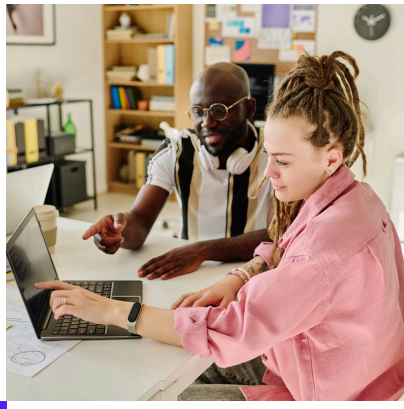
Elastic Email

Security and Compliance Handbook



About Us

Elastic Email is a cloud-based communication platform, originating from email delivery and marketing, designed to help small businesses create, send, and manage email campaigns, team communication, and a help desk.

01 Introduction

This document outlines the practices and commitments we have in place to protect your data and support your regulatory obligations.

02 Our Commitment to Security

Outlines our approach to maintaining the confidentiality, integrity, and availability of customer data.

03 Infrastructure and Data Hosting

Describes global data center locations, redundancy, and safeguards for reliable, secure hosting.

04 API Security

Covers encryption, password protection, logging, and secure API key management practices.

05 Email Authentication

Explains how SPF and DKIM protect domain reputation and prevent email spoofing.

06 Access Control

Details user roles, permissions, and best practices for authentication and access security.

07 Monitoring and Logging

Describes activity tracking, event logging, and procedures for identifying and responding to incidents.

08 Data Privacy & Compliance

Summarizes GDPR and other regulations and laws alignment, and customer responsibilities for lawful data processing.

09 Vendor & Third-Party Risk

Explains how Elastic Email manages subprocessors and vendor relationships securely.

10 Limitations & Customer Responsibilities

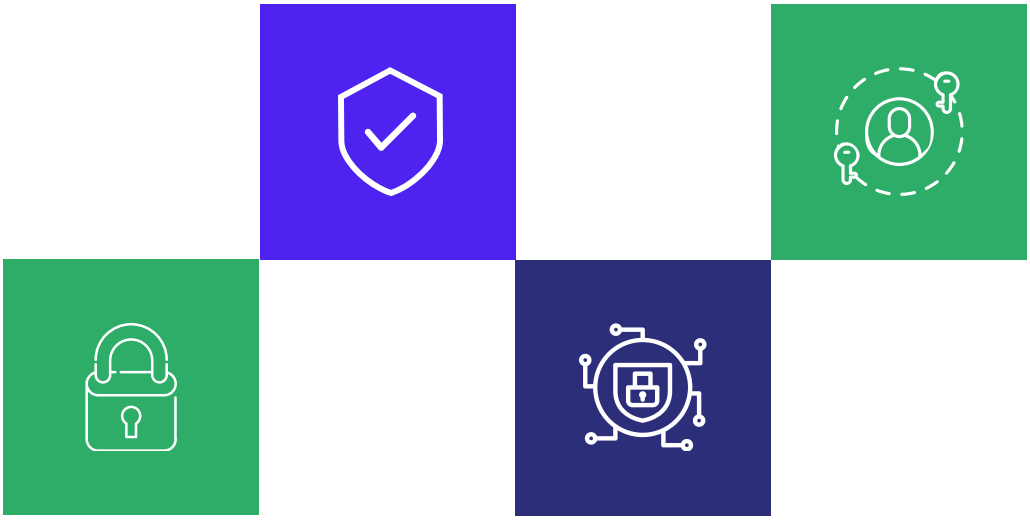
Clarifies shared security responsibilities and areas requiring customer diligence.

Security isn’t an add-on — it’s the foundation of trust, because **safeguarding data means safeguarding relationships.**

