



Security & Trust

Fuel50 is committed to ensuring it puts the security of its global clients first. From our robust and best-in-class security management and data handling, to our infrastructure and privacy policies, Fuel50 is a company and solution you can trust.

Security

Security Framework

Fuel50 is an HR system provider and as such receives, stores and processes Personally Identifiable Information (PII) and other client data as part of its platform services.

Fuel50 Software as a Service (SaaS) operates in a secure data center. The following document describes the technical and security measures implemented by Fuel50 for secure handling of clients' data.

The Fuel50 Security & Privacy team manages a robust Information Security & Privacy Management System (ISPMS), which is implemented based on the following industry standards:

ISO 27001:2013	Information technology – Security techniques – Information security management systems – Requirements
ISO 27017:2015	Information technology – Security techniques – Code of practice for information security controls
ISO 27701:2019	Information technology – Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines
ISO 22301:2019	Information technology – Security and resilience – Business continuity management systems – Requirements

Fuel50 has successfully completed a SOC 2 Type II examination for infrastructure and operations of our platform.

Our security framework includes:

- Policies, procedures and controls
- Asset management
- Risk management
- Access management
- Organizational security
- Physical security
- Cryptography
- Operations security
- Supplier security
- Business continuity
- Compliance

Security and Privacy is the responsibility of all Fuel50 personnel. The entire team is regularly trained, and our systems and processes are audited at planned intervals. The Global Security & Privacy Manager defines and maintain the security portfolio up-to-date. The ISPMS Steering Committee reviews the entire program and controls on a regular basis during the Management Review Meetings.

Organizational Security

Each employee goes through a comprehensive security training, and awareness campaigns and meetings happen regularly.

Background Check

Prior to employment, potential candidates undergo interviews for suitability into the vacant role and a full spectrum background check. Upon employment, the candidate must read, sign, and adhere to a series of documents outlining their responsibilities for information security.

Termination of Employment

Terminated employees are removed from all systems. All access to management systems, hardware, tools and SaaS platform is revoked immediately. All assets must be returned to the company.

Acceptable Use Policy (AUP)

Fuel50 AUP is a set of rules that must be followed by all Fuel50 employees. The document focuses on the handling procedures of any asset - including data, hardware, and information systems (software) - to produce security-conscious operations for minimizing risk to people, processes, technology, and environments.

Security Awareness

An information security competence and awareness program is in place so employees can perform their functions in a secure manner.

Endpoint Security

All workstations at Fuel50 are configured to comply with our standards for security. These standards require all workstations to be properly configured and updated, and to be tracked and monitored by a secure endpoint management solution.

Access Control

Users are only provided with access to the network, systems, applications, and network services that they have been specifically authorized to use. Access to the system is audited, logged, and verified.

To further reduce the risk of unauthorized access to data, a Fuel50 Access Control model is based on Role Based Access Control (RBAC) to create separation of state. There is continuous monitoring at the application and infrastructure level with all monitoring data sent to a Security Information and Event Management (SIEM) system. Principles of least privilege are enforced.

Fuel50 employs multi-factor authentication for all access to systems with client

data. Whenever possible, Fuel50 uses private keys for authentication, in addition to the multi-factor authentication on a separate device. Clients can also use Federated Access Control; Fuel50 uses Security Assertion Markup Language (SAML) version 2.0 protocol for Identity Provider (IDP) Single Sign-On (SSO).

All employees are required to use an approved password manager. Password managers generate, store, and enter unique and complex passwords to avoid password reuse, phishing, and other password-related risks. To manage access to these accounts, Fuel50 uses 1Password for authentication.

Monitoring & Logging

Fuel50 access control and continuous monitoring logs all database access and ships the logs to a centralized SIEM system. Administrative access, use of privileged commands, and system calls on all servers are logged and retained.

Log information is protected against tampering and unauthorized access. System administrator and system operator activities are logged, and access/change actions can be reviewed.

Malware Protection

Servers and endpoint devices such as laptops and desktops are protected and monitored from malwares, malicious and unsafe codes or applications by deploying a set of protection tools.

Physical Security

Access to the office, data centers, and work area containing sensitive information will be physically restricted to limit access to only authorized personnel. Employees use fob cards for entering the offices and maintain a visitor log. There are surveillance cameras and security in place to monitor the building.

Supplier Management

Fuel50 uses third-party sub-processors to provide its services. Prior to engaging any third-party sub-processor, Fuel50 Security & Privacy Team performs diligence to evaluate their privacy, security, and confidentiality practices, and executes a non-disclosure agreement implementing its applicable confidentiality obligations.

The assessment process is repeated annually.

Vulnerability & Penetration Testing

Fuel50 engages independent vendors to conduct application and infrastructure-level vulnerability scanning and penetration testing on the SaaS platform. All findings are logged into a database, risks are identified, assessed, and treated until residual risk comes down to the lowest acceptable level. Executive summary reports of vulnerability scans are available to users upon request.

Data Handling

Client Data Protection

Data as an asset (Classification and Handling)

At Fuel50, data is treated as a valuable asset. Information assets of the organization will be classified based on their relative business value, legal requirements and impact due to loss of confidentiality, availability and integrity of the information asset. The level of security will be identified based on the information classification performed.

Customer data is classified at the highest level.

Data Encryption

- Data in Transit: Fuel50' cryptographic controls use Hyper-Text Transfer Protocol Secure (HTTPS) over Transport Layer Security (TLS) version 1.2
- Data at Rest: Fuel50 uses Data at Rest Encryption using Key Management Service (KMS). All data is encrypted using 256-bit Advanced Encryption Standard (AES-256), with each encryption key itself encrypted with a regularly rotated set of master keys.

