FELT MAPS, INC

SECURITY AND COMPLIANCE WHITEPAPER

Abstract

This document outlines the security and compliance processes adopted by Felt Maps, Inc.

Table of Contents

Infrastructure and Network Security

Physical Access Control

Felt is hosted on a combination of Render and Amazon Web Services (AWS). Felt does not operate its own servers, nor do Felt employees have physical access to Render or AWS datacenters, servers, or storage.

Render

Render is a Platform as a Service provider. Felt uses Render's services in its Oregon, US datacenter.

Render is independently audited for SOC2 compliance. All sensitive Felt data stored on Render is encrypted at rest.

Amazon Web Services (AWS)

AWS is the leading cloud provider used by enterprises and governments worldwide. Felt uses AWS' services in its US datacenters. By using AWS, Felt inherits all the security and compliance features built by AWS and dependent upon the world's biggest companies, including most of the world's leading financial institutions.

Logical Access Control

All Felt employees use designated accounts to access our infrastructure. Employees are not allowed to share access credentials. All access is further protected behind two-factor authentication. All private keys are stored with strong encryption. Access controls are monitored automatically every day and manually quarterly.

Penetration Testing

Felt employs annual penetration testing by an independent third-party. The third-party engages with the production instances of Felt service and are under contract.

Any findings from the penetration testing are investigated by Felt's security team and prioritized accordingly. Penetration testing schedule is monitored automatically.

Third-Party Audits

Both Render and AWS are rigorously audited by third-parties. Both Render and AWS boast SOC 2 Type 2 compliance as well as ISO 270001 certification.

Felt undergoes SOC 2 compliance audits and is SOC 2 Type 2 compliant.

Intrusion Prevention and Detection

Felt aims to make unauthorized intrusion as hard as possible. All Felt compute instances both on AWS and Render run in their own virtual private networks. No Felt compute instance allows SSH access and all compute instances on AWS uses a Serverless infrastructure, meaning all instances are ephemeral and automatically killed when their task is complete or they reach their age-limit, currently set to 24 hours.

Furthermore, Felt uses AWS's CloudTrail technology to monitor access to its services and Cloudtrail logs are further automatically monitored daily for unauthorized access.

Business Continuity and Disaster Recovery

Provisioning

All parts of Sentry service are over-provisioned, meaning all non-transient services like compute instances and databases have a lot of extra capacity in case of a demand spike. Our compute platform on Render is automatically spread across different availability zones and our platform on AWS is automatically horizontally scalable via Amazon's Serverless stack.

Business Continuity Planning (BCP)

All customer data is uploaded to AWS' S3 service. Felt uses versioned controlled S3 buckets with 99.99% availability. All data that is stored on Render is backed up daily. Felt also runs annual business continuity recovery exercises and their schedule is monitored automatically.

Disaster Recovery

All Felt data is uploaded to AWS' S3 service and all Felt buckets are versioned controlled with no public access permissions. In the unlikely case of a disaster, Felt is able to recover the original data from S3 buckets.

Data Security and Privacy

The security and the privacy of customer data is paramount to everything Felt.

Data Encryption

All customer data uploaded to Felt is encrypted at transit and at rest. Customer data uploads from the browser happen over HTTPS via transport layer security (TLS) encrypted connections and the data is stored on versioned AWS S3 buckets that are server-side encrypted. The settings on these buckets are monitored daily automatically.

Application data that is stored on Render databases are also stored with encryption at rest. Felt never stores your password in cleartext.

All Felt web traffic happens over HTTPS and certificates are managed automatically via Render and Cloudflare. Felt's HTTPS settings are monitored automatically.

Data Access

Felt employees might access customer data only for documented reasons and for a limited amount of time. All access happens via individual accounts tied to each employee and is logged for potential audits. Felt employees can store data on their systems for technical troubleshooting or customer support only for a limited amount of time and only if their systems are end-to-end encrypted. Felt employees' personal devices used for such access are monitored hourly automatically.

Application Security

Google Sign-in

Felt allows users to sign-in via Google in lieu of a password. Signing in via Google allows users to benefit from Google's world-class authentication safety features such as multi-factor authentication, passkey authentication and federated logins. Many Felt users integrate their federated login systems with Google, allowing them to have a Single Sign-On provider via Google.

