Quick Reference Guide

Wasabi Data Security Features and Compliance

Wasabi ensures the physical security of our data centers; employs strong authentication and authorization controls for all cloud compute, storage and networking infrastructure; and encrypts data at rest and in transit to safeguard confidential data. The storage service is built and managed according to security best practices and standards, and is designed to comply with a range of industry and government regulations including:

CJIS
Criminal Justice Information Service

FERPA
Family Education Rights and Privacy ACT

FINRA
Financial Industry Regulatory Authority
SEC Compliance White Paper

HIPAA
Health Insurance Portability & Accountability Act

MPAA
Motion Picture Association of America

GDPR
General Data Protection Regulations

Physical Security of Data Centers

The Wasabi service is hosted in premier top-tier data center facilities that are highly secure, fully redundant, and certified for compliance with:

- SOC 2
- ISO 27001

Each site is staffed 24/7/365 with on-site security personnel to protect against unauthorized entry. Security cameras continuously monitor the entire facility— both indoors and outdoors. Biometric readers and two-factor or greater authentication mechanisms secure access to the building. Each facility is unmarked so as not to draw attention from the outside.

Improving Compliance with Object Lock and Immutable Storage Buckets

Data immutability can help users comply with certain government and industry regulations by adequately protecting against accidental or malicious data destruction. An immutable object cannot be deleted or modified by anyone—including Wasabi.

Immutability can be set at the bucket level or at the object level. With bucket level immutability, when users create a Wasabi storage bucket, they have the option of making it immutable for a configurable retention period (in increments of days, weeks, months or years). Data written to that bucket cannot be deleted or altered in any way, by anyone, until the retention expiration date of the bucket has been reached.

Object lock allows customers to set retention dates at the individual object level. The objects have the same immutable advantages as described above, but the retention policy is set at the object level. This means that the “locked” objects that share a bucket may have different retention expiration dates.

Data Privacy and Security

Wasabi supports a comprehensive set of data privacy and security capabilities to prevent unauthorized disclosure of electronic records. Strong user authentication features tightly control access to stored data. Access control lists (ACLs) and administratively defined policies selectively grant permissions to users or groups of users.

Wasabi encrypts data at rest and data in transit to prevent record leakage. All data stored on Wasabi is encrypted by default to protect data at rest. And all communications with Wasabi are transmitted using HTTPS to protect data in transit.