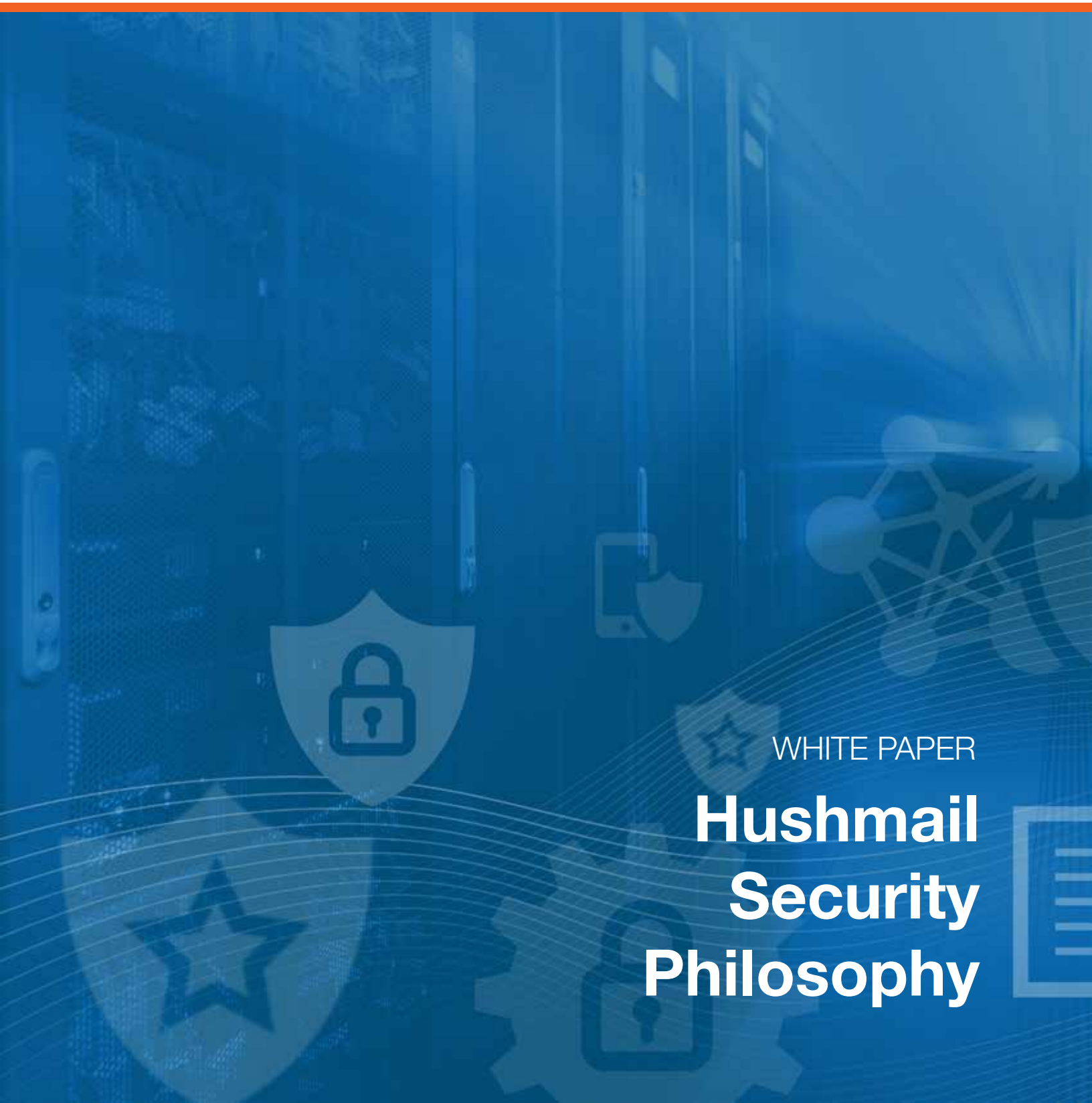
Hushmail



WHITE PAPER

Hushmail Security Philosophy

Table of Contents

Security Philosophy

A Culture of Security and Privacy

At Hushmail, enhancing organizations' security and preserving their privacy are at the core of what we do, informing every decision we make. At other companies, security and privacy may be important features of the products and services, but at Hushmail they are our top priorities throughout our organization. They are the basis of our products, our customer service and our company culture.

We provide security through technology, but we know that technology alone cannot ensure complete security. At Hushmail we complement our systems and software with clearly defined policies that ensure accountability, vigilance and company-wide compliance.

Simplicity Brings Security

We also value simplicity. Not only by making products that our customers can use easily, but also because keeping things simple helps us keep our customers secure and to better understand potential threats. For that reason, we are committed to keeping both our systems and our organization simple, nimble and flexible, by embracing a structure and culture that strives for simple solutions that function flawlessly.