Personal Access Tokens

Felt allows users to create personal access tokens (PAT) to access Felt resources programmatically via application programming interfaces (API)s. PATs are stored with encryption on Felt databases and are exposed in cleartext only during creation. They are never logged. Users can revoke their PATs any time, or create multiple ones for various use-cases.

Email Security

Felt uses a strong domain-based message authentication, reporting, and conformance (DMARC) setup for its email. This makes spoofing (pretending to be Felt) or phishing scams much harder to employ. Felt's DMARC settings are monitored automatically daily. For all domain name service setups, including DMARC, Felt uses AWS' Route 53 service, inheriting the security and audit capabilities of AWS services.

Secure Software Development Lifecycle (SDLC)

Continuous Delivery (CD)

Felt uses a continuous delivery methodology to deliver its software, meaning every single code change is delivered quickly to production. This allows quick resolution of customer issues, including security patches.

Continuous Integration (CI)

Felt uses a continuous integration methodology to develop its software, meaning all code is continuously tested at each step of the process. These tests include static analysis of our code against vulnerabilities, introduction of unexpected dependencies against supply-chain attacks, as well as unit and integration tests against bugs that might impact users and their security.

Version Control

All Felt code is version controlled. Code changes must be requested via cryptographically verified methods and all code changes must be approved by another person before they can be delivered to production via the CI/CD pipeline.

Corporate Security

Malware Protection

All Felt provided computers are registered to our Mobile Device Management (MDM) software. This MDM ensures that the workstations have correctly configured password managers, automatic updates, antivirus software, full disk encryption, and screensaver lock. These settings are checked for every single employee's workstation every day.

Contingency Planning

Felt runs regular business continuity and disaster recovery tabletop scenarios to plan for unforeseen events. These events include but are not limited to loss of key personnel, degradation of key infrastructure, and operational force majeure events. The remediations for these possible events are discussed annually.

Policies

Felt maintains a wide array of policies regarding security. These policies are reviewed and updated annually where necessary.

- Acceptable Use Policy
- Asset Management Policy
- Backup Policy
- Business Continuity Plan
- Code of Conduct
- Controls Assessment Program
- Data classification Policy
- Data Classification, Handling, and Retention
- Data Protection Policy
- Disaster Recovery Plan
- Encryption Policy
- Incident Management Policy
- Incident Response Plan
- Information Security Policy
- Password Policy
- Physical Security Policy
- Responsible Disclosure Policy
- Risk Assessment Policy
- Software Development Lifecycle Policy
- System Access Control Policy
- Vendor Management Policy
- Vulnerability Management Policy

Background Checks

Felt runs a background check for all new hires globally. This check contains information such as:

- Enhanced Identity Verification
- US Criminal Record Check
    - National Sex Offender Registry Scan
    - Security Watchlist Scan
    - Fraud Scan
    - OFAC Global Sanctions Scan
    - Criminal Record Scan
    - Federal Record Scan
    - Single State County Record Scan
    - All State County Record Scan

Security Training

All Felt employees are required to go through annual security training, as well as be presented with the policies. Acceptance of these policies and completion of security training is monitored automatically before employees can access any internal systems that include customer data.

Disclosure Policy

Felt aims to notify customers of any data breaches as soon as possible via email and has documented policies.

Vulnerability Disclosure

Security researchers are encouraged to reach out to Felt's security team at security@felt.com via a working proof of concept. Felt does not have a bounty bug program, and encourages researchers to responsibly disclose issues.

Compliance Attestations and Certifications

Felt has received the following compliances:

SOC 2 Type II (SOC 2 Type 2)

Interested parties can reach out to support@felt.com to request a copy of our SOC 2 Type II report.

Data Privacy Addendum

Felt works with many educational institutions with their unique needs such as Family Educational Rights and Privacy Act (FERPA) and Children's Online Privacy Protection Rule (COPPA) requirements. Felt maintains a robust Data Protection Addendum (DPA). Interested parties can reach out to support@felt.com to request our DPA.