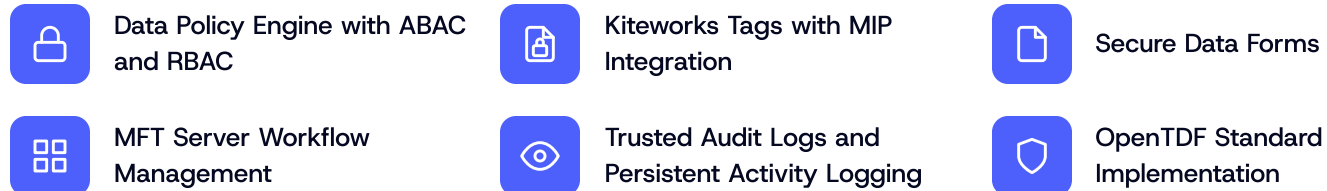


KITEWORKS SUPPORTS 10 CFR CHAPTERS I & II — NRC AND DOE REQUIREMENTS

From Access-Controlled Safety Analysis Reports to Audit-Ready DOE Energy Test Records on One Platform

Solution Highlights



10 CFR Chapters I and II — the bodies of federal regulations administered respectively by the U.S. Nuclear Regulatory Commission (Chapter I, Parts 1–199) and the U.S. Department of Energy (Chapter II, Parts 200–699) — together govern the licensing, construction, operation, and oversight of nuclear facilities and related energy activities, and they appear in the current edition maintained on the Electronic Code of Federal Regulations. Compliance obligations extend to applicants and licensees for combined nuclear power reactor licenses and land disposal of radioactive waste (NRC, Chapter I), electric utilities and other entities engaged in the generation, transmission, or distribution of electric energy, powerplant owners and operators, natural gas exporters, and manufacturers of commercial and industrial equipment subject to Department of Energy energy conservation test procedures under Part 431 (DOE, Chapter II). These requirements apply within the United States and its jurisdiction. The regulation imposes obligations spanning safety analysis report submission, inspection and test reporting, emergency situation reporting, license termination certification, financial management system standards, and equipment energy efficiency determinations, enforced through NRC and DOE administrative oversight, licensing conditions, and reporting mandates. Kiteworks supports organizations working toward compliance with 10 CFR Chapters I and II. Here's how:

Safeguarding Safety Analysis Report Contents (NRC, Chapter I)

Sections 52.17, 52.47, 52.79, and 52.109 require applicants to compile and submit highly sensitive technical information, including site safety analysis reports, final safety analysis reports covering facility design and fission product release evaluations, site boundaries and characteristics, and the ownership and possession records that persist after a facility permanently ceases operations. Kiteworks protects this material through the Data Policy Engine's Attribute-based Access Controls, evaluating data asset attributes such as folder path or tag, sender and recipient user attributes such as domain or profile, and the action a user attempts. Kiteworks Tags automatically classify files as they enter the system, so a document tagged Confidential carries different access rules than one tagged Internal_Use_Only, and Data classification tagging with Microsoft Information Protection integration synchronizes those labels. For § 52.109 facilities in the post-operation period, RBAC file sharing roles and folder expiration settings govern who retains possession-related records and for how long. For organizations that require the additional layer of persistent, object-level encryption, Kiteworks also offers an OpenTDF Standard Implementation — available on request — that embeds attribute-based access control policies directly within the data itself, so access controls travel with the file regardless of where it moves or which systems process it.

Governing Application Submissions and Financial Management Controls (NRC, Chapter I & DOE, Chapter II)