The Importance of Encryption

We believe that encryption is an essential tool for maintaining security and privacy. So, in addition to TLS/SSL encryption, OpenPGP encryption is integrated into our products and services.

Application Security

Security is built into our applications.

Encryption

Account creation occurs server-side in a web application. The email address, passphrase, and other values needed for account creation are sent from the web browser to the server.

SSL/TLS for Data in Transit

Our systems require strong TLS/SSLencryption for all communication between customer computers and devices and our servers. For transmitting email between email servers, Hushmail uses SSL/TLS encryption whenever it is available, although we allow email transmission to and from systems that do not support TLS/SSL if the customer's configuration allows it.

Hushmail uses advanced SSL/TLS security features such as Forward Secrecy, HTTP Strict Transport Security and Certificate Pinning.

OpenPGP Encryption

The bodies and attachments of emails between Hushmail customers are also protected with OpenPGP encryption, which uses a unique key for each recipient, and the emails and attachments stay encrypted when stored on disk on the Hushmail servers.

OpenPGP encryption is available through Hushmail's webmail service and iPhone app, and when accessing Hushmail over IMAP or POP3.

Encryption for Emails Sent Outside of Hushmail

When Hushmail customers send email to recipients who are not using Hushmail, the email can still be OpenPGP encrypted using a secure question and answer method. With the email encrypted and stored on our servers, the recipient receives an email notifying them that they have received a secure email, and they are provided a link to access it.

When the recipient picks up the encrypted message, they can generate and store their own OpenPGP keys at that time, which will result in greater security for future messages.

This feature provides a range of options for configuring the process by which encrypted messages are picked up and when OpenPGP keys are generated for recipients.

Enhanced Encryption in Hushmail for iPhone

When sending an OpenPGP-encrypted email using Hushmail for iPhone, the encryption is applied to the messages before they even leave the device, so email is protected by SSL/TLS up to our servers and by OpenPGP all the way to the recipient.

Archiving

Administrators can configure their domains with special archive keys, so that all email sent to and from their users will be archived for future access.

Authentication

Passphrases

We encourage the use of strong passphrases rather than passwords to protect data.

Hushmail does not store the passphrases themselves on our system, but rather a hashed value produced from the passphrase. That hashed value can be used to verify that a passphrase is correct, but the actual passphrase cannot be derived from the hashed value.

In webmail, the passphrase is sent to our servers for verification through an encrypted SSL/TLS connection. In Hushmail for iPhone, the hashed value is created on the iPhone so the passphrase is never sent to the server for authentication.

Two-Step Verification

Two-step verification requires a Hushmail customer to provide a verification code in addition to a correct passphrase when using a computer or device for the first time. We will send this verification code by SMS or by email to an alternate address, or it can be generated by a smartphone app. This makes it more difficult for unauthorized parties to access an account, even if they have the passphrase.

Rate Limiting

All authentication to our system is rate limited. If too many attempts are made to access an email account, the email account will be locked for a period of time.

Application Firewall

Our application firewall detects and blocks attempts to break into our systems. It is a combination of well-established open-source technologies and those created in house. Our firewall is deeply integrated with our applications to ensure that suspicious activity is quickly detected and threats are mitigated. This deep integration allows us to block threats more aggressively with minimal risk of false positives.

If the application firewall detects an event that is suspicious but not considered severe enough to merit immediate blocking, our network operations team is automatically alerted, and investigates.

Antivirus and Spam Filtering

Hushmail detects viruses and spam using multiple email scanners, which leverage a wide range of technologies including machine learning and pattern matching. We combine commercial and open-source solutions with systems we develop ourselves to ensure maximum coverage.

In addition to automated systems that prevent spam, our abuse team monitors our network for unusual activity in order to block threats or quickly purge them from affected mailboxes.

Hushmail for iPhone Device Security

In addition to the OpenPGP encryption and other security features of our products and services, Hushmail for iPhone offers enhanced device security. This includes a feature that allows you to keep your email locked even when your iPhone is unlocked. The app also integrates Touch ID, and offers full use of the iPhone's built-in file protection.

Network Security

Our applications run on a network built for security.

Network Simplicity

Simplicity is fundamental to our security strategy, and our network reflects that. There is very limited access through the firewalls to a minimal set of network services. This helps minimize the risk of a malicious part being able to breach our systems and helps ensure that our network operations can better detect abnormal activity.

Network Segmentation

Our network is segmented into zones categorized by the level of exposure to the Internet and the sensitivity of data stored on systems. The network used for customer data is physically different from the office networks, and the office networks are in no way privileged in their access to the network that holds customer data.

