Fulcrum

Fulcrum Security Whitepaper

Overview of Approach

Version 5.2
OCTOBER 2026

Table of Contents

Table of Contents....1
Introduction....2
Organizational Security....2
Artificial Intelligence (AI)....3
Data Protection....3
- Secure Development Process....3
- Encryption....4
  - In Transit....4
  - At Rest....4
- Data Sovereignty....4
- Network Security....5
- Endpoint Security....5
- Access Control....5
  - Least Privilege....5
  - Authentication....6
- Monitoring and Logging....6
- Data Retention, Disaster Recovery, Business Continuity....6
- Vendor Management....7
- Validation....7

Introduction

We make Fulcrum to help our users improve data quality by giving them a platform optimized for ensuring field data capture is streamlined and error-free. Protecting the data of our customers while it is in our custody is a responsibility we take seriously. Information security can be complex and we are committed to helping our customers understand our approach and the practices we employ to keep their data safe.

Organizational Security

Responsibility for information technology security and security of our cloud infrastructure is segmented between our Information Technology and our Reliability and Release Engineering Teams, respectively.

The engineering team is responsible for designing, implementing, and testing security features within the Fulcrum platform. This includes mitigation of any findings from penetration tests or security assessments.

Fulcrum is audited on a yearly basis by CPA-certified external auditors who issue a SOC 2 report regarding the design and operational effectiveness of internal controls. Fulcrum is also subject to an external Mobile Application Security Assessment (MASA) to validate the security controls of our Android application and a penetration test that targets our Android, iOS, and web applications performed by an external party, on a yearly basis.
Fulcrum officially achieved its ISO/IEC 27001:2022 certification with a cycle start date of October 14, 2026, and an expiration date of October 13, 2029

Artificial Intelligence (AI)

Fulcrum uses AI to enhance its services while still prioritizing customer data privacy. AI usage varies by feature with some features processing customer data only within Fulcrum while others may send customer data to 3rd party AI services for processing. When data is sent to 3rd party AI services, it is done so in accordance with our policies which are based on the NIST Privacy and Artificial Intelligence Risk Management Frameworks. With confidentiality being maintained, only necessary customer data is sent and is not used for model training. As with all our 3rd party data processors, our data sovereignty commitment does not apply and if that is of concern, then it is recommended not to use any features supported by 3rd party AI services. For details regarding which 3rd party providers Fulcrum uses at any given time, see the Fulcrum trust center at https://trust.fulcrumapp.com/.

For more detail on which services, models and data are used for each AI feature, see the "Fulcrum AI Feature Data Sheet" document, also available in the Fulcrum Trust Center.

Data Protection

The goal of Fulcrum's security program is to protect customer data from unauthorized access as it is collected in the field, transmitted to the hosted Fulcrum infrastructure and stored in the Fulcrum database. The approaches below represent the current state of our security efforts, which are being constantly re-evaluated in response to the changing security landscape.

Secure Development Process

The Fulcrum development process is focused on short cycle time by means of Kanban and lean thinking. Our process includes consideration for emergency releases or hotfixes as part of the lifecycle. This enables us to address security issues as part of our normal system development process, based on severity.

As our security team monitors security alerts, such as CERT alerts and MITRE CVEs, and develops findings from our own penetration testing program, they coordinate with the engineering and product management teams to assess the impact of findings and the complexity of mitigations. Remediations are then added to the Fulcrum product roadmap, based on the results of the assessment, with fixes for more severe findings prioritized for faster release.

Encryption

In Transit

All interactions with the Fulcrum service, whether from Fulcrum client applications or from user-developed applications, use the Fulcrum API. All data transmitted between client applications and the Fulcrum API is done using strong encryption protocols. Fulcrum supports the latest recommended secure cipher suites to encrypt all traffic in transit, including the required use of TLS (Transport Layer Security) by all clients.

At Rest

Data at rest in Fulcrum is encrypted using FIPS 140-2 compliant encryption standards (AES-256), which applies to all types of data at rest within Fulcrum — relational databases, file stores, database backups, etc. Fulcrum has implemented appropriate safeguards to protect the creation, storage, retrieval, and destruction of secrets such as encryption keys and service account credentials.

Data Sovereignty

The Fulcrum service currently has four data locality options: United States, Australia, Canada and European Union, with physical protection for the infrastructure that comprises the Fulcrum operating environment. These regions are mutually exclusive and do not share data or information flows between them. Customers must choose a location in which to host their account. Accounts cannot span regions. Each Fulcrum customer's data is hosted in our multi-tenant infrastructure and logically separated from other customers' data. We use a combination of strategies to ensure customer data is protected from failures and returns quickly when requested. All Customer data is stored with managed services from our 3rd party cloud service providers. Each Fulcrum region is composed of two or more infrastructure provider regions which in turn is composed of 3 or more availability zones.

Network Security

Fulcrum segments its cloud-based systems into separate networks to better protect sensitive data. Systems supporting testing and development activities are hosted in a separate network from systems supporting the Fulcrum production infrastructure. All instances within our production environment are immutable.

