Kiteworks

GUIDE

Kiteworks' Guide to the Saudi Arabia National Cybersecurity Authority (NCA) Data Cybersecurity Controls (DCC)

Navigating Governance, Protection, and Resilience for Robust Data Cybersecurity

Introduction

The National Cybersecurity Authority (NCA) of Saudi Arabia has introduced the Data Cybersecurity Controls (DCC) to bolster the nation's cybersecurity posture. These controls are designed to safeguard national data, support organizations in protecting their data assets, and promote awareness about secure data handling practices. The DCC encompasses 3 main domains, 11 subdomains, 19 main controls, and 47 specific controls, providing a comprehensive framework for data cybersecurity. The implementation of these controls aligns with Saudi Arabia's Vision 2030, which emphasizes the importance of digital transformation and the need for robust cybersecurity measures to support this transition.

Compliance with the DCC is mandatory for government organizations, private sector entities operating Critical National Infrastructures (CNIs), and all forms of physical and digital data. Failing to adhere to these controls can result in significant consequences for organizations. Noncompliance may lead to financial penalties, legal repercussions, and reputational damage. In the event of a data breach or cybersecurity incident, organizations that have not implemented the required controls may face increased scrutiny and potential liability. Furthermore, noncompliance can undermine the trust of customers, partners, and stakeholders, hindering an organization's ability to operate effectively in an increasingly digital landscape.

The NCA plays a crucial role in regulating and operationalizing cybersecurity efforts in Saudi Arabia. It collaborates with both public and private entities to enhance the country's cybersecurity posture and protect its critical infrastructures and national interests. The NCA conducts evaluations through self-assessments or external assessments to ensure compliance with the DCC. Organizations falling under the scope of these controls must prioritize their implementation and maintain ongoing compliance to avoid the consequences of noncompliance. By following the DCC, organizations demonstrate their commitment to data security, contribute to the overall strength of the nation's cybersecurity posture, and position themselves to thrive in the digital age while mitigating the risks associated with cyber threats.

This guide showcases how Kiteworks can support entities operating in Saudi Arabia which are working to comply with DCC requirements to mitigate cyber risks and meet national data security standards.

الهيئة الوطنية
للأمن السيبراني
National Cybersecurity Authority

The Kiteworks Secure File Sharing and Governance Platform

Kiteworks' FedRAMP- and FIPS-140-2-compliant file sharing and governance platform enables public entities 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 is ISO 27001, ISO 27017, and ISO 27018 certified and enables public entities to access and share personal data securely, reducing the risk of data breaches, malware attacks, and data loss.

Governance and Compliance

Kiteworks supports National Cybersecurity Authority (NCA) of Saudi Arabia Data Cybersecurity Controls (DCC) compliance and provides comprehensive reports on file activity and access.

Simplicity and Ease of Use

Kiteworks enables secure file sharing and collaboration among public entities, individuals, and third-party organizations.

Automation

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

The Kiteworks Platform and NCA DCC Regulations

Main Domain: Cybersecurity Governance

The Cybersecurity Governance domain covers periodic reviews, audits, HR cybersecurity management, and awareness training to ensure compliance. Kiteworks' multilayered approach aids compliance through access controls, least-privilege principle, encryption, activity logging, and administrative controls. It limits access, monitors activities, and proves adherence to regulations. Granular policies, DLP scanning, comprehensive logs, and separated admin duties facilitate audits. Configurable retention, detailed logs, and permanent file erasure help meet deletion, privacy, and security mandates.

