nylas

PUBLIC

WHITE PAPER

Nylas Security White Paper

Enterprise-grade security and privacy controls at the heart of the Nylas communications platform.

DOCUMENT OWNER
Security

LAST REVISION
April 10, 2026

VERSION
v2.2

CONTENTS

ABSTRACT

This white paper provides a comprehensive overview of the security, privacy, and compliance framework governing the Nylas cloud communications platform. It outlines the organization's multilayered approach to protecting customer data, which integrates robust operational security — such as access control, encryption at rest and in transit, and continuous system monitoring — with a strong commitment to industry standards like SOC 2 Type II, HIPAA, PCI-DSS, and ISO 27001. The document further details governance structures, including incident response protocols, business continuity planning, and rigorous third-party risk management. Additionally, it addresses the controlled use of artificial intelligence — emphasizing data minimization, transparency, and strict adherence to privacy regulations such as GDPR and CCPA — ultimately serving as a resource to ensure the confidentiality, integrity, and availability of the Nylas infrastructure.

CONTACT For security, compliance, and privacy inquiries, please contact **security@nylas.com**.

02

SECTION 02

Security

Nylas adheres to a high level of operational excellence through multiple interlocking components that make up the security program. The controls that follow are outlined below.

02 / SECURITY — ACCESS, IDENTITY & RESILIENCE

Access control

Access to data is assigned on the principle of least privilege and role-based access, with procedures and controls to limit access to customer data and mitigate insider threats.

Authentication

API requests are authenticated using short-lived access tokens, application-level API keys, or session-based credentials. Nylas supports Hosted OAuth and Bring Your Own (BYO) models, with automated token management.

Availability

All service-impacting and business-critical incidents are monitored and responded to 24/7, 365 days a year. Real-time uptime, status, and SLAs are published at status.nylas.com.

Background checks

Processes determine whether a prospective member of the workforce is sufficiently trustworthy to work in an environment containing Nylas information systems and customer data.

Backups

Regular backups of customer data are performed in accordance with defined retention and recovery requirements.

Business continuity & disaster recovery

A Business Continuity Plan and Disaster Recovery Plan ensure ongoing confidentiality, integrity, availability, and resilience, including procedures for system restoration. Both are updated and tested at least annually and reviewed in third-party audits.

Change control

Formal change management processes approve, track, and review changes within the computing environment.

Code reviews

A comprehensive test suite and industry best-practice code reviews ensure security safeguards are upheld prior to launching new features.

02 / SECURITY — ENCRYPTION, NETWORK & THREATS

ENCRYPTION AT REST

AES-256

All customer data encrypted at rest. Highly sensitive data such as end-user credentials gets an extra application-level layer.

ENCRYPTION IN TRANSIT

TLS 1.2+

Bidirectional session traffic between the customer application and Nylas is encrypted; methods are updated and renewed on expiry.

Denial-of-service (DoS) prevention

Best practices for preventing DoS attacks, including a Web Application Firewall (WAF) and established DoS mitigation practices.

Incident response

An extensive program using anomaly detection, intrusion detection, and other methods to detect, identify, report, respond to, and resolve security incidents in a timely manner.

OAuth2 & passwords

OAuth2 is supported for secure authentication to supported providers. Strong authentication controls, including multi-factor authentication, govern access to systems that process customer data.

Perimeter controls

Industry-standard practices secure the infrastructure; firewalls restrict access from external networks and between internal systems, limited to only the ports and protocols required.

Physical security

As a remote-first, cloud-native CPaaS company, Nylas selects cloud service providers with strong physical security programs securing their data centers.

02 / SECURITY — GOVERNANCE, MONITORING & VENDORS

Policies and procedures

Documented security policies and procedures prevent, detect, contain, and remediate security events — assigning responsibilities to roles, running a formal risk management program with periodic assessments, and providing a framework of controls safeguarding systems and customer data.

Protection of storage media

Storage media containing customer data is properly sanitized or destroyed prior to disposal or re-use. All media is protected against unauthorized access or modification, tracked in an asset registry.

Responsible disclosure

A vulnerability disclosure program allows external researchers to report security issues responsibly.

System hardening

System configuration parameters include procedures to disable unnecessary services on devices and servers.

System monitoring

All access to the production environment is logged and audited regularly; the production cluster is accessible only to authorized operational staff and engineers. Code must pass rigorous security tests before deployment.

