NEW ENERGY DILIGENCE

SECURITY & DATA PROTECTION SUMMARY

Last Updated: April 20, 2026

askned.ai · San Rafael, CA · jon@askned.ai

NED handles confidential transaction materials on behalf of clients in renewable energy M&A, project finance, independent engineering, and advisory engagements. This summary describes our security posture, data classification practices, and the NIST SP 800-53 controls we have implemented. Specific vendor names, product tiers, and configuration details are available to prospective clients under NDA through our standard security questionnaire process.

1. Platform Summary

NED builds its security posture on independently certified cloud platforms. We do not operate our own server infrastructure for client data. Document storage and business email are procured under commercial business terms with Data Processing Agreements in place. AI assistance is subscribed at a professional tier with model training disabled at the account level; see Section 2 for details. Each platform is selected for its security credentials, redundancy, and independent certification.

Category	Purpose	Provider Certifications	Encryption
AI Assistance	Document review, analysis, and drafting with tenant isolation per engagement	SOC 2 Type II, ISO 27001, ISO/IEC 42001	TLS / AES-256
Document Storage	Secure storage and client sharing	SOC 2, ISO 27001, FedRAMP, HIPAA, PCI DSS, FIPS 140-2	TLS / AES-256 with cryptographic key wrapping
Business Email	Encrypted business email with enterprise threat protection	SOC 2, ISO 27001, HIPAA, GDPR	Encrypted transport, MFA enforced

2. AI Analysis

NED uses a leading AI assistant provided by a company that holds organizational SOC 2 Type II, ISO 27001:2022, and ISO/IEC 42001:2023 certifications. ISO/IEC 42001 is the international standard for AI management systems and provides independent assurance of the provider's governance of AI model development and operation.

Subscription Tier and Training

NED subscribes at a professional-tier subscription plan. Model training has been disabled in NED's account settings, which means client documents and conversations are not used to train AI models. Under this configuration, conversation data is retained by the provider for a limited operational period (approximately 30 days) for trust and safety review, after which it is deleted from the provider's systems. NED verifies the training-disabled setting as part of its periodic security review.

This subscription tier does not provide flow-through contractual commitments such as a Data Processing Agreement, Business Associate Agreement, or zero-data-retention addendum. Clients requiring these contractual assurances for a specific engagement — for example, financial institutions under banking regulator oversight, or organizations subject to GDPR data-processor obligations — should raise this requirement with NED before

engagement. NED can provision an alternative arrangement (commercial-tier AI subscription or direct API access under commercial terms) on a per-engagement basis.

Use of AI

NED uses the AI platform to assist with document review, analysis, drafting, and research. All AI-assisted output is reviewed and verified by a qualified NED principal before delivery to the client. The AI produces draft work product; NED provides the judgment, verification, and professional accountability.

Workspace Isolation

NED uses the platform's project workspace feature to maintain a dedicated, isolated workspace for each client engagement. Documents and conversations belonging to one engagement are not accessible from any other engagement within NED's account.

3. Document Storage & Sharing

Encryption

Files are encrypted at rest using AES-256 and in transit using modern TLS. The platform applies an additional cryptographic key-wrapping layer and holds FIPS 140-2 certification for its cryptographic modules.

Access Controls & Redundancy

Zero-trust architecture with SSO, MFA, and role-based permissions. Folder-level access is configured per engagement. Files are replicated to a backup facility at time of upload. The platform maintains active-active data center redundancy and supports point-in-time recovery.

Certifications

SOC 1, SOC 2, ISO 27001, HIPAA, FedRAMP, PCI DSS, FIPS 140-2, FINRA SEC 17a-4.

4. Business Email

Encryption & Threat Protection

Messages sent within NED's organization are encrypted automatically. For sensitive communications to external recipients, enterprise-grade email encryption is available upon client request. Inbound and outbound mail pass through enterprise threat protection including anti-phishing, malicious-attachment scanning, spoofing quarantine, and spam filtering.

Authentication

Multi-factor authentication is enforced on all accounts. Legacy authentication protocols are blocked at the tenant level.

Certifications

SOC 1, SOC 2, ISO 27001, HIPAA, GDPR.