Data Cybersecurity Controls (DCC)	Control Description	Kiteworks Solution
1-1-1 Periodical Cybersecurity Review and Audit	With reference to ECC control 1-8-1, the cybersecurity function in the organization must review the implementation of the Data Cybersecurity Controls at least annually as specified for each data classification level.	Kiteworks, a comprehensive platform for secure content collaboration, helps organizations comply with robust authentication, authorization, and admin reporting features. It offers various authentication methods, including multi-factor authentication and integration with identity providers, ensuring secure access to sensitive data. With role-based access and least-privilege defaults, Kiteworks enforces granular control over permissions. Administrators have access to extensive reporting capabilities, including system-level activity logs, built-in and custom reports, and compliance-specific dashboards for regulations like GDPR and HIPAA. These features enable administrators to effectively monitor and review the implementation of the DCC controls, facilitating annual audits and ensuring ongoing compliance with the NCA's cybersecurity requirements.
1-1-2 Periodical Cybersecurity Review and Audit	With reference to ECC control 1-8-2, cybersecurity review and audit must be conducted periodically by independent parties outside the organization's cybersecurity function as specified for each data classification level.	Kiteworks' comprehensive tracking features monitor the activities of end-users, administrators, and system components. These features are complete, detailed, timely, consolidated, and normalized, ensuring that organizations can quickly and comprehensively prove compliance to auditors. Kiteworks' tracking capabilities also support security requirements, such as SecOps, SIEM, and SOAR, by providing timely visibility into activities that help security teams hunt for threats, identify attack signatures, mitigate ongoing attacks, and perform post-attack forensics. Furthermore, Kiteworks' tracking features facilitate operational workflows defined by the organization, making jobs easier and more productive for both end-users and administrators. By leveraging these robust tracking capabilities, organizations can confidently undergo independent cybersecurity reviews and audits, demonstrating their adherence to the NCA's Data Cybersecurity Controls.

Data Cybersecurity Controls (DCC)	Control Description	Kiteworks Solution
1-2-1-2 Cybersecurity in Human Resources	A signed agreement by personnel pledging to not use social media, communication applications, or personal cloud storage to create, store, or share the organization's data, with the exception of secure communication applications approved by relevant authorities.	Kiteworks provides a customizable banner message on the login page of the web application. This feature allows administrators to communicate important information to users, such as reminding them of their obligation to refrain from using unauthorized platforms for handling the organization's data. The banner message can be tailored to match the organization's branding and communication style, ensuring that the message is effectively conveyed to all users. Additionally, Kiteworks' comprehensive reporting capabilities, which log various user activities such as logins, uploads, downloads, and shares, enable administrators to monitor user behavior and identify any potential violations of the signed agreement.
1-3-1-1 Cybersecurity Awareness and Training Program	In addition to the subcontrols in ECC control 1-10-3, the cybersecurity awareness program must cover topics related to data protection, including the following: Risks of data leakage and unauthorized access to data during its life cycle.	Kiteworks offers a range of authentication options that ensure only authorized users can access sensitive data. These authentication methods include credential-based authentication, certificate-based authentication, multi-factor authentication (MFA), SAML 2.0 Single Sign-on (SSO), Kerberos Single Sign-on (SSO), OAuth, LDAP/ Microsoft Active Directory (AD), Azure Active Directory (Azure AD), and locally managed users and credentials. Kiteworks enables organizations to implement strong access controls, reducing the risk of data leakage and unauthorized access. Moreover, a single Kiteworks instance can support a mix of multiple authentication types, providing flexibility to meet the organization's specific security requirements.

Data Cybersecurity Controls (DCC)	Control Description	Kiteworks Solution
1-3-1-2 Cybersecurity Awareness and Training Program	In addition to the subcontrols in ECC control 1-10-3, the cybersecurity awareness program must cover topics related to data protection, including the following: Secure handling of classified data while traveling and outside the workplace.	Kiteworks offers geographic controls and IP address control features that allow organizations to restrict user access based on the country of origin determined by the user's IP address or explicitly block or allow access from specific IP addresses or ranges. These restrictions can be set at the individual user level, user profile level, or system level, ensuring that classified data is securely accessed only from approved locations. Additionally, Kiteworks' authentication and identity management, access controls and policies, the principle of least privilege, DLP scanning, encryption for data at rest and in transit, and complete audit logging further support the secure handling of classified data, even when users are traveling or working remotely.
1-3-1-3 Cybersecurity Awareness and Training Program	In addition to the subcontrols in ECC control 1-10-3, the cybersecurity awareness program must cover topics related to data protection, including the following: Secure handling of data during meetings (virtual and in-person).	The platform provides authentication and identity management, ensuring that only authorized users can access sensitive data during meetings. Access controls and policies are applied to all content folders, emails, connections, and functions, enabling granular control over who can view, edit, or share data. The principle of least privilege is enforced, meaning users start with no privileges and are granted access as needed, minimizing the risk of data exposure. Kiteworks also offers DLP scanning to identify and protect sensitive information, encryption for data at rest and in transit, and complete audit logging to track all user activities. These features collectively ensure that data is securely handled during meetings, whether virtual or in-person.