Our Commitment to **Security**

WE PROTECT EVERY MESSAGE, CONNECTION, AND CUSTOMER

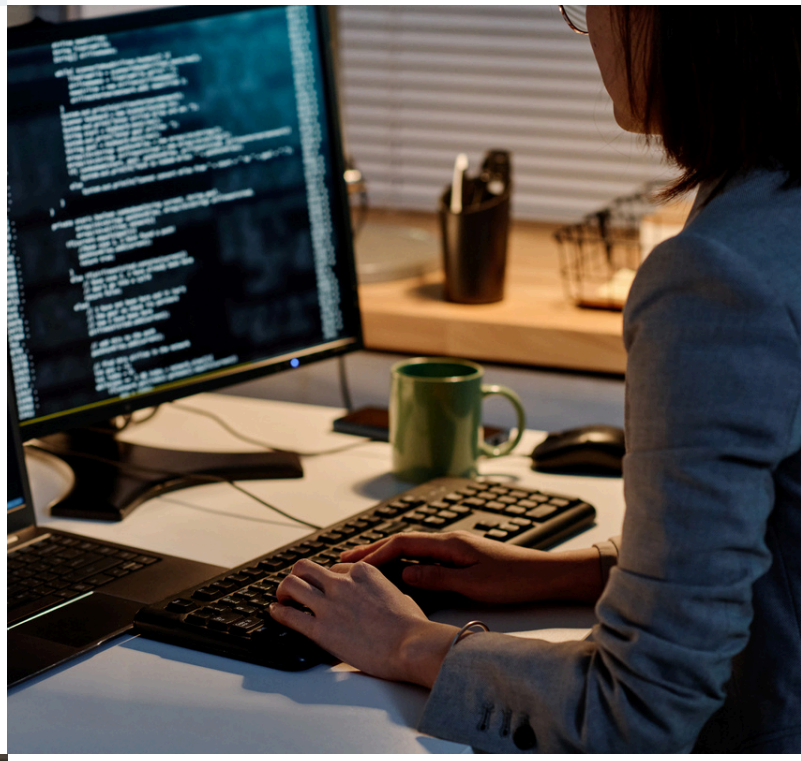
At Elastic Email, we take the security of your privacy and data extremely seriously, and we want to be as transparent as possible about how we conduct business and implement security measures. We recognize that email infrastructure is a critical component for our customers, often carrying sensitive data. Our goal is to design and operate our systems with confidentiality, integrity, and availability in mind, and to enable our customers to meet their compliance and privacy obligations.



Infrastructure and Data Hosting

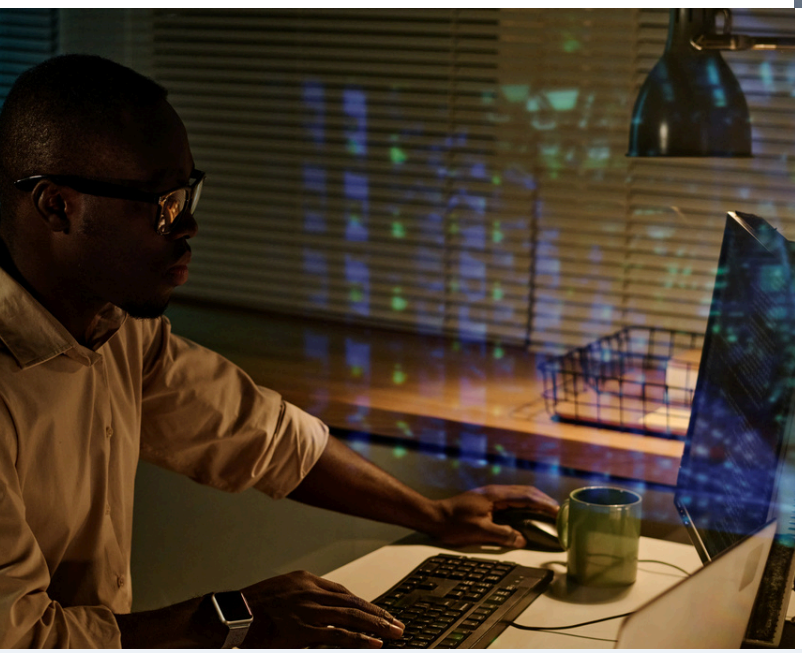
CLOUD-BASED DATA CENTERS

Elastic Email uses cloud-based data centres located in the United States, Canada, and the European Union.



DATA REDUNDANCY AND BACKUPS

Databases have full real-time replication configured, and storage uses redundancy to improve reliability. Multi-tenancy is achieved through separate databases and logical data separation.



AUTHENTICATION REQUIREMENTS

For domain-based email sending, customers are required to verify domains, add appropriate DNS records (SPF, DKIM) to improve deliverability, and help authentication.


Security is
a **strategic**
investment,
not an
afterthought.

Application and API **Security**

USER ACCOUNT SECURITY

Elastic Email account passwords are hashed when they are stored. A hash is one-way encryption, so no one can view the passwords, and they can only be reset.

