NEW ENERGY DILIGENCE

SECURITY & DATA PROTECTION SUMMARY

Last Updated: March 26, 2026

www.newenergydiligence.com · 741 Bamboo Terrace, San Rafael, CA 94903 · 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 document describes our security platforms, data classification practices, and the NIST SP 800-53 controls we have implemented. It is intended for distribution to client compliance, legal, and IT teams.

1. PLATFORM SUMMARY

NED builds its security posture on three enterprise-grade, independently certified platforms. We do not operate our own server infrastructure for client data.

Platform	Purpose	Key Certifications	Encryption
Anthropic Claude Max	AI-assisted analysis; isolated per-client Projects	SOC 2 Type II	TLS 1.3 / AES-256
Box.com	Document storage and secure client sharing	SOC 2, ISO 27001, FedRAMP, HIPAA, PCI DSS, FIPS 140-2	TLS 1.3 / AES-256 at rest and in transit
GoDaddy / Microsoft 365	Business email with Advanced Email Security (Proofpoint)	SOC 2, ISO 27001, HIPAA, GDPR	End-to-end encryption, MFA enforced

2. ANTHROPIC CLAUDE MAX — AI ANALYSIS

NED uses Anthropic's Claude at the Max subscription tier. Model training is disabled — client documents and conversations are not used to train any AI model and are not shared with any other entity. Claude is used to assist with document review, analysis, and drafting. All AI output is reviewed and verified by a qualified NED principal before delivery.

Projects — Isolated Per Engagement

NED uses Claude's Projects feature to maintain a dedicated, isolated workspace for each client. Documents and conversations are contained within the client's project and are not accessible to other clients.

Security documentation: privacy.claude.com

3. BOX.COM — DOCUMENT STORAGE & SHARING

Encryption

Files encrypted at rest using AES-256. Files encrypted in transit using TLS 1.3 (TLS 1.2 fallback). Box employs a key-wrapping strategy applying a second layer of 256-bit AES encryption. Box is FIPS 140-2 certified.

Access Controls & Redundancy

Zero-trust architecture with SSO, MFA, and role-based permissions. NED configures folder-level access per engagement. Files automatically replicated to backup facility at upload. Active-active data center redundancy. Ransomware rollback capability.

Certifications

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

Security documentation: box.com/trust

4. GODADDY / MICROSOFT 365 — EMAIL

Encryption & Threat Protection

Microsoft 365 encrypts all intra-organization messages automatically. For sensitive communications to external recipients, upon client request, NED can use GoDaddy's Advanced Email Security (powered by Proofpoint), which encrypts outbound messages end-to-end in transit. Advanced Email Security includes anti-phishing, malicious attachment scanning, spoofing quarantine, and spam filtering.

Authentication

MFA enforced on all accounts via Microsoft Security Defaults. Authenticator app (TOTP) recommended. Legacy authentication protocols blocked.

Certifications

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

Security documentation: godaddy.com/help/tips-for-protecting-my-email-40055 · microsoft.com/trust-center

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 renewable energy companies. For most of these engagements, the relevant materials — data room documents, IE reports, financial models, equipment specifications, interconnection agreements, transaction correspondence, software specifications and project documentation, and marketing and communications materials — fall squarely 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 (csrc.nist.gov/pubs/sp/800/53/r5/upd1/final). Controls listed below apply to the three platforms NED uses — Anthropic Claude, Box, and Microsoft 365 — and to NED's practices for session management, authentication, and access control.

NED never stores client data on laptops or local devices. All client materials reside exclusively on Claude (Anthropic's infrastructure), Box, or Microsoft 365.

NIST Control	Reference	How NED Implements It — Platforms: Claude, Box, Microsoft 365
Multi-Factor Authentication	IA-2	MFA enforced on all three platforms — Claude, Box, and Microsoft 365. Authenticator app (TOTP), not SMS, per NIST SP 800-63B. Microsoft Security Defaults enforce MFA and block legacy authentication. Box enforces MFA via zero-trust architecture.
Session Lock	AC-11	All NED devices auto-lock after inactivity. Client data is never stored on local devices — a locked device exposes no client materials. Claude, Box, and Microsoft 365 each require separate re-authentication with MFA.
Password Management	IA-5	Passwords are never reused across services. Password complexity and length requirements meet or exceed NIST SP 800-63B guidelines.
Encryption in Transit	SC-8	TLS 1.3 (TLS 1.2 fallback) on all three platforms — Anthropic, Box, and Microsoft 365. No client materials transmitted over unencrypted channels.
Encryption at Rest	SC-28	AES-256 at rest on all three platforms. Box applies additional key-wrapping (second layer of AES-256). FIPS 140-2 certified (Box). Client data is never stored unencrypted on local devices.
Least Privilege Access	AC-3, AC-6	Access to client materials limited to NED principals working on the relevant engagement. Box folder permissions configured per engagement. Claude Projects enforce isolation at the AI layer.
Login Attempt Controls	AC-7	All platform accounts (Claude, Box, Microsoft 365) lock or alert after a threshold of failed login attempts. Limits brute-force credential attacks.

Data Backup	CP-9	Box replicates all files to backup facility at time of upload. Active-active data center redundancy. Ransomware rollback to last uncorrupted version. No local backup copies held by NED.

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 serves two purposes: it 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 it conforms to standard professional services data retention practices consistent with applicable statutes of limitations and recordkeeping norms.

Archived materials are stored in a dedicated area of NED’s Box environment. 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.

For questions about NED's security practices, contact Jon Previtali at jon@askned.ai or (415) 694-0935.

This document was prepared by New Energy Diligence — askned.ai. Last updated March 24, 2026.