Data Cybersecurity Controls (DCC)	Control Description	Kiteworks Solution
1-3-1-5 Cybersecurity Awareness and Training Program	In addition to the subcontrols in ECC control 1-10-3, the cybersecurity awareness program must cover topics related to data protection, including the following: Procedures for secure data disposal.	When a user deletes a file, it is permanently removed from the system and cannot be recovered. This action is logged, including the user's ID, file name, and time of deletion, ensuring a complete audit trail. Kiteworks does not keep any backups of deleted files, guaranteeing that sensitive data is thoroughly erased when no longer needed. Furthermore, administrators can enforce data retention policies, specifying how long data should be kept before automatic deletion. Once the retention period expires, the data is permanently deleted and irretrievable. Kiteworks also provides tools for securely wiping data from lost or stolen devices, including remote wipe capabilities.
1-3-1-6 Cybersecurity Awareness and Training Program	In addition to the subcontrols in ECC control 1-10-3, the cybersecurity awareness program must cover topics related to data protection, including the following: Risks of sharing documents and information through non-secure channels.	Kiteworks provides robust access control features, including role-based access, granular permissions, and least-privilege defaults. Users are assigned a set of permissions that govern their access to features and resources, with the system automatically granting the least permissions necessary. Access to files and folders is controlled through pre-defined collaboration roles, such as Owner, Manager, Collaborator, Downloader, Viewer, and Uploader. These roles enable users to create folders, delegate managers, and invite users, while ensuring that access is restricted based on the user's role. Additionally, user profiles can be configured to restrict sending files to external users, further mitigating the risks of sharing sensitive information through non-secure channels. Kiteworks also provides a comprehensive, searchable activity log that captures all necessary data for compliance and audits, including user actions, IP addresses, and metadata.

Main Domain: Cybersecurity Defense

The Cybersecurity Defense domain covers system and facility protection, mobile device security, data confidentiality and availability, cryptography, secure data disposal, and printer/copier security. Kiteworks supports compliance through one-click updates for rapid patching, administrative controls limiting data access, and multiple data protection methods. Features like automatic updates, admin roles restricting activity, remote wipe, dynamic watermarking, DLP integration, and DRM policies blocking downloads facilitate adherence to regulations. These capabilities allow organizations to mitigate risks quickly, monitor administrator actions, prove policy conformance, and safeguard sensitive information through layered access limitations and data protections.

Data Cybersecurity Controls (DCC)	Control Description	Kiteworks Solution
2-1-1-1 Identity and Access Management	In addition to the subcontrols in ECC control 2-2-3, cybersecurity requirements for identity and access management must cover at least the following: Strict restriction to allow only the minimum number of personnel accessing, viewing, and sharing data based on lists of privileges limited to Saudi-national employees unless exempted by the Authorizing Official (the head of the organization or his/her delegate) and those lists are approved by the Authorizing Official.	Kiteworks provides a robust role-based access control system and the principle of least privilege. Users are assigned permissions that govern their access to features and resources, with the system automatically granting the minimum permissions necessary. Access to files and folders is controlled through pre-defined collaboration roles, such as Owner, Manager, Collaborator, Downloader, Viewer, and Uploader. These roles allow for granular control over user access, ensuring that only authorized personnel can access, view, and share data. Kiteworks also provides a separate set of admin roles, including System, Application, Helpdesk, and DLI, which control access to administrative features. Custom admin roles can be created, and a hierarchy of permissions can be set, further enhancing access control.
2-1-1-2 Identity and Access Management	In addition to the subcontrols in ECC control 2-2-3, cybersecurity requirements for identity and access management must cover at least the following: Prohibiting the sharing of approved lists of privileges with unauthorized persons.	Kiteworks provides a robust role-based access control system and the principle of least privilege. Users are assigned permissions that govern their access to features and resources, with the system automatically granting the minimum permissions necessary. Access to files and folders is controlled through pre-defined collaboration roles, such as Owner, Manager, Collaborator, Downloader, Viewer, and Uploader. These roles enable granular control over user access, ensuring that only authorized individuals can view and manage the lists of privileges. Additionally, Kiteworks allows user profiles to be restricted from sending files to external users, further preventing the sharing of approved privilege lists with unauthorized persons.

