Kiteworks

NIST 800-171 Compliance Guide



1 Introduction

3 The Kiteworks Secure File Sharing and Governance Platform

4 The Kiteworks Platform and NIST 800-171

4 3.1 Access Control

8 3.2 Awareness and Training

9 3.3 Audit and Accountability

11 3.4 Configuration Management

13 3.5 Identification and Authentication

15 3.6 Incident Response

16 3.7 Maintenance

17 3.8 Media Protection

18 3.9 Personnel Security

19 3.10 Physical Protection

20 3.11 Risk Assessment

21 3.12 Security Assessment

22 3.13 System and Communications Protection

25 3.14 System and Information Integrity

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 CU Registry—the government service for tracking CUI—has identified 85 subcategories.[2]

[1] NIST 800-171, Revision 1, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/final

[2] Controlled Unclassified Information: Executive Order 13556
https://csrc.nist.gov/csrc/media/projects/forum/documents/feb2014/pviscuso_cui-briefing.pdf



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 14 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 security

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
https://library.educause.edu/~/media/files/library/2016/4/nist800.pdf

[4] Ibid.

The Kiteworks Secure File Sharing and Governance Platform

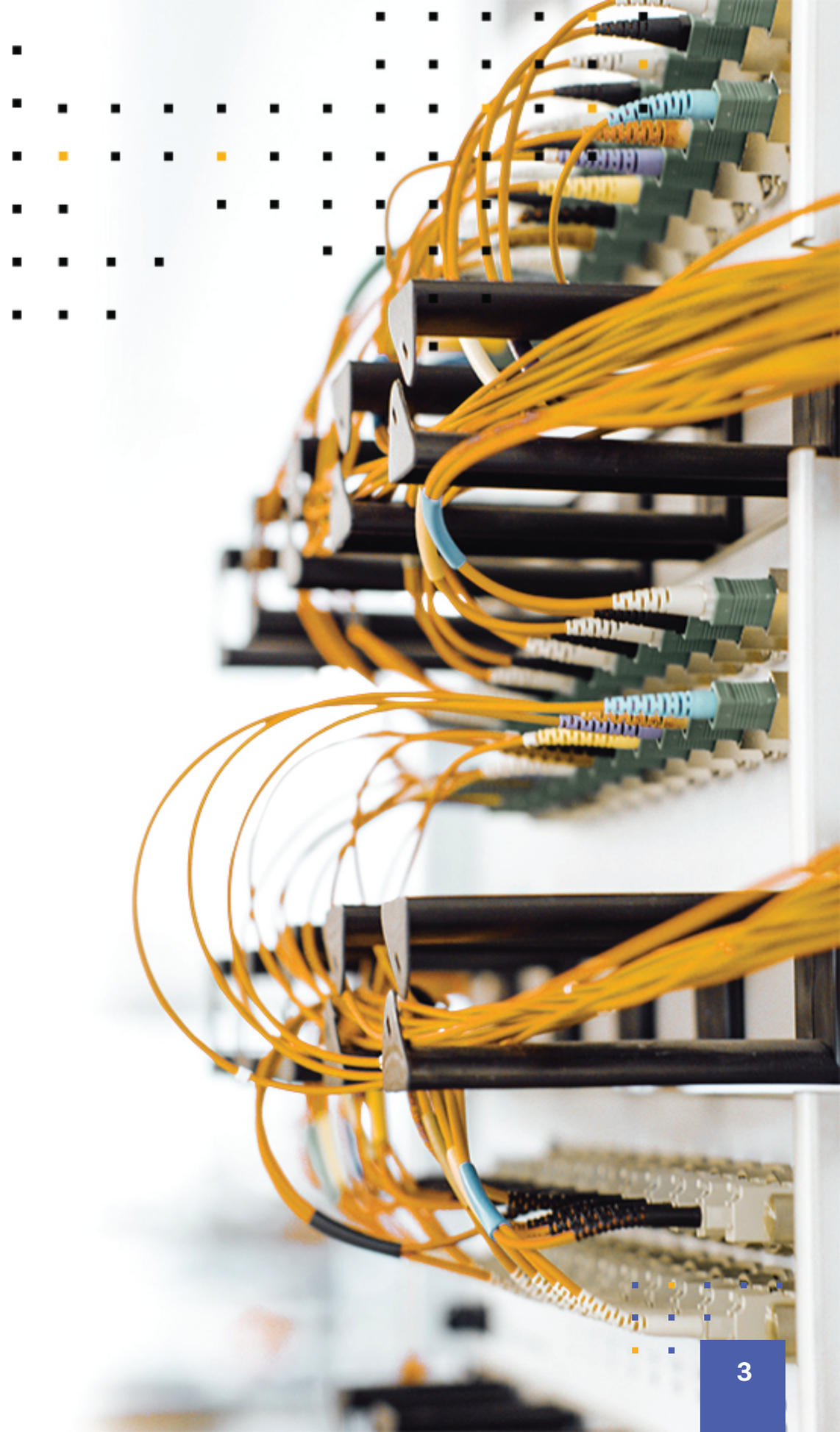
Kiteworks' FedRAMP- and FIPS-140-2-compliant file sharing and governance platform enables enterprises to share sensitive information quickly and securely while maintaining full visibility and control over their file-sharing activities. The Kiteworks platform provides:

