

Key Survey
Security Fact Sheet



Key Survey

Security Fact Sheet

This document is applicable to Key Survey - the official trademark of WorldAPP, Inc, hereinafter “the Company”.

Certifications

As a data collection platform Key Survey has always had “security” and “privacy” of data at the forefront of its values. To demonstrate an ongoing commitment to this Key Survey has obtained ISO/IEC 27001 & 27701 accreditations.

Our compliance has been audited and certified by Bureau Veritas, an independent and accredited certifying body.

Hosting & Infrastructure

The Key Survey platform is a cloud solution hosted in public cloud infrastructure of Google Cloud Platform (GCP).

Key Survey makes use of multiple availability zones within our primary GCP region - us-east5 (Columbus) - to ensure secure and resilient operations. Backups for data and applications are stored in the us-east1 (Iowa) region, which guarantees secure and uninterrupted service in the event of regional outages.

Google Cloud Platform supports numerous security standards and compliance certifications, including ISO27001, SOC 1 & 2, PCI-DSS, HIPAA, FedRAMP, GDPR, FIPS 140-2, and NIST 800-171.

Third-Party Cyber Risk Assessment

FORM has completed CyberGRX third-party validated cyber risk assessment to have our controls and overall security posture independently evaluated leveraging CyberGRX’s sophisticated assessment methodology.



This assessment replaces the outdated static spreadsheets and presents a dynamic and comprehensive approach to third-party risk assessment. The CyberGRX utilizes response analysis, threat intelligence and independent evidence validation to provide customers with a holistic view of their third-party cyber risk posture.

To request Key Survey's CyberGRX assessment report, email us at se@form.com.

Authentication & Access Management

Access provisioning is performed on a need-to-know basis and following the principle of least privilege.

Customer data resides securely on database servers behind multiple firewalls.

Customers are able to limit access for support team to their Key Survey accounts by time or completely close the access.

All authentication activity is logged.

Data Security & Backups

Customers have full access to their data during the contract time and can delete the data from the production database at any point.

The Company provides a multi-tenant solution where customer data is segregated using unique user IDs.

All traffic to and from the Key Survey platform is encrypted in transit using TLS v1.2 or better with modern cipher suites.

All data is encrypted at rest by using AES-256, block-level storage encryption.

Backups at Key Survey are cloud-stored in GCP's infrastructure within the United States. The backup process ensures secure, access-controlled, and redundant storage of each component - from instance images to databases.



Application Security

Key Survey leverages agile development best practices, including test-driven development, pair programming, and code reviews.

Application code is regularly evaluated for vulnerabilities by the means of Static Code Analysis Tooling (SAST) as part of the Continuous Integration (CI) pipeline.

Applications are deployed and operated in next-generation infrastructure utilizing Kubernetes (k8s), which allows for application-level network isolation