Data Cybersecurity Controls (DCC)	Control Description	Kiteworks Solution
2-1-2 Identity and Access Management	Managing identities and access rights to view data using Privileged Access Management systems.	The platform supports a wide range of authentication methods, including credential-based authentication, certificate-based authentication, multi-factor authentication (MFA), SAML 2.0 Single Sign-on (SSO), Kerberos Single Sign-on (SSO), OAuth, LDAP/Microsoft Active Directory (AD), Azure Active Directory (Azure AD), and locally managed users and credentials. This flexibility allows organizations to integrate Kiteworks with their existing Privileged Access Management systems, ensuring secure and controlled access to sensitive data. Furthermore, Kiteworks employs role-based access control and the principle of least privilege, automatically granting users the minimum permissions necessary to perform their tasks. Administrators must explicitly enable elevated permissions, maintaining strict control over access rights.
2-1-3 Identity and Access Management	In addition to ECC subcontrol 2-2-3-5, the approved lists of privileges and privileges used to handle data must be reviewed as specified for each data classification level.	Kiteworks provides a hierarchy of admin roles that can set granular permissions, including no access, view only, or full access, and can be further divided into page controls. This feature enables organizations to regularly review and adjust privilege lists based on each data classification level.
2-2-1-1 Information System and Information Processing Facilities Protection	In addition to the subcontrols in ECC control 2-3-3, cybersecurity requirements for Information System and Information Processing Facilities Protection must include at least the following: Applying security patches and updates from the time of announcement on systems used to handle data as specified for each data classification level.	The Kiteworks development team continuously works to identify and rectify security flaws through a well-funded bounty program, engaging cybersecurity engineers to stay ahead of evolving threats. The hardened virtual appliance streamlines the update process, allowing system administrators to download, verify, and apply updates to the entire solution, including the operating system, databases, web servers, and application code, in a single step. This ensures that all components are compatible and thoroughly tested, reducing the burden on the customer.

Data Cybersecurity Controls (DCC)	Control Description	Kiteworks Solution
2-2-1-2 Information System and Information Processing Facilities Protection	In addition to the subcontrols in ECC control 2-3-3, cybersecurity requirements for Information System and Information Processing Facilities Protection must include at least the following: Reviewing the security configuration and hardening of systems used to handle data as specified for each data classification level.	Kiteworks provides granular access permissions for administrators based on customizable admin roles. This ensures administrative separation of duties, a crucial aspect of security and compliance policies. Certain administrative roles grant access to a comprehensive dashboard that includes system-level activity logs, reports, storage, and bandwidth consumption data. Other roles provide access to the CISO Dashboard, which offers a visual summary of logged activities based on various filters, such as geographic location, activity origin, and destination. Additionally, some administrative roles allow access to compliance-specific dashboards that summarize tracking data relevant to regulations like GDPR and HIPAA, facilitating ongoing internal audits and periodic external audits.
2-2-1-3 Information System and Information Processing Facilities Protection	In addition to the subcontrols in ECC control 2-3-3, cybersecurity requirements for Information System and Information Processing Facilities Protection must include at least the following: Reviewing and hardening the default configuration (e.g., default passwords and backgrounds) of the technology assets used to handle the data.	Administrators can control password requirements for their organization, including setting minimum password length, requiring a mix of uppercase and lowercase letters, numbers, and special characters, and setting a password expiration period. Kiteworks also supports password history, preventing users from reusing their previous passwords and ensuring that passwords are regularly changed. Additionally, Kiteworks can integrate with directory services via LDAP or SSO, allowing organizations to manage user credentials and access controls centrally and consistently apply password policies across all systems.
2-3-1-1 Mobile Devices Security	In addition to the subcontrols in ECC control 2-6-3, cybersecurity requirements for mobile devices must cover at least the following: Centrally managing the organization's owned mobile devices using Mobile Device Management (MDM) system and activating the remote wipe feature.	Kiteworks provides mobile apps for iOS and Android that adhere to the AppConfig management standard used by the MDM industry. These apps encrypt all content stored on the device in a secure container. When a Kiteworks administrator removes a user or revokes a user's permission to use the mobile app, the user's data on the app is automatically wiped. Administrators can also perform a remote wipe of a user's device or devices directly from the user management section of the Admin Console.