EVENT LOGGING

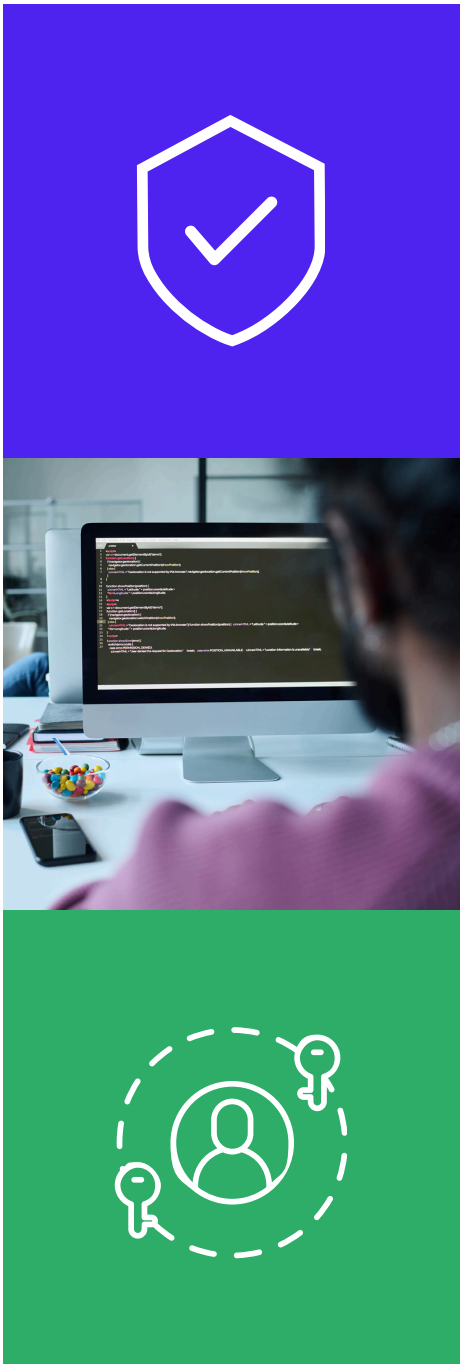
Login and security-relevant events (password changes, API key operations, exports) are logged with metadata (IP address, browser, user agent).

API SECURITY

All API, web interface, and SMTP traffic supports encryption (SSL/TLS) for data in transit.

ACCESS PROTECTION

We support a granular access model for our accounts, users, and administrators, granting only the required access to all stakeholders.



Email Authentication

Elastic Email supports sender authentication via SPF and DKIM records. These mechanisms help ensure that outgoing mail aligns with your domain, protecting the sender reputation and reducing spoofing risk.

Access Control

Elastic Email supports granular access control. Roles and permissions define what users can do. It's recommended that customers enforce strong passwords, enable 2FA, and restrict API key usage to the minimal required scope.

Monitoring and Logging

Activity logs are maintained for account-level operations. Customers are encouraged to monitor their own usage patterns and set alerts for unusual activity.

Data **Privacy** & **Compliance**

Data Privacy

Elastic Email stores and processes your personal data and your contacts' personal data solely to perform the services you have signed up for. We don't sell your information or use it for profiling secondary business objectives.

Compliance

Elastic Email is aware of regulatory frameworks such as the General Data Protection Regulation (GDPR) and has published guidance for customers to help them address their obligations under the GDPR.

Governance

All employees undergo general security training and testing as part of Elastic Email's standard onboarding process. Elastic Email handles sensitive data through the internal system to minimize risk and combat security breaches.

PROTECTING PERSONAL DATA THROUGH TRANSPARENCY, RESPONSIBILITY AND GLOBAL STANDARDS

Elastic Email is committed to ensuring that data privacy and protection are integral parts of every service we deliver. We comply with global regulations, such as the General Data Protection Regulation (GDPR), and support customers in meeting their legal obligations as data controllers.

Our privacy framework includes strict data-handling procedures, transparent policies, and technical safeguards that limit access to customer information. Personal data is processed only for legitimate business purposes and in accordance with customer instructions.

We believe that compliance is not a checkbox exercise, but a continuous responsibility. By maintaining accountability and openness, we help our customers build trust with their audiences and ensure that every message is sent with privacy in mind.

Vendor & Third-Party Risk

Elastic Email employs third-party service providers (e.g., cloud hosts, analytics tools), and customers are encouraged to inquire about subprocessors, data flows and contracts (Data Processing Addendum) with Elastic Email.

Customers should ensure that their use of Elastic Email aligns with internal vendor management policies and that appropriate due diligence has been conducted.

Customer Responsibility

Elastic Email offers a secure and resilient platform for email marketing, delivery, and communication, with features and controls to help customers manage authentication, monitor usage, and configure robust send infrastructure. To maximize security and compliance value, we recommend customers:

- retain responsibility for how they configure and use the service, eg, credential management, domain authentication, API security, consent management.
- ensure their data is handled in accordance with applicable laws and that they implement appropriate controls over their own processes, such as list management, data minimization, deletion, and retention.

Get In Touch

329 Howe St PMB 2135
Vancouver, BC, Canada
https://elasticemail.com
support@elasticemail.com

Author: Elastic Email
Publish date: November, 2025