5. NIST Data Classification — What NED Accepts

NED works across renewable energy M&A and project finance, independent engineering, tax credit transfers, owner engineering, equipment assessment, accelerated lifetime testing and factory audits, software development and integration, and marketing support. For most of these engagements the relevant materials — data room documents, IE reports, financial models, equipment specifications, interconnection agreements, transaction correspondence, software specifications, and marketing materials — fall within Level 2 (Internal / Sensitive) and are well within NED's security posture.

NED aligns data handling with the NIST-consistent four-level commercial data classification framework (NIST SP 800-53, NIST IR 8496). The table below describes each level and NED's acceptance policy.

Level	Classification	Examples	NED Status
1	**Public**	Press releases, public filings, published research, public project announcements	✓ Accepted
2	**Internal / Sensitive**	Draft IE reports, non-final term sheets, financial models, project data rooms, transaction timelines (shared under NDA)	✓ Accepted — standard for NED engagements
3	**Confidential**	PII, SSNs, tax IDs, bank details, HIPAA data, PCI DSS cardholder data, attorney-client privileged materials, Reg FD information	✗ Not accepted
4	**Restricted**	Classified government data, Top Secret, cryptographic keys, court-ordered restricted information, trade secrets under DTSA	✗ Not accepted

Reference: nccoe.nist.gov/data-classification

6. NIST SP 800-53 Controls Implemented

NED applies the following security controls consistent with NIST Special Publication 800-53 Rev. 5. Controls apply across our three platform categories — AI assistance, document storage, and business email — and to NED's operational practices for session management, authentication, and access control.

Client data is not stored on laptops or local devices. All client materials reside exclusively on the encrypted cloud platforms identified above.

NIST Control	Reference	Implementation
Multi-Factor Authentication	IA-2	MFA is enforced across all platform accounts, using phishing-resistant methods consistent with NIST SP 800-63B.
Session Lock	AC-11	NED devices auto-lock after inactivity. Because client data is not stored locally, access to any platform requires separate re-authentication with MFA.
Password Management	IA-5	Passwords are not reused across services. Complexity and length requirements meet or exceed NIST SP 800-63B guidelines.
Encryption in Transit	SC-8	Modern TLS is used across all platforms. Client materials are not transmitted over unencrypted channels.
Encryption at Rest	SC-28	AES-256 at rest across all platforms, with additional cryptographic key wrapping on the document storage platform. Client data is not stored unencrypted on any device.
Least Privilege Access	AC-3, AC-6	Access to client materials is limited to NED personnel working on the relevant engagement. Permissions are configured per engagement, and tenant isolation is enforced at the AI layer.
Login Attempt Controls	AC-7	Account lockout and alerting controls are enabled to limit credential-based attacks.
Data Backup	CP-9	Files are replicated to a backup facility at time of upload. Active-active data center redundancy supports point-in-time recovery.

7. Data Retention

NED retains client materials — including deliverables, work product, engagement records, and client-provided source materials — in a secure, access-controlled archive for a minimum of seven (7) years from the conclusion of the engagement. This practice allows NED to retrieve materials quickly on the client's behalf if needed for future reference, litigation support, regulatory inquiry, or follow-on work, and conforms to standard professional services data retention practices consistent with applicable statutes of limitations and recordkeeping norms.

Archived materials are stored in a dedicated, access-restricted area of NED's document management platform. They are subject to the same encryption, access controls, and security practices described in this document.

Clients who require earlier deletion — for example, due to internal compliance requirements or contractual obligations — may submit a written request at any time. NED will return or delete materials as directed. Instructions are included in the engagement letter or professional services agreement.

8. Further Information Available Under NDA

The following categories of information are available to prospective and current clients through our security questionnaire process, under NDA:

- Specific vendor and product identification for each platform category
- Detailed configuration profiles and baseline settings
- Responses to industry-standard questionnaires (SIG, CAIQ)
- Subprocessor lists and data residency information
- Incident response procedures and notification commitments
- Alternative commercial-tier AI arrangements for regulated engagements (DPA, BAA, or ZDR coverage)
- Custom security terms for regulated industries (banking, GDPR, healthcare)

For questions about NED's security practices, or to request our full security questionnaire, please contact jon@askned.ai.