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 comply with NIST 800-171.

3.1 Access Control

NIST 800-171 Requirement	Details	How Kiteworks Supports NIST 800-171 Compliance
3.1.1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	The Kiteworks platform enforces strict access controls to protect all content, including CUI, under management.
3.1.2	Limit system access to the types of transactions and functions that authorized users are permitted to execute.	System administrators and content owners can control who receives which type of access: view and edit, view only, or access denied.
3.1.3	Control the flow of CUI in accordance with approved authorizations.	Administrators and content owners can ensure that non-authorized users never gain access to CUI. Kiteworks Automation Agents 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	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	Administrators can define different roles and access levels for CUI, reducing the risk of collusion.
3.1.5	Employ the principle of least privilege, including for specific security functions and privileged accounts.	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.

NIST 800-171 Requirement	Details	How Kiteworks Supports NIST 800-171 Compliance
3.1.6	Use non-privileged accounts or roles when accessing nonsecurity functions.	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	Prevent non-privileged users from executing privileged functions and audit the execution of such functions.	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.
3.1.8	Limit unsuccessful logon attempts.	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	Provide privacy and security notices consistent with applicable CUI rules.	The Kiteworks platform can be customized to display privacy and security notices required by an organization.
3.1.10	Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.	The Kiteworks platform locks sessions after a period of inactivity, though it does not use pattern-hiding displays.
3.1.11	Terminate (automatically) a user session after a defined condition.	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	Monitor and control remote access sessions.	The Kiteworks platform monitors and logs all remote access to CUI. All remote access is governed through strict access control policies. System administrators can monitor and manually terminate active sessions.

NIST 800-171 Requirement	Details	How Kiteworks Supports NIST 800-171 Compliance
3.1.13	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	The Kiteworks platform encrypts all transmission of content using Transport Layer Security (TLS). The platform also encrypts content at rest using AES-256 encryption.
3.1.14	Route remote access via managed access control points.	The Kiteworks platform enables system administrators to control which nodes (servers) are available for client access (HTTPS or SFTP).
3.1.15	Authorize remote execution of privileged commands and remote access to security-relevant information.	The Kiteworks platform provides a separate administrative interface that requires authentication and provides its own IP access restrictions.
3.1.16	Authorize wireless access prior to allowing such connections.	The Kiteworks platform provides flexible deployment options with some or all of the Kiteworks servers behind the corporate firewall.
3.1.17	Protect wireless access using authentication and encryption.	The Kiteworks platform uses authentication and encryption regardless of transport mechanism, protecting both wired and wireless access.
3.1.18	Control connection of mobile devices.	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.
3.1.19	Encrypt CUI on mobile devices and mobile computing platforms.	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.

NIST 800-171 Requirement	Details	How Kiteworks Supports NIST 800-171 Compliance
3.1.20	Verify and control/limit connections to and use of external systems.	The Kiteworks platform provides controlled access to cloud enterprise content management systems like Google Drive, Box, Dropbox, Microsoft OneDrive, and Microsoft SharePoint Online.
3.1.21	Limit use of organizational portable storage devices on external systems.	N/A
3.1.22	Control CUI posted or processed on publicly accessible systems.	The Kiteworks platform can be deployed as a private or hybrid cloud or as a private hosted deployment in an isolated environment or AWS, per FedRAMP requirements.