Server Hardening

Our servers are configured to be compliant with the CIS Security Configuration Benchmark.

Penetration Testing

Vulnerability scans are run against our network regularly, and manual penetration testing is conducted and documented.

Updates and Vulnerability Management

All systems on the production network are monitored for updates by a combination of automated systems and manual processes. Security updates are applied as soon as possible after becoming available—24 hours a day.

Operating systems that are prone to viruses and other security issues are explicitly prohibited from any network that stores customer data.

File Change Monitoring

File change monitoring on systems exposed to the Internet ensures that we will be alerted of a system compromise.

Centralized and Segregated Logging

Our logs are centralized on a segregated system and retained for up to 18 months, depending on the information, to ensure we can audit suspicious activity.

Physical Security

We ensure the physical security of our data and systems.

Of Customer Data

Hushmail servers are located in Vancouver, British Columbia, Canada, in a hosting facility monitored by onsite security teams and closed-circuit television. Access is controlled by card keys and limited to essential personnel only. Visitors are prohibited.

When customer data is stored offsite for backups it is always encrypted so it cannot be used, even if stolen.

Of the Office

The Hushmail offices, also located in Vancouver, are kept locked at all times, and any visitors must be escorted by staff. The offices are monitored by video and an alarm system.

Customer data is never stored on computers at the Hushmail offices.

Process Security

Our business processes are designed to ensure security.

Social Engineering

Every hacker knows that the best way to exploit any system is through its people. Hushmail team members are trained to always be cautious, and verify identities rigorously. In particular, the support team follows strict guidelines when granting access to any information.

Lost Passwords and Passphrases

Many organizations have a certain amount of flexibility when it comes to letting customers in when passwords or passphrases are lost. Unfortunately, that flexibility also makes the organizations vulnerable.

At Hushmail we are strict about granting access in the case of a lost passphrase. Unless a customer has configured the passphrase recovery option as part of their Hushmail Business account setup, we will never grant access to an account without the correct passphrase.

Access Control

At Hushmail we have rigorous controls over the access granted to team members. We ensure that new team members are thoroughly vetted, that they are granted access only to systems required for their job functions, and that if anyone leaves the organization, all access is promptly revoked.

Use of Third-Party Services

When we use third-party services, we conduct a documented security evaluation, and specify what sort of information can be used with the third-party service. Customer emails can never be exposed to a third-party service, with the exception of emails that customers have explicitly reported as spam.

Risk Assessment

We regularly apply risk assessment techniques to evaluate new courses of action, and to review changing conditions around previous choices. These decisions are documented.

Policy and Compliance

We use SSAE 16 SOC 2 as a basic framework for our security policy. We complement it with measures intended to best serve the needs of our customers.

For many other companies, SOC 2 compliance means simply hosting their service at an SOC 2-compliant data centre. However, Hushmail is fully SOC 2 compliant at an organizational level. This means that every aspect of our operations is covered, not just server hosting.

We are also compliant with the HIPAA Security Rule, FIPAA and PCI-SAQ D.

Hushmail's security policy outlines operational protocols in a variety of areas, including:

- **Authority and Responsibility.** Who is responsible for what within our organization.
- **Policy Management.** How we create, change, review and enforce policy.
- **Risk Assessment.** How we formally make decisions and assess risk.
- **Incident Response.** How we deal with unusual events.
- **Privacy Rules.** How a customer's data is handled, and how we communicate that information to the customer.
- **Training and Awareness Requirements.** How we train staff and contractors.
- **Arrival and Departure Processes.** How staff and contractors enter into employment and leave employment.
- **Data Classification.** The types of data we deal with and specifies rules for managing that data.
- **Third-Party Service Providers.** How we deal with third-party service providers.
- **Encryption.** Proper use of encryption when it is required by other policies.
- **System Development Processes.** Our methods for building, testing, deploying, evaluating, maintaining, and upgrading systems.
- **Acceptable Usage.** What employees and contractors can and cannot do with company systems.

- **Inventory Control.** What the company owns.
- **Facility Protection.** Who can enter our facilities and how we restrict access to those who do not qualify for entrance.
- **Identification, Authentication and Authorization.** How people obtain the right to access systems and data.
- **Logging and Auditability.** Rules for recording actions, including how long records must be kept.
- **Network Protection.** How computer systems must be protected from attacks.
- **System Availability.** How we deal with ensuring our systems are available for use by customers.
- **Disaster Recovery.** How we deal with extreme events.
- **Compliance with Standards.** How we maintain compliance with SSAE-16, HIPAA, PCI and other standards.

Security policy documentation is available upon request.