Data Cybersecurity Controls (DCC)	Control Description	Kiteworks Solution
2-3-1-2 Mobile Devices Security	In addition to the subcontrols in ECC control 2-6-3, cybersecurity requirements for mobile devices must cover at least the following: Centrally managing BYOD devices using Mobile Device Management (MDM) system and activating the remote wipe feature.	Kiteworks provides robust data protection measures to ensure the security and integrity of user data on mobile devices. When a user deletes a file, it is permanently removed from the system and cannot be recovered. This action is logged, including the user's ID, file name, and time of deletion, maintaining user privacy and ensuring that sensitive data is completely erased when no longer needed. The system does not keep any backups of deleted files, ensuring that there are no residual copies that could potentially be recovered. Additionally, Kiteworks offers tools for securely wiping data from devices in the event they are lost or stolen, including the ability to remotely wipe data from a device, preventing data recovery even if the device falls into the wrong hands.
2-4-1-1 Data and Information Protection	In addition to the subcontrols in ECC control 2-7-3, cybersecurity requirements for data and information protection must cover at least the following: Using watermark feature to label the whole document when creating, storing, printing, on the screen and on each copy so that the symbol can be traced to the user or device level.	Kiteworks embeds incriminating watermarks dynamically based on policy settings that apply to the combination of the user, the content, and the action the user is attempting to perform on the content. The watermark contents, configured by the administrator, typically include the date and user ID of the user accessing the content, allowing for easy tracing of any leaks. The watermark appears in Kiteworks secure viewers, such as when a recipient views an email attachment or a shared file, and in the SafeEDIT UI, which provides a virtual editing interface for files without leaving the Kiteworks secure enclave. In these cases, policies usually prevent downloading, copying, or printing of the file or its parts.
2-4-1-2 Data and Information Protection	In addition to the subcontrols in ECC control 2-7-3, cybersecurity requirements for data and information protection must cover at least the following: Using Data Leakage Prevention technologies and Rights Management technologies.	By integrating with DLP technologies, Kiteworks enables organizations to monitor and control the flow of data, preventing unauthorized access, use, or transmission of sensitive information. This integration allows organizations to enforce data protection policies consistently across their IT environment, including within the Kiteworks platform. Additionally, Kiteworks' built-in security features, such as granular access controls, encryption, and auditing capabilities, complement the functionalities of DLP and Rights Management technologies.

Data Cybersecurity Controls (DCC)	Control Description	Kiteworks Solution
2-4-1-3 Data and Information Protection	In addition to the subcontrols in ECC control 2-7-3, cybersecurity requirements for data and information protection must cover at least the following: Prohibiting the use of data in any environment other than the production environment, except after conducting a risk assessment and applying controls to protect that data, such as data masking or data scrambling techniques.	Kiteworks administrators and content managers can set digital rights management (DRM) policies that prevent sensitive content from leaving the Kiteworks system. These policies restrict interaction with sensitive data to a watermarked view-only UI, a watermarked virtual editing UI, or block access completely. Additionally, Kiteworks can be connected to external DLP servers that identify files that should not be allowed to leave the system. In such cases, Kiteworks can be configured to block the export of those files, and only an administrator can release them.
2-5-1-1 Cryptography	In addition to the subcontrols in ECC control 2-8-3, cybersecurity requirements for cryptography must cover at least the following: Using secure and up-to-date cryptographic methods and algorithms when creating, storing, transmitting data, and for overall network communication medium, as per the requirements of the "advanced level" in the National Cryptographic Standards (NCS-1:2020).	Kiteworks double-encrypts customer files to minimize the attack surface available to an intruder who has gained access to the operating system. This is a critical part of assumed-breach architecture, where the system protects data even when an attacker has breached the outer layers of the appliance, exposing the inner layers to further attack. Even if an attacker breaches the outer layers, they can't decrypt files simply by gaining access to the operating system. The innermost layer of encryption is at the operating system level, where the operating system itself encrypts and decrypts files as they are written to and read from disk. In outer layers, Kiteworks' application software in the virtual appliance also performs its own encryption of files using a separate file-level key. In this way, even if an attacker gains access to the operating system, they will only have access to encrypted blobs that can only be decrypted with the file-level key.

