Mailshake Information Security Policy

Information Security Policies

Policy #	IS-01
Effective Date	June 30, 2019
Contact	josh@mailshake.com

At Mailshake, we have developed robust engineering, security, and hiring processes to safeguard customer data. This document details some of the things we do to keep your information secure.

Encryption

We apply the most advanced encryption technology publicly available to secure data. Using industry-leading encryption technologies such as TLS/SSL and AES-256 encryption, Mailshake encrypts data in transit and at rest, including on payment pages and into and out of Amazon Web Services (AWS). All data in transit requires HTTPS and SSL certificates, while data at rest utilizes AWS encryption-at-rest technology built into their Relational Database Service (RDS).

Sensitive Data

We do not store credit card or other payment information, aside from general details such as the last four digits of a card. We do not encourage our users to submit any highly sensitive data such as social security numbers, data that might be subject to HIPAA rules, etc.

In cases where our application needs authentication or other credentials that are sensitive, they are stored either in an encrypted AWS Parameter Store or in our encrypted database that is within our Virtual Private Cloud (VPC). The company's 1Password account also stores credentials for applications with which we integrate or use for business purposes.

Hiring Policy

We have a rigorous hiring process to ensure that anyone we hire can perform their job function. We provide internal training when needed, but strive to hire experts with strong track records and references. Our employees work closely with each other and share knowledge as an integral part of each task that is performed, leaving no single employee alone with confidential and critical knowledge. For new employees, we interview thoroughly, require coding exams, and research referrals to be as sure as possible that the employee has the right skills for the position.

Account Security

All Mailshake employees are required to have multi-factor authentication enabled to access their email and other Google Workspace products. A technical policy is in place to enforce this. Similarly, all engineers with access to our hosting platforms are required to have multi-factor authentication enabled. We have specific security roles and policies to limit the permissions we give individuals.

Hosting

We host Mailshake services in AWS servers in the us-east-1 region located in Northern Virginia in the United States. AWS data centers are state of the art, using innovative architectural and engineering approaches. Amazon has many years of experience in designing, constructing, and operating large-scale data centers. This experience has been applied to the AWS platform and infrastructure. AWS data centers are housed in nondescript facilities, and physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. All visitors and contractors are required to present identification and are signed in and be escorted continually by authorized staff.

AWS only provides data center access and information to employees and contractors who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, access is revoked immediately, even if that person continues to be an employee of Amazon or AWS. All physical access to data centers by AWS employees is logged and audited routinely.

When a storage device has reached the end of its useful life, AWS procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. AWS uses the techniques detailed in DoD 5220.22-M (“National Industrial Security Program Operating Manual”) or NIST 800-88 (“Guidelines for Media Sanitization”) to destroy data as part of the decommissioning process. All decommissioned magnetic storage devices are degaussed and physically destroyed in accordance with industry-standard practices.

AWS is trusted by over a million organizations, including security-focused companies such as FICO, Airbnb, Dow Jones, Intuit, and GE. If you’d like to learn more about AWS security practices, please refer to the following links:

- ISO Global Certification
- Overview of Security Processes
- Service Organization Controls Report
- AWS Customer Case Studies

We use many AWS-provided solutions including relational databases, queuing, messaging, identity management, encryption, and caching. As part of our business continuity plans in case of disaster, our

system is architected for automated recovery. We aim to eliminate single points of failure in our infrastructure and have built redundancy into many of our services. Most Mailshake services are redundant across two (2) or more physically isolated and resource-independent availability zones in Northern Virginia.

We use AWS CloudFront to efficiently serve content globally. CloudFront has numerous locations around the world, which lets us speed user access to content such as course assets (images, videos, audio), logos, characters, and course templates.

Network Security

All traffic to and from our reachable infrastructure is encrypted via SSL. Most of our infrastructure is locked down inside a virtual private cloud that protects all inter-system communication. These private systems only communicate to the outside world via a gateway server.

There are one or two servers used by our most trusted engineers as gateways into the private network for troubleshooting issues and monitoring system performance. These servers are only accessible via SSH ports and are restricted to a very small number of IP addresses.