Third parties

Any vendor, subprocessor, or subcontractor receiving customer confidential data agrees to maintain appropriate safeguards aligned with industry standards — including third-party providers of AI and machine learning services.

Vulnerability management

A vulnerability management program identifies, assesses, and remediates risks to systems and data, including mitigation of issues found by penetration tests, the Bug Bounty Program (BBP), auditors, or other external constituents.

03 / ARTIFICIAL INTELLIGENCE & DATA PROCESSING

Controlled, limited, and transparent

Nylas leverages AI technologies to support specific product features and internal operations. These capabilities are implemented in a controlled and limited manner, with a focus on protecting customer data and maintaining transparency. AI-powered functionality may process user-provided content for purposes such as summarization, structuring, or generating insights within defined workflows.

Nylas applies data minimization principles to AI processing and limits the data shared with third-party AI providers to what is necessary. Where third-party AI services are used, Nylas conducts vendor due diligence and ensures appropriate contractual and security safeguards are in place.

No training

Nylas does not use customer data to train general-purpose machine learning models. AI processing is performed in accordance with applicable data protection and privacy requirements, and internal policies and controls govern the use of AI technologies — including restrictions on the processing of sensitive data where appropriate.

04 / COMPLIANCE

Nylas engages one or more third parties to evaluate processes and systems against industry-accepted standards at least annually, ensuring continued compliance with obligations imposed by law, regulation, or contract. Results and any remediation activities are documented and available upon request.

SOC 2 TYPE II

Assures customers the provider's security apparatus is working smoothly. Nylas' report covers the security, availability, and confidentiality trust service criteria.

ISO 27001

Provides requirements for an information security management system within the context of an organization.

ISO 27701

Sets requirements for establishing, implementing, maintaining, and continually improving a Privacy Information Management System.

HIPAA

Protects sensitive patient health information. Nylas supports customers building HIPAA-compliant applications and offers a Business Associate Agreement (BAA) for eligible use cases.

PCI-DSS SAQ-A

Nylas does not store, process, or transmit cardholder data — using Stripe, a PCI Level 1 certified processor — and has completed the PCI DSS Self-Assessment Questionnaire and Attestation of Compliance.

05 / PRIVACY

Artificial intelligence (AI)

Any use of AI technologies involving personal data is aligned with applicable privacy laws and internal data handling policies.

CCPA

The California Consumer Privacy Act gives consumers more control over the personal information businesses collect. Nylas is compliant with California privacy regulations — see the Supplemental California Privacy Notice in the Nylas Privacy Policy.

Data minimization

Nylas limits the processing of personal data to what is necessary for the provision of services, processing information you submit, that is automatically collected through use, and that is collected from third parties when securing and marketing the services.

Data portability & erasure

Individuals may contact Nylas with personal-information inquiries or to modify, update, or exercise applicable statutory rights, irrespective of where they reside — at .

Data processor agreement

A legally binding agreement between Nylas and the customer outlining privacy provisions.

Data quality

Under laws including the CCPA and GDPR, individuals have the right to access personal information and to correct, amend, restrict, or delete it.

05 / PRIVACY — CONTINUED

Data retention

Nylas retains personal information until it is no longer needed to fulfill the processing purposes — see “Closing Your Account and Deletion” in the Nylas Privacy Policy.

GDPR

The EU GDPR harmonizes data privacy laws across Europe to protect and empower all EU citizens’ data privacy. Under the GDPR, Nylas is considered a data processor.

Personal data breach

In compliance with GDPR, Nylas maintains incident response procedures designed to notify customers of applicable data breaches in accordance with contractual and legal obligations.

Privacy policy

The Nylas Privacy Policy is publicly accessible at nylas.com/privacy-policy.

Subprocessors

Nylas maintains a Record of Processing Activities (RoPA). Customers receive email notification ten (10) days prior to any update to the Nylas subprocessor list — see the Nylas Subprocessors page.

INQUIRIES For security, compliance, and privacy inquiries — including data-subject requests — contact **security@nylas.com**.

LEARN MORE

Security you can verify

Reports, certifications, real-time status, and subprocessor details are available through the Nylas Trust Center.

TRUST CENTER	STATUS	CONTACT
nylas.com/trust	status.nylas.com	security@nylas.com