Sections 51.62, 52.17, 52.47, 52.79, 52.80, 52.99, 52.103, 52.109, 52.110 (NRC, Chapter I), and 501.191, 590.208, 600.121, and 600.122 (DOE, Chapter II) impose access, submission, and processing-control obligations across license applications, ITAAC schedules, fuel-loading notifications, termination certifications, small-volume natural gas exports, and federal financial management systems. Kiteworks fulfills these through the Data Policy Engine, whose Attribute-based Access Controls govern each data access dynamically based on attributes of the data, the user, and the attempted action, while RBAC assigns pre-defined file sharing roles to each invited user. For § 600.121 financial management systems, Kiteworks Admin roles enable the segregation of administrative duties via a separate set of admin roles that control access to administrative features, and Folder file-lifetime retention policy enforces record retention. Secure Data Forms collects structured application and certification data, creating a secure shared folder controlled by the form builder for each submission, while Managed File Transfer authenticates every workflow accessing Kiteworks folders and SFTP directories and applies access controls to license-related transfers. For § 590.208 small-volume exports, Data Sovereignty configures the system to store and route a user's data only within their assigned country, assigned via LDAP or SAML attributes, and File Share packages protect exports with ACL, expiration, authentication requirements, and forensic watermarking. For § 600.122 payment processing, secure send-file packages with short links deliver protected files. Beyond these mapped controls, the Commission's licensing determinations under § 52.97 remain organizational and process-level obligations the applicant must administer directly.

Reporting and Recordkeeping Across NRC and DOE Mandates

The bulk of Chapters I and II impose tracking and recordkeeping duties: emergency reporting under §§ 205.351, 205.352, and 205.353 (DOE, Chapter II); compliance accounting under § 205.387 (DOE, Chapter II); greenhouse gas reporting under § 300.1 (DOE, Chapter II); ITAAC and notification records under §§ 52.80, 52.99, 52.103, and 52.110 (NRC, Chapter I); land disposal application records under § 51.62 (NRC, Chapter I); and the full slate of Part 431 energy efficiency test procedures spanning §§ 431.16, 431.64, 431.76, 431.86, 431.96, 431.106, 431.134, 431.154, 431.174, 431.193, 431.204, 431.224, 431.264, 431.294, 431.304, 431.324, 431.344, 431.444, 431.445, 431.464, and 431.484 (DOE, Chapter II), plus financial records under §§ 600.121 and 600.122 (DOE, Chapter II). Kiteworks captures these through Secure Data Forms, where each submission creates a human-readable PDF and adds a row to a machine-readable CSV that captures data from all submissions, supported by standard field types for structured report fields such as utility name, area affected, and time of occurrence. The audit log persists all events as Activities with structured per-event data, permission tagging, and filterable retrieval for audit trails, and Trusted Audit Logs convert those records to human-readable formats for administrative reporting, filterable and searchable, with report generation and export for compliance audits. Admin reporting produces default or custom reports, ad hoc or scheduled, exportable via CSV. For emergency dissemination under § 205.351, MFT Server Workflow management runs on a schedule or trigger and sends email notifications on completion, failure, or retry. Folder file-lifetime retention policy enforces the record-keeping periods these reporting programs require.

Kiteworks gives NRC and DOE licensees, applicants, and regulated entities a single platform to support the protection, control, and tracking obligations woven through 10 CFR Chapters I and II. The Data Policy Engine, RBAC file sharing roles, segregated admin roles, and Data Sovereignty routing govern who submits, accesses, and processes license applications, export authorizations, and federal financial records under NRC's Chapter I and DOE's Chapter II frameworks alike. Kiteworks Tags with MIP integration and folder-level access controls protect safety analysis reports and other sensitive technical filings today, with an OpenTDF Standard Implementation available on request for organizations that require persistent, object-level encryption with embedded access policies. Secure Data Forms, MFT Server workflows, the audit log, and Trusted Audit Logs capture every emergency report, ITAAC notification, and energy efficiency test record with exportable, audit-ready evidence. Across both chapters, Kiteworks unifies secure exchange, governance, and reporting on one platform built for regulated nuclear and energy operations.

Ready to make your 10 CFR compliance program audit-ready?

www.kiteworks.com

Kiteworks



Kiteworks' mission is to empower organizations to effectively manage risk in every send, share, receive, and use of private data. The Kiteworks platform provides customers with a secure data exchange that delivers data governance, compliance, and protection in a unified control plane. Kiteworks unifies, tracks, controls, and secures sensitive data moving within, into, and out of their organization, significantly improving risk management and ensuring regulatory compliance on all private data exchanges. Headquartered in Silicon Valley, Kiteworks protects over 100 million end-users and thousands of global enterprises and government agencies.