Data Cybersecurity Controls (DCC)	Control Description	Kiteworks Solution
2-5-1-2 Cryptography	In addition to the subcontrols in ECC control 2-8-3, cybersecurity requirements for cryptography must cover at least the following: Using secure and up-to-date cryptographic methods and algorithms when creating, storing, transmitting data, and for overall network communication medium, as per the requirements of the "moderate level" in the National Cryptographic Standards (NCS-1:2020).	Kiteworks employs a double-encryption strategy for customer files to minimize the attack surface available to an intruder who has gained access to the operating system. This approach is a critical part of the assumed-breach architecture, where the system protects data even when an attacker has breached the outer layers of the appliance. The innermost layer of encryption is at the operating system level, where the OS itself encrypts and decrypts files as they are written to and read from disk. In outer layers, Kiteworks' application software in the virtual appliance performs its own encryption of files using a separate file-level key. As a result, even if an attacker gains access to the operating system, they will only have access to encrypted blobs that can only be decrypted with the file-level key.
2-6-1-1 Secure Data Disposal	Cybersecurity requirements for secure data disposal must cover at least the following: Identification of technologies, tools, and procedures for the implementation of secure data disposal according to the data classification level.	Kiteworks has robust data protection measures in place to ensure the security and integrity of user data. When a user deletes a file, it is permanently removed from the system and cannot be recovered. This action is logged, including the user's ID, file name, and time of deletion, maintaining user privacy and ensuring that sensitive data is completely erased when no longer needed.
2-6-1-2 Secure Data Disposal	Cybersecurity requirements for secure data disposal must cover at least the following: When storage media is no longer needed, it must be securely disposed by using the technologies, tools, and procedures identified in subcontrol 2-6-1-1.	Kiteworks has robust data protection measures in place to ensure the security and integrity of user data. When a user deletes a file, it is permanently removed from the system and cannot be recovered. This action is logged, including the user's ID, file name, and time of deletion, maintaining user privacy and ensuring that sensitive data is completely erased when no longer needed. Kiteworks does not keep any backups of deleted files, ensuring that there are no residual copies that could potentially be recovered.

Data Cybersecurity Controls (DCC)	Control Description	Kiteworks Solution
2-6-1-3 Secure Data Disposal	Cybersecurity requirements for secure data disposal must cover at least the following: When storage media needs to be re-used, data must be securely erased (secure erasure) in a manner it cannot be recovered.	Kiteworks has robust data protection measures in place to ensure the security and integrity of user data. When a user deletes a file, it is permanently removed from the system and cannot be recovered. This action is logged, including the user's ID, file name, and time of deletion, maintaining user privacy and ensuring that sensitive data is completely erased when no longer needed. Kiteworks does not keep any backups of deleted files, ensuring that there are no residual copies that could potentially be recovered. Additionally, Kiteworks provides tools for securely wiping data from devices in the event they are lost or stolen, including the ability to remotely wipe data from a device, preventing data recovery even if the device falls into the wrong hands.
2-6-1-4 Secure Data Disposal	Cybersecurity requirements for secure data disposal must cover at least the following: Implementation of secure data disposal or erasure operations referred to in sub-controls 2-6-1-2 and 2-6-1-3 must be verified.	Kiteworks has robust data protection measures in place to ensure the security and integrity of user data. When a user deletes a file, it is permanently removed from the system and cannot be recovered. Crucially, any time a user deletes a file, this action is logged and can be confirmed. The log includes the user's ID, file name, and time of deletion. This logging feature is critical for maintaining user privacy, ensuring that sensitive data is completely erased when no longer needed, and providing a verifiable record of secure data disposal or erasure operations.
2-6-1-5 Secure Data Disposal	Cybersecurity requirements for secure data disposal must cover at least the following: Keeping a record of all secure data disposal and erasure operations that have been conducted.	Kiteworks has robust data protection measures in place to ensure the security and integrity of user data. When a user deletes a file, it is permanently removed from the system and cannot be recovered. Importantly, any time a user deletes a file, this action is logged and can be confirmed. The log includes the user's ID, file name, and time of deletion. This logging feature is critical for maintaining a comprehensive record of all secure data disposal and erasure operations, enabling organizations to demonstrate compliance. By leveraging these features, Kiteworks helps organizations maintain a complete audit log of data disposal and erasure activities, ensuring that sensitive data is securely erased when no longer needed and supporting the organization's ability to prove compliance with relevant regulations.

Data Cybersecurity Controls (DCC)	Control Description	Kiteworks Solution
2-6-2 Secure Data Disposal	The implementation of the secure data disposal requirements must be reviewed as specified for each data classification level.	When a user deletes a file, it is permanently removed from the system and cannot be recovered. Crucially, any time a user deletes a file, this action is logged and can be confirmed. The log includes the user's ID, file name, and time of deletion. This logging feature enables organizations to review and verify that secure data disposal requirements are being met for each data classification level. By providing a comprehensive audit log of data deletion activities, Kiteworks facilitates regular reviews of secure data disposal practices, allowing organizations to demonstrate compliance and ensure that sensitive data is being securely erased in accordance with the organization's data classification policies.