3.2 Awareness and Training

NIST 800-171 Requirement	Details	How Kiteworks Supports NIST 800-171 Compliance
3.2.1	Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.	The Kiteworks platform issues alerts when security violations occur, making managers, system administrators, and others aware of activities that jeopardize the security of CUI.
3.2.2	Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.	The Kiteworks platform's alerts help reinforce security training by displaying instructions or warnings as recommended when users are logging in. In addition, the platform's alerts remind users of possible security violations and preferred practices.
3.2.3	Provide security awareness training on recognizing and reporting potential indicators of insider threat.	The Kiteworks platform's logs can be used when training users to recognize potential indicators of insider threats.



3.3 Audit and Accountability

NIST 800-171 Requirement	Details	How Kiteworks Supports NIST 800-171 Compliance
3.3.1	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	The Kiteworks platform logs all access to and sharing of content. Administrators and managers can generate reports for use in security investigations.
3.3.2	Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.	The Kiteworks platform assigns each user a unique ID and tracks all activity on a per-user and per-file basis.
3.3.3	Review and update logged events.	The Kiteworks platform enables system administrators and CUI managers to review logged events.
3.3.4	Alert in the event of an audit logging process failure.	The Kiteworks platform alerts administrators in the event of a logging process failure.
3.3.5	Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.	Logs generated by the Kiteworks platform can be exported to SIEM systems and other security analysis platforms for event correlation and threat hunting.
3.3.6	Provide audit record reduction and report generation to support on-demand analysis and reporting.	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.

NIST 800-171 Requirement	Details	How Kiteworks Supports NIST 800-171 Compliance
3.3.7	Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.	The Kiteworks platform integrates with Network Time Protocol (NTP) servers to provide authoritative time stamps for audit records.
3.3.8	Protect audit information and audit logging tools from unauthorized access, modification, and deletion.	Logs in the Kiteworks platform are protected from editing and deletion.
3.3.9	Limit management of audit logging functionality to a subset of privileged users.	By default, the Kiteworks platform limits access to audit logging features to system administrators. The platform protects audit logs and administrative features with configurable access controls.



3.4 Configuration Management

NIST 800-171 Requirement	Details	How Kiteworks Supports NIST 800-171 Compliance
3.4.1	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	The Kiteworks platform provides one-click compliance reports that can be used to track the baseline configuration of the Kiteworks system.
3.4.2	Establish and enforce security configuration settings for information technology products employed in organizational systems.	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.
3.4.3	Track, review, approve or disapprove, and log changes to organizational systems.	The Kiteworks platform enables system administrators to track, review, and control all changes made to the platform.
3.4.4	Analyze the security impact of changes prior to implementation.	The Kiteworks platform provides compliance audits that report configuration changes that degrade security below recommended levels.
3.4.5	Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.	The Kiteworks platform enforces and logs all logical access restrictions applied to CUI under management.
3.4.6	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	System administrators can configure the Kiteworks platform to employ the principle of least functionality, restricting features to only essential capabilities.

NIST 800-171 Requirement	Details	How Kiteworks Supports NIST 800-171 Compliance
3.4.7	Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.	The Kiteworks platform ships as a hardened appliance with nonessential services disabled. All unused ports are blocked. We also provide the ability to enable/disable SFTP/SSH access.
3.4.8	Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.	The Kiteworks platform enforces whitelisting of apps on mobile devices accessing the platform.
3.4.9	Control and monitor user-installed software.	The Kiteworks platform enforces mobile app whitelisting, preventing unauthorized apps from accessing CUI.



3.5 Identification and Authentication

NIST 800-171 Requirement	Details	How Kiteworks Supports NIST 800-171 Compliance
3.5.1	Identify system users, processes acting on behalf of users, and devices.	The Kiteworks platform assigns individual users unique IDs and uses those IDs to track user activity on the platform across all devices.
3.5.2	Establish and enforce security configuration settings for information technology products employed in organizational systems.	The Kiteworks platform enables managers and system administrators to define security policies for the platform itself.
3.5.3	Track, review, approve or disapprove, and log changes to organizational systems.	Only authorized administrators may make changes to the Kiteworks platform. All changes are logged.
3.5.4	Analyze the security impact of changes prior to implementation.	N/A
3.5.5	Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.	The Kiteworks platform logs all changes made to the platform.
3.5.6	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	The platform enables administrators to apply the principle of least functionality when assigning user roles and setting access permissions.
3.5.7	Enforce a minimum password complexity and change of characters when new passwords are created.	The platform enables managers and system administrators to define password configuration requirements, including requirements for password complexity.

