Kiteworks

COMPLIANCE BRIEF

# Kiteworks Enhances Security and Compliance for Research Organizations and Universities

## Leverage Centralized Governance, Managed File Transfer, and Flexible Deployment Options to Safeguard Sensitive Data and Meet Compliance Obligations

For universities, federally funded research and development centers (FFRDC), and university-affiliated research centers that handle sensitive federal information through government research contracts, compliance with the Cybersecurity Maturity Model Certification (CMMC) framework is critical. The framework, developed by the United States Department of Defense (DoD), ensures that organizations handling controlled unclassified information (CUI) and federal contract information (FCI) have robust cybersecurity practices in place to prevent cyberattacks like malware, ransomware, and phishing. Achieving CMMC compliance is a requirement for organizations seeking to bid on DoD contracts, and the level of compliance required depends on the sensitivity of the information they will handle. Universities and research centers that maintain government research contracts must understand the importance of safeguarding federal information, as the protection of such data is paramount to federal agencies and can impact the ability of the federal government to carry out its designated missions and business operations.

## Increase Control and Security With Centralized Governance

Kiteworks supports CMMC compliance by providing organizations with the ability to increase control and governance over their sensitive digital assets. The platform is SOC 2 certified, FedRAMP Moderate Authorized, and FIPS 140-2 compliant, ensuring that it adheres to rigorous guidelines and reviews. By unifying security for third-party communications, including email, file sharing, mobile, managed file transfer, and SFTP, Kiteworks provides centralized governance and protection of sensitive digital assets, making it an ideal solution for organizations handling sensitive research data that requires strict security controls to prevent unauthorized access, disclosure, or modification. Kiteworks also integrates with existing security investments, such as DLP and ATP solutions, to prevent data leaks and quarantine unknown threats, further enhancing security measures. Leveraging these integrations and maintaining security controls, universities and research organizations can ensure they meet strict security and compliance requirements necessary for their government-funded research projects, while also protecting sensitive digital assets from cyberattacks and data breaches.

## Automate and Protect File Data With Managed File Transfer

By leveraging Kiteworks' Managed File Transfer (MFT) capabilities, research universities can ensure the safety and security of their sensitive research data in automated transfer environments while maintaining control and governance. With vault-to-vault transfers and a library of 2,000 connectors and workflow functions, Kiteworks' MFT enables secure and flexible business processes. Granular policy controls prevent data breaches and compliance violations, ensuring the safety of CUI and FCI. The scalable and reliable solution helps research universities securely transfer sensitive research data and improve the efficiency of their file transfer processes while maintaining compliance with industry standards.

## Meet Contract Obligations With Flexible Deployment

Kiteworks offers valuable flexible deployment options for universities and research organizations with a tight budget looking to meet contract obligations. Kiteworks' platform is flexible and supports on-premises, private cloud, hybrid, hosted, and FedRAMP private cloud deployment options tailored to specific requirements. The platform's ability to find the perfect balance between privacy, compliance, scalability, and costs minimizes security vulnerabilities and reduces maintenance costs. By leveraging Kiteworks' flexible deployment options, universities and research organizations can be confident in their ability to meet contract obligations while minimizing security risks and reducing costs.

Kiteworks provides a comprehensive solution for universities and research organizations handling sensitive federal information through government research contracts, ensuring compliance with the CMMC 2.0 framework. The platform offers centralized governance, preventing unauthorized access, disclosure, or modification of sensitive digital assets. Kiteworks' MFT platform, with granular policy controls, ensures secure transfer of sensitive research data, preventing data breaches and compliance violations. Flexible deployment options, including on-premises, private cloud, hybrid, hosted, and FedRAMP private cloud, allow organizations to minimize security vulnerabilities while reducing maintenance costs. Kiteworks supports nearly 90% of CMMC 2.0 Level 2 requirements out of the box. By leveraging Kiteworks, universities and research organizations can confidently meet contract obligations, protecting sensitive digital assets from cyberattacks and data breaches.