Data Anonymization/Deletion

Customer data is stored for as long as it is needed to meet Fuel50 operational needs, together with contractual legal and regulatory requirements. Data is retained for the duration of the contract or unless indicated within the Contract/Master Service Agreement (MSA).

Fuel50 will anonymize customer PII after a period of 90 days of the termination of contracts, however, upon expiration of the applicable retention period and when expressly required by a customer, we will securely destroy the data in accordance with applicable laws and regulations.

Compliance

Fuel50 complies with applicable legal, regulatory and contract requirements as well as industry best practices. There is a comprehensive Privacy Program in place and annual audits are performed against regulatory requirements.

Cryptographic controls are used in compliance with all relevant agreements, laws, and regulations. Regular technical compliance reviews, including penetration testing and IT health checks of all information systems, are taken to ensure continued compliance.

Risk Management

Fuel50 has a Risk Management Procedure in place to identify, assess and treat risks depending on the level of impact and likelihood. After treatment, all risks are re-assessed for residual risk evaluation. Risks are only accepted when they reach the lowest level and no longer represent threats to Fuel50 system and data assets.

Incident Management

Fuel50 has an established procedure for responding to potential security incidents. All security incidents are managed by following the non-conformity treatment process:

- Immediate action
- Root-cause analysis and incident classification (based on severity)
- Corrective action

All processes are documented and updated annually. Lessons learned are kept for future reference. In the event of an incident, affected customers will be informed by our Client Success Team and Security department when necessary.

Business Continuity and Disaster Recovery

Continuity management is a risk based approach to managing risks/issues that can cause interruption/disruption to business operations or service delivery operations. Fuel50 manages these risks by determining the most common causes of interruption/disruption and have prepared plans for treatment of these issues.

Within Fuel50, the specific roles are identified in relation to continuity management endeavours. Each role has a defined responsibility.

Fuel50 Business continuity plans are effectively implemented by:

- Having all stakeholders briefed on the contents of the BCP and aware of their individual responsibilities;
- Cloud platforms to be tested and audit results discussed during Management Meetings; and,
- Failover tests updated annually.

Datacenter Disaster Recovery Process

Fuel50 instances reside in two regions (North America and Europe) utilizing its Availability Zones to provide fault tolerance and redundancy at the data center level of operations. Each region utilises its own Database and client data is backed up within the same region.

Recovery Time Objective & Recovery Point Objective

Fuel50 Recovery Time Objective is committed to the Service Level Agreements. Services delivered from CorpIT to internal-facing employees must be recovered within 24 hours. Services delivered from cloud-based software to external-facing clients must be recovered within 7 hours.

Fuel50 Recovery Point Objective (RPO) is dependent on multiple factors and when delivered from Saas: deliveries to external-facing clients must be recovered to a point within 24 hours. The 24-hour value is based on conducting backups of the supplied client data within each data center.

NOTE: Client-provided data is not backed up to removable media or removed from the data centers for backup purposes.

Fuel50 GDPR Strategy

Fuel50 SaaS is fully compliant to GDPR requirements and the organisation has crafted a strategy for aligning with the European Union (EU) General Data Protection Regulation (GDPR) requirements, including but not limited to engaging the EU Representative, conducting annual revision to its DPIA (Data Privacy Impact Assessment), administrative controls for rights management, Breach reporting, DPA (Data Processing Agreement), etc. and technical controls for Data Protection in transit and at rest.

Based on the GDPR principles, Fuel50 provides the following information to show its compliance.

1. Lawfulness, fairness and transparency

Lawfulness: All information is collected and processed lawfully based on contractual requirements.

Fairness: Fuel50 only process data according to the documented policies and procedures.

There is no undocumented collection, use or disclosure of client data that.

Transparency: We keep the Security White Paper as a means to be transparent with our clients in terms of how our data practices are being carried. Fuel50 only access client data and client instances when they have been explicitly permitted to do so by the client in order to address client requests (e.g. troubleshooting) and for support purposes, there is no casual data access.

2. Purpose limitation

Client data collected by Fuel50 is for specified, explicit and legitimate purposes, which depends on client's Business and Use case. All client provided data is used for service delivery as per contracted terms and agreements.

3. Data minimization

Fuel50 has minimum data requirements: First Name, Last Name, and Email Address. Any further information provided by clients are up to the complete discretion of the client and to support their Business Case and Use Case toward the use of Fuel50.

4. Accuracy

Fuel50 provides all clients with complete control over their own data. All clients have a Web Based User Interface (WebUI) access to Fuel50 SaaS for control and data entry, deletion and modification. Fuel50 has no control over the accuracy of client data inputted into the system.

5. Storage limitations

Fuel50 data retention period is governed by the contractual agreement with the client.

6. Integrity and confidentiality

Fuel50 makes sure that client personal data is processed in a manner that ensures industry-standard security of personal data. Fuel50 protects client data against unauthorized or unlawful processing and against accidental loss, destruction or damage.

Fuel50 does not 'share' or 'sell' any data. All client provided data is used for service delivery as per contracted terms and agreements. Any data transferred to suppliers is done so as a part of Fuel50 service delivery. Suppliers are bound by contractual agreements to process data for Fuel50 only for Fuel50 business needs.

7. Accountability

Fuel50 is responsible for Personal Information under its control and has a designated Global Security & Privacy Manager acting as Data Protection Officer (DPO) who is accountable for Fuel50 compliance with this Privacy Code of Conduct. Fuel50 uses an Access Control Process overlaid with Role Based Access Control (RBAC) for separation of duties and segregation of roles. Upon request, Fuel50 provides specific and understandable information about its policies and practices.