NIST 800-171 Requirement	Details	How Kiteworks Supports NIST 800-171 Compliance
3.5.8	Prohibit password reuse for a specified number of generations.	The Kiteworks platform can be configured to prohibit password reuse.
3.5.9	Allow temporary password use for system logons with an immediate change to a permanent password.	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.
3.5.10	Store and transmit only cryptographically protected 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 unsecurely.
3.5.11	Obscure feedback of authentication information.	The Kiteworks platform transmits all authentication information using secure Transport Layer Security (TLS) connections. By default, passwords are not displayed in plaintext on screens.

3.6 Incident Response

NIST 800-171 Requirement	Details	How Kiteworks Supports NIST 800-171 Compliance
3.6.1	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	N/A
3.6.2	Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.	The Kiteworks platform logs incidents and generates alerts when suspicious or malicious incidents occur.
3.6.3	Test the organizational incident response capability.	N/A



3.7 Maintenance

NIST 800-171 Requirement	Details	How Kiteworks Supports NIST 800-171 Compliance
3.7.1	Perform maintenance on organizational systems.	N/A
3.7.2	Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.	The Kiteworks platform limits access to configuration and maintenance controls to authorized users such as system administrators.
3.7.3	Ensure equipment removed for off-site maintenance is sanitized of any CUI.	The Kiteworks platform can perform a remote wipe of the secure containers on mobile devices that have been lost, stolen, or decommissioned.
3.7.4	Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.	The Kiteworks platform scans CUI for viruses and other malware by default, using F-Secure Anti-Virus software. The platform integrates with Check Point SandBlast and APIs enable integration with other Advanced Threat Prevention technologies to scan CUI for advanced persistent threats and Zero Day attacks.
3.7.5	Require multi-factor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance.	The Kiteworks platform can be configured to require multi-factor authentication for any administrative session. Multi-factor authentication is enforced through integration with third-party authentication solutions that support 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	Supervise the maintenance activities of maintenance personnel without required access authorization.	The Kiteworks platform logs the activities of all users, including maintenance activities of users with varying degrees of privilege.

3.8 Media Protection

NIST 800-171 Requirement	Details	How Kiteworks Supports NIST 800-171 Compliance
3.8.1	Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.	N/A
3.8.2	Limit access to CUI on system media to authorized users.	The Kiteworks platform protects CUI by encrypting content and enforcing access controls.
3.8.3	Sanitize or destroy system media containing CUI before disposal or release for reuse.	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	Mark media with necessary CUI markings and distribution limitations.	N/A
3.8.5	Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.	The Kiteworks platform enforces access controls on mobile devices regardless of their location.
3.8.6	Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.	The Kiteworks platform encrypts all CUI at rest with AES-256 encryption.
3.8.7	Control the use of removable media on system components.	N/A

NIST 800-171 Requirement	Details	How Kiteworks Supports NIST 800-171 Compliance
3.8.8	Prohibit the use of portable storage devices when such devices have no identifiable owner.	N/A
3.8.9	Protect the confidentiality of backup CUI at storage locations.	The Kiteworks platform encrypts and enforces access controls for all CUI under management, including CUI on redundant servers.

3.9 Personnel Security

NIST 800-171 Requirement	Details	How Kiteworks Supports NIST 800-171 Compliance
3.9.1	Screen individuals prior to authorizing access to organizational systems containing CUI.	The Kiteworks platform permits access to CUI only to authorized users.
3.9.2	Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.	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.

3.10 Physical Protection

NIST 800-171 Requirement	Details	How Kiteworks Supports NIST 800-171 Compliance
3.10.1	Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.	N/A
3.10.2	Protect and monitor the physical facility and support infrastructure for organizational systems.	N/A
3.10.3	Escort visitors and monitor visitor activity.	N/A
3.10.4	Maintain audit logs of physical access.	N/A
3.10.5	Control and manage physical access devices.	N/A
3.10.6	Enforce safeguarding measures for CUI at alternate work sites.	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.

3.11 Risk Assessment

NIST 800-171 Requirement	Details	How Kiteworks Supports NIST 800-171 Compliance
3.11.1	Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.	The Kiteworks platform contributes to risk assessment with administrative dashboards and built-in reporting for compliance with industry regulations.
3.11.2	Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.	The Kiteworks platform scans CUI for malware with F-Secure Anti-Virus software. The platform integrates with Check Point SandBlast and APIs enable integration with other Advanced Threat Prevention technologies to scan CUI for advanced persistent threats and Zero Day attacks.
3.11.3	Remediate vulnerabilities in accordance with risk assessments.	System administrators and security personnel can use the Kiteworks platform to adjust configurations and automated workflows involving CUI in response to risk assessments.