Network access to the Fulcrum production environment from open, public networks is restricted. Only those network protocols essential for delivery of the Fulcrum service to its users are open at our perimeter and there are mitigations against distributed denial of service (DDoS) attacks deployed at the network perimeter. Additionally, Fulcrum logs all network and cloud API calls and uses a third-party CNAPP (Cloud-Native Application Protection Platform) to provide monitoring and alerting for behaviors that indicate a potential intrusion.

Endpoint Security

All workstations issued to Fulcrum personnel are configured to comply with our standards for security. All workstations are configured, updated, tracked, and monitored by Fulcrum via a mobile device management (MDM) solution. Workstations use up-to-date monitoring tools to detect potential malware and unauthorized software. These tools include MDM policies and macOS-native tools such as Xprotect and Gatekeeper. Company-owned mobile devices are automatically enrolled in our mobile device management system.

Access Control

Least Privilege

To minimize the risk of data exposure, Fulcrum adheres to the principle of least privilege and role-based permissions when provisioning access—workers are only authorized to access data that they reasonably must handle in order to fulfill their current job responsibilities. All production access is reviewed at least quarterly. Staff are provisioned onto corporate systems using a third-party Identity Provider to manage single sign-on (SSO) and are granted access only to applications and data needed for their role.

Authentication

To further reduce the risk of unauthorized access to data, Fulcrum employs layered authentication for all access to our production environment that houses customer data.
All access is controlled through the Fulcrum SSO system, including multi-factor authentication (MFA). In order to gain access to Fulcrum production resources the employee must first be assigned appropriate permissions with approvals.

Monitoring and Logging

Account-level audit logging is available to all Fulcrum account holders and can be accessed via the Fulcrum API for manual or automated analysis. Additionally, all Fulcrum API calls are logged across the entire Fulcrum application. Fulcrum systems and databases have system logging enabled, to capture administrative access, privileged commands, and system calls. Logs are retained for 14 days and stored separately from production systems and backups. Logs are accessible by administrative staff only for manual and automated analysis.

Data Retention, Disaster Recovery, Business Continuity

All customer-collected data, including full record histories are retained within a customer's Fulcrum account for the life of the subscription, unless the data is deleted by the customer. Fulcrum databases are fully backed up nightly, with backups retained for 90 days. These backups are also available off site should our primary data centers become unavailable. In addition each Fulcrum database also contains a standby (reader) instance which is kept in sync (in near real time) and is serving traffic, so in the event of a failure the standby is immediately promoted to the writer and a new reader instance is created and all data synced. Additionally, a second data center, in the same data compliance region is also kept in sync using the same methods and is available to take over should the primary data center become unavailable.

Data collected via Fulcrum mobile applications on customer-owned mobile devices exists only on those mobile devices until it is synchronized with the Fulcrum production system. If data is deleted prior to synchronization, or if the mobile device is corrupted, destroyed, or otherwise rendered inoperable, unsynchronized data cannot be recovered.

The Fulcrum warm stand-by is housed in a separate region to provide sufficient isolation in the event of the unavailability of the primary cloud infrastructure. Technical staff are geographically dispersed across timezones to ensure coverage in the event of a natural disaster or other event.

Vendor Management

With the exception of the native mobile applications, the Fulcrum production system is deployed within top-tier public cloud providers.

Validation

Fulcrum has annual penetration tests of the company's public-facing systems housed in Amazon Web Services (AWS) performed by an outside security vendor. This testing follows the industry-standard Penetration Testing Execution Standard (PTES) found at http://www.pentest-standard.org/index.php/Reporting. This process includes:

1. Passive information gathering to enumerate all public websites belonging to Fulcrum and mirror their contents locally for examination.
2. Analysis of the Fulcrum Android application to discover application programming interface (API) endpoints.
3. Port scanning Fulcrum assets hosted at AWS to determine open ports and operating system/application versions.
4. Scanning these assets using Nessus/OpenVAS to determine any existing vulnerabilities.
5. Active attempts at exploitation using the standard Metasploit framework.

The findings of each test are reviewed with the Fulcrum product management and addressed the development lifecycle, based on severity.

Legal & Regulatory Register

Requirement / Law	Region/ Scope	Impact on Fulcrum	Owner	Status/ Last Review
GDPR	EU Customer Data	Data privacy, DSRs, encryption	CISO/ Legal	Ongoing Operations
ISO 27001:2022	Fulcrum Application	ISMS Framework & Controls	CISO	Original Cycle Start Date: October 14, 2026 Original Cycle Expiration Date: October 13, 2029
CCPA/CPRA	California, USA	Consumer privacy rights	CISO	Quarterly Review Pending
SOC2 Type II	Fulcrum Application	Assurance of operational effectiveness of controls	CISO	10/7/2025
Mobile Application Profile (MAP)	Fulcrum Android Application	Unlocks the "Independent Security Review" badge on Google Play as a verification of third-party validation against industry-standard security benchmarks.	CISO	Previous certification expired 6/11/2026. Next scan starts on 4/29/2027
DPF Data Privacy Framework	Fulcrum Application	Expresses Fulcrum's commitment to a rigorous set of privacy principles.	COO	2/1/2026