Main Domain: Third-party and Cloud Computing Cybersecurity

The Third-party and Cloud Computing Cybersecurity domain covers asset protection requirements when using third-party services. Kiteworks facilitates compliance through Enterprise Connect for external repository integration, collaboration roles governing access, least privilege principles, activity logging, intrusion detection, anomaly monitoring, data classification, and flexible policy assignment. These features enable secure collaboration, limit data exposure, detect suspicious activities, categorize sensitive assets, determine risk levels based on custom criteria, monitor user actions, and prove adherence to third-party and external sharing regulations.

Data Cybersecurity Controls (DCC)	Control Description	Kiteworks Solution
3-1-1-3 Third-Party Cybersecurity	In addition to the controls in ECC subdomain 4-1, cybersecurity requirements for third-party cybersecurity must include at least the following: Documenting all data-sharing operations within third parties, including data-sharing justification.	Kiteworks provides features such as Enterprise Connect and comprehensive access controls. Enterprise Connect enables access to content in external repositories, making it appear as shared folders within the Kiteworks system. When a user accesses a file through Enterprise Connect, their access is logged into the external system using their third-party credentials, ensuring that the access controls of the third-party system are applied. Additionally, Kiteworks governs access to files and folders using pre-defined collaboration roles, such as Owner, Manager, Collaborator, Downloader, Viewer, and Uploader. These roles enable granular control over user permissions and can be used to document and justify data-sharing operations with third parties. User profiles can also be configured to restrict downloading files sent via secure links, control access based on the client used, and enable or disable read mode for clients.
3-1-1-4 Third-Party Cybersecurity	In addition to the controls in ECC subdomain 4-1, cybersecurity requirements for third-party cybersecurity must include at least the following: When transferring data outside the kingdom, the capability of the hosting organization abroad to safeguard data must be verified, approval of the Authorizing Official must be obtained, and complying with related laws and regulations.	The Kiteworks platform is designed with data sovereignty in mind, providing solutions that allow organizations to comply with data residency and sovereignty requirements. Kiteworks can be configured to store data in specific geographic locations, enabling compliance with data residency requirements that mandate certain types of data to be stored within the borders of a specific country or region. The platform also offers secure file transfer and email data protection solutions, helping organizations manage and control cross-border data transfers. Kiteworks' encryption and access control features protect personal information during cross-border transfers, ensuring secure transmission and compliance with data sovereignty requirements. Furthermore, Kiteworks supports data portability requirements by enabling users to securely access, transfer, and download their personal information, making it easy for users to transmit their personal information to other organizations upon request, even across borders.

Data Cybersecurity Controls (DCC)	Control Description	Kiteworks Solution
3-1-1-5 Third-Party Cybersecurity	In addition to the controls in ECC subdomain 4-1, cybersecurity requirements for third-party cybersecurity must include at least the following: Requiring third parties to notify the organization immediately in case of cybersecurity incident that may affect data that has been shared or created.	The Kiteworks platform logs and sends notifications of activity related to intrusion attempts and detected anomalies, enabling the identification and notification of potential security breaches. Kiteworks logs events such as failed access attempts on common server ports, file integrity issues, rogue background jobs, and signatures of common network attacks. These comprehensive logs can help detect cybersecurity incidents that may impact data shared with or created by third parties.
3-1-1-6 Third-Party Cybersecurity	In addition to the controls in ECC subdomain 4-1, cybersecurity requirements for third-party cybersecurity must include at least the following: Reclassifying data to the least level to achieve the objective before sharing it with third parties using data masking or data scrambling techniques.	Kiteworks provides asset management for content assets by classifying them in the context of a content-based risk policy when a user requests an action on that content. Kiteworks' classification is performed based on conditions such as the folder path, specified MIP or custom sensitivity labels, file type, creator, and other criteria. This allows organizations to ensure that data is appropriately classified before being shared with third parties, minimizing the risk of exposing sensitive information. By leveraging Kiteworks' content classification capabilities, organizations can reclassify data to the least level required to achieve the objective, applying data masking or data scrambling techniques as necessary. This helps maintain data security and privacy when sharing information with third parties.
3-1-2-2 Third-Party Cybersecurity	In alignment with related laws and regulations, and in addition to the applicable controls in ECC and controls within DCC domain (1), (2), and (3); cybersecurity requirements when dealing with consultancy services that works on high-sensitivity strategic projects at the national level must cover at least the following: Requiring contractual commitment by consultancy services including employees' non-disclosure agreements and secure disposal of the organization's data at the end of the contract or in case of contract termination, including providing evidences of such disposal to the organization.	Kiteworks provides features that can help organizations communicate and enforce these requirements by allowing administrators to set up custom banner messages on the login page of the web application. These banners can be used to communicate important information to users, such as reminders about non-disclosure agreements and secure data disposal obligations. The banner messages can be customized to match the organization's branding and communication style, ensuring that consultancy service employees are aware of their responsibilities. Additionally, Kiteworks provides comprehensive reporting capabilities, logging various activities such as logins, uploads, downloads, views, and admin activities. These logs can be used to monitor consultancy service employees' actions and ensure compliance with data disposal requirements.