3.12 Security Assessment

NIST 800-171 Requirement	Details	How Kiteworks Supports NIST 800-171 Compliance
3.12.1	Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.	The Kiteworks platform features built-in compliance reports to make security assessment quick and easy for system administrators and CUI managers.
3.12.2	Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.	N/A
3.12.3	Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.	N/A
3.12.4	Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.	N/A

3.13 System and Communications Protection

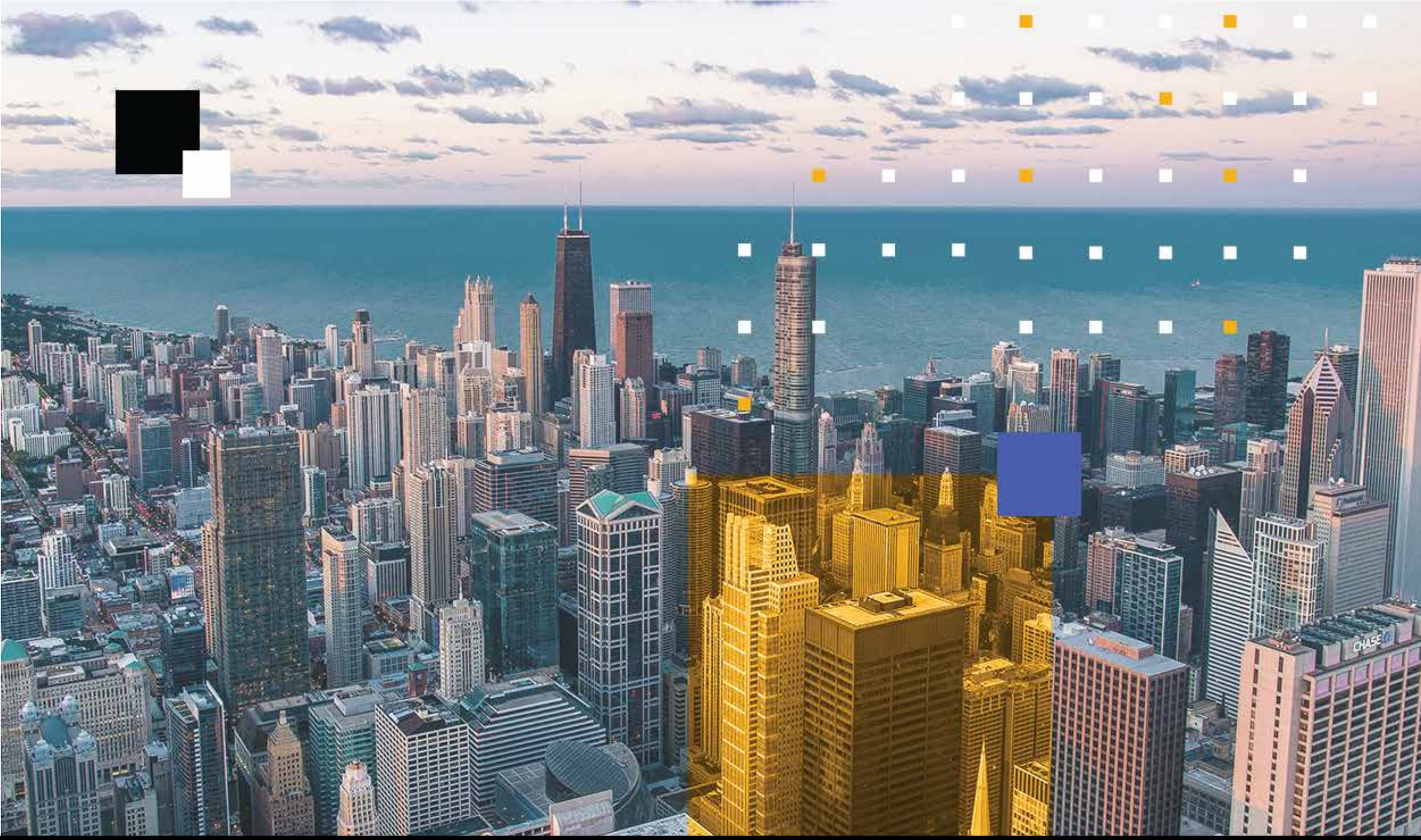
NIST 800-171 Requirement	Details	How Kiteworks Supports NIST 800-171 Compliance
3.13.1	Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.	The Kiteworks platform 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.
3.13.2	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	The Kiteworks platform has been designed and developed with information security in mind. The platform's tiered architecture separates functionality, improves scalability, and supports the enforcement of data sovereignty policies. The platform's source code is routinely analyzed for quality and security. The platform's availability on a private or hybrid cloud or as a private hosted deployment in an isolated environment on AWS enables customers to adopt the deployment model that best suits their security needs.
3.13.3	Separate user functionality from system management functionality.	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.
3.13.4	Prevent unauthorized and unintended information transfer via shared system resources.	The Kiteworks platform prevents unauthorized access or sharing of CUI. Only authorized users and processes can access and share CUI.
3.13.5	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	The Kiteworks platform's tiered architecture allows web interfaces and other system functions to be deployed outside network DMZs for public access, while ensuring that application logic and CUI storage remain on internal networks.