Engineering, Quality Assurance (QA), and Deployment

We develop all software in-house using GitHub as our code source repository. Our team develops software and conducts code reviews in repositories using pull requests. All pull requests must be approved by at least one other engineer, reviewed for potential performance and security issues, pass all automated tests, and pass linting rules that help protect against bad coding practices. No code is merged until those steps are completed and automated builds ensure that after code is merged, it still passes all tests and linting before being deployed to our infrastructure. Rollback procedures are in place in case we need to revert the code to a previous state.

User Authentication

We also follow best practices around our processes for user authentication when users are logging into our sites and services. When a user signs up for a Mailshake ID, they either provide their email address, or a team admin sends an invite to the user's email address. This is part of the process that creates a unique login and set of credentials for each person using Mailshake.

Mailshake does not store passwords either in clear text or in a decryptable format. We use the SHA-256 algorithm to generate a unique hash based on the user's supplied password and a salt that is unique for each user. When password validation is attempted, we generate the hash again and compare it to the one stored for the user.

We require a minimum length for passwords and we maintain a list of bad passwords that we outright reject. When a user changes their password, we require that they enter the correct existing password in order to set a new password. In the event of a forgotten password, we generate a unique link that is sent to their email address where they can set a new password. Those links are good for 24 hours before they cease to function.

Disaster Recovery and Incident Management

Our team is prepared to handle disasters of various kinds. We have a simple process that we follow to ensure we've properly communicated with anyone who is affected and to prevent future incidents from happening.

1. Incident categorization: figure out what kind of issue we're dealing with
2. If there is a significant impact on system usability:
    a. Post a notice on Twitter summarizing the issue
    b. Provide periodic updates and estimations for when services will be restored
3. For data loss:
    a. Take the application down and put a maintenance notice up so that no new data is collected
    b. Restore the database cluster from the last backup before the incident
    c. Take the application back up
4. If there was a data breach where customer information was exposed or obtained:
    a. Determine what specific data was breached
    b. If the breach involved a third-party, work with them to gather details and run through any procedures they may have
    c. Notify the customers involved via email that their data was breached
    d. Research and investigate how the data was obtained
    e. Put in solutions to prevent similar issues in the future
5. Patch the issue: if necessary, issue a temporary fix to restore services while working on a longer-term fix

Vulnerability Management

We periodically review each of the various aspects of our system to look for vulnerabilities, outdated software packages, etc. We monitor news articles for newly found security bugs in software or products that we use, are informed via social media about newsworthy issues that may affect our security practices, and we receive newsletters and alerts from Amazon Web Services about security concerns they have learned about either with their products or from incidents experienced by their vast collection of customers using their products.

Acceptable Use

Our terms of service provide us with rules for our customers in how they may use our platform. We do not allow programmatic efforts to target our system aside from defined endpoints such as proper use of our public API. Employees are always expected to act in an ethical manner; not using Mailshake infrastructure for personal or illegal use, only viewing customer data when required to troubleshoot issues, etc.

Security Event Monitoring

We have configured many alarms to monitor system performance which notifies us via email (and other mechanisms) about abnormalities in usage patterns or when certain systems are experiencing high load or issues. We also subscribe to AWS budget notifications which alert us when we've used much more resources than we have in our plan; this can help bring network attacks or similar to our attention. We also have installed diagnostic tools on some parts of our system that allow us to visually drill into usage patterns.

Approval and Ownership

	Name	Date	Signature
Policy Author	Josh Sherman		
Owner / Approved By	Robert Senoff		
Owner / Approved By	Sujan Patel		

Revision History

Version	Description	Approval Date	Approver Name
1.0	Initial document.	6/30/2019	Robert Senoff
1.1	Updated to include info about sensitive data.	8/5/2019	Sujan Patel
1.2	Changed contact and policy author to Dave Donaldson, along with other minor edits.	4/29/2020	Sujan Patel
1.3	Changed contact and policy author to Josh Sherman.	6/28/2023	Josh Sherman

1.4	Minor edits to product names.	7/6/2023	Josh Sherman
1.5	Removed Colin Mathews from approval and ownership section.	7/31/2023	Josh Sherman