Data Cybersecurity Controls (DCC)	Control Description	Kiteworks Solution
3-1-2-3 Third-Party Cybersecurity	In alignment with related laws and regulations, and in addition to the applicable controls in ECC and controls within DCC domain (1), (2), and (3); cybersecurity requirements when dealing with consultancy services that works on high-sensitivity strategic projects at the national level must cover at least the following: Documenting all data-sharing operations within consultancy services, including data-sharing justification.	Kiteworks provides comprehensive audit logging capabilities that enable organizations to track and document various data-sharing activities. The platform logs a wide range of user actions, including views, downloads, uploads, edits, emails, shared folders and files, comments, tags, user authentication, file access, file uploads, file deletion, sharing, permissions, user management, configuration changes, servers, sources, settings, and system updates. These detailed logs allow organizations to monitor and document data-sharing operations performed by consultancy services. By leveraging Kiteworks' extensive logging features, organizations can track who accessed specific content, when files were downloaded or uploaded, changes made to files, and sharing activities. The logs also capture details such as user IDs, file names, timestamps, and IP addresses, providing a comprehensive audit log of data-sharing operations.
3-1-2-4 Third-Party Cybersecurity	In alignment with related laws and regulations, and in addition to the applicable controls in ECC and controls within DCC domain (1), (2), and (3); cybersecurity requirements when dealing with consultancy services that works on high-sensitivity strategic projects at the national level must cover at least the following: Requiring consultancy services to notify the organization immediately in case of cybersecurity incident that may affect data that has been shared or created.	Kiteworks logs activity related to intrusion attempts and detected anomalies, enabling the identification and notification of potential security breaches. Kiteworks logs events such as failed access attempts on common server ports, file integrity issues, rogue background jobs, and signatures of common network attacks. These comprehensive logs can help detect cybersecurity incidents that may impact data shared with or created by consultancy services. By continuously improving and updating these security features and maintaining detailed logs, Kiteworks provides organizations with the necessary tools to identify and respond to potential security incidents involving consultancy services. This supports organizations' timely notification and appropriate action in the event of a cybersecurity incident that may affect shared or created data during high-sensitivity strategic projects at the national level.

Data Cybersecurity Controls (DCC)	Control Description	Kiteworks Solution
3-1-2-5 Third-Party Cybersecurity	In alignment with related laws and regulations, and in addition to the applicable controls in ECC and controls within DCC domain (1), (2), and (3); cybersecurity requirements when dealing with consultancy services that works on high-sensitivity strategic projects at the national level must cover at least the following: Reclassifying data to the least level to achieve the objective before sharing it with consultancy services using data masking or data scrambling techniques.	Kiteworks provides flexible and customizable data classification capabilities that allow organizations to define their own classification categories and criteria, ensuring that data is appropriately classified before being shared. Classification policies can be based on various factors, such as folder path, user domain, profile, and individual users, providing a more flexible approach than simple tags. This granular control enables organizations to reclassify data to the least level required to achieve the objective, applying data masking or data scrambling techniques as necessary. Organizations can ensure that sensitive information is protected and shared with consultancy services only at the appropriate level, minimizing the risk of data exposure, supporting compliance when dealing with consultancy services working on high-sensitivity strategic projects at the national level.

Kiteworks

Kiteworks

www.kiteworks.com

March 2024