NIST 800-171 Requirement	Details	How Kiteworks Supports NIST 800-171 Compliance
3.13.6	Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).	The Kiteworks platform supports the whitelisting and blacklisting of IP addresses and can be configured to deny network traffic by default.
3.13.7	Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).	N/A
3.13.8	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	The Kiteworks platform encrypts CUI in transit using Transport Layer Security. System administrators can configure the platform not to accept TLS 1.0 or 1.1 connections.
3.13.9	Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.	The Kiteworks platform enables system administrators to set session timeout policies, disconnecting users after a defined period of inactivity.
3.13.10	Establish and manage cryptographic keys for cryptography employed in organizational systems.	The Kiteworks platform uses keys to encrypt content in transit and at rest. Kiteworks customers have full ownership of their cryptographic keys.
3.13.11	Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.	The Kiteworks platform is available in a FIPS 140-2 configuration.
3.13.12	Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.	N/A

NIST 800-171 Requirement	Details	How Kiteworks Supports NIST 800-171 Compliance
3.13.13	Control and monitor the use of mobile code.	Kiteworks provides a Java applet for compatibility with older browser technologies. The applet can be disabled by system administrators.
3.13.14	Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.	N/A
3.13.15	Protect the authenticity of communications sessions.	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 pre-defined randomness requirements and recognizes only session identifiers that are system-generated, and uses only pre-defined certificate authorities for verification of the establishment of protected sessions.
3.13.16	Protect the confidentiality of CUI at rest.	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 a secure container that shields the CUI from access from other applications and processes.

3.14 System and Information Integrity

NIST 800-171 Requirement	Details	How Kiteworks Supports NIST 800-171 Compliance
3.14.1	Identify, report, and correct system flaws in a timely manner.	Kiteworks monitors and reviews vulnerabilities in the Kiteworks platform and prioritizes and resolves these vulnerabilities based on impact and severity.
3.14.2	Provide protection from malicious code at designated locations within organizational systems.	The Kiteworks platform protects against malicious code by scanning CUI entering or exiting the platform for viruses, advanced persistent threats, and Zero Day attacks. On mobile devices, it stores CUI in secure containers (protected areas of storage and memory) that shield CUI from malware infection.
3.14.3	Monitor system security alerts and advisories and take action in response.	The Kiteworks platform can be configured to export logs to SIEM systems being used for security monitoring and alerts.
3.14.4	Update malicious code protection mechanisms when new releases are available.	The Kiteworks platform automatically applies updates to its integrated anti-malware solutions from F-Secure and Check Point.
3.14.5	Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.	The Kiteworks platform scans all uploaded files for infections of malware and indications of Zero Day threats. When integrated with a Data Loss Prevention (DLP) service, the platform can also scan content and block or quarantine any CUI transmissions that might violate DLP policies.
3.14.6	Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	The Kiteworks platform monitors all communications under management for signs of malware and other security anomalies that could signal the presence of an attack.
3.14.7	Identify unauthorized use of organizational systems.	The Kiteworks platform identifies access attempts by unauthorized users.



Kiteworks

For more information, please visit www.kiteworks.com or call (650) 249-9544.
Follow Kiteworks on LinkedIn, Twitter, and Kiteworks' Blog.
© 2021 KITEWORKS. All rights reserved