IT SECURITY & DATA PRIVACY

flock

OUR APPROACH TO SECURITY

Flock takes security extremely seriously. Our most important responsibility is to make sure customer data is secure and protected against unauthorized access. We go through regular audits to meet compliance and make sure we're always adhering to the highest security standards and protocols.

SOC 2 TYPE II CERTIFIED

SOC 2 Type II compliant security architecture w/annual audits

TLS TRANSPORT LAYER SECURITY

Traffic between clients and servers is encrypted using TLS 1.2 w/AES cipher

aws

Hosted on Amazon's AWS servers with a 99.99% uptime record

SECURITY FEATURES

All traffic in transit between Flock clients and servers and data at rest (on disk on our servers) is encrypted using TLS 1.2 with an AES preferred cipher for encrypting all communication, and where available, perfect forward secrecy is used to protect against compromise of long-term private keys.

SSAE Type 2
Flock employs the most rigorous auditing and security standards

AWS Hosting
TLS v1.2 based encryption with secure ciphers

Data Retention
Export data and retrieve deleted or edited messages

Multi-level Admin Controls
Single-point provisioning with custom user permissions

SSO Integration w/Google
Integrates with Google OAuth and SAMLv2 (Azure/Okta)

Domain & IP Whitelisting
Control who can access your environment and from where

IT SECURITY & DATA PRIVACY

AUTHENTICATION

SAML-based SSO Flock enables web-based, cross-domain single sign-on (SSO) via the Security Assertion Markup Language 2.0 (SAML 2.0). SAML 2.0 is the universally accepted standard for exchanging data between security domains.

DATA ENCRYPTION

All communication between mobile applications and backend servers are on top of TLS. All production data at rest is encrypted using AES 256 encryption. This is applicable to all data at rest within the Flock ecosystem. Backend business-to-business communication is based on IPSec Tunnels.

DATA STORAGE

Flock hosts all services in the cloud using Amazon Web Services (AWS). AWS Web Application Firewall (WAF) is used for extra protection. All communication to AWS is TLS v1.2 based with a minimal set of secure ciphers. AWS Data Centre holds all the non-sensitive data like files, images, reporting information, logs etc. Backups are secured and stored in S3 buckets.

COMPLIANCE

Flock is SOC 2 and GDPR compliant. Flock implements best-in-class internal processes and protocols to ensure compliance with regulatory requirements.

Privacy Policy | Data Protection Addendum | List of sub-processors

DISASTER RECOVERY

Flock's web application is hosted in multiple Availability Zones (AZ) within Amazon's North Virginia Cloud Region. We can survive the loss of an entire AZ without service interruption. Redundant copies of customer data are maintained with a well-defined policy for Data Backup and Recovery.