
3.16.1 Security Engineering Principles	Apply systems security engineering principles in the specification, design, development, implementation, and modification of the system and system components.	Yes, supports compliance	Kiteworks is SOC 2 certified, FedRAMP Authorized, and FIPS 140-2 compliant, following all of the guidelines and reviews therein. Kiteworks applies a secure software development life cycle (SDLC) process using principles of OWASP, SANS, CWE, CVSS v3-based vulnerability management, defensive and offensive security processes, as well as automated testing, penetration testing, and a bug bounty program.
3.16.2 Unsupported System Components	a. Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer; or b. Provide options for alternative sources for continued support for unsupported components.	Yes, supports compliance	Kiteworks replaces internal components of the hardened virtual appliance as needed to maintain support. Kiteworks customers simply click on an update to apply the changes to their system in most cases.
3.16.3 External System Services	a. Require the providers of external system services to comply with organizational security requirements, and implement the following controls: [Assignment: organization-defined controls]. b. Define and document organizational oversight and user roles and responsibilities with regard to external system services. c. Implement the following processes, methods, and techniques to monitor control compliance by external service providers on an ongoing basis: [Assignment: organization-defined processes, methods, and techniques].	Yes, supports compliance	System administrators on the Kiteworks platform can configure security settings for the platform. Administrators can also configure security settings for users and their mobile devices when those users access CUI under the platform's management.

3.17 Supply Chain Risk Management Plan

NIST SP 800-171 Requirement	Security Requirement Description	Kiteworks Supports Compliance	Kiteworks Solution
3.17.1 Supply Chain Risk Management Plan	a. Develop a plan for managing supply chain risks associated with the development, manufacturing, acquisition, delivery, operations, maintenance, and disposal of the system, system components, or system services. b. Review and update the plan [Assignment: organization-defined frequency].	Out of Scope	N/A
3.17.2 Acquisition Strategies, Tools, and Methods	Develop and implement acquisition strategies, contract tools, and procurement methods to protect against, identify, and mitigate supply chain risks.	Out of Scope	N/A
3.17.3 Supply Chain Controls and Processes	a. Establish a process or processes for identifying and addressing weaknesses or deficiencies in the supply chain elements and processes. b. Employ the following controls to protect against supply chain risks to the system, system component, or system service and to limit the harm or consequences from supply chain related events: [Assignment: organization-defined supply chain controls].	Out of Scope	N/A
3.17.4 Component Disposal	Dispose of system components, documentation, or tools containing CUI using the following techniques and methods: [Assignment: organization-defined techniques and methods].	Yes, supports compliance	Kiteworks secure container and remote wipe functionality enable the removal of access to corporate data.

The information provided on this page does not, and is not intended to, constitute legal advice; instead, all information, content, and materials available on this page are for general informational purposes only. Information on this website may not constitute the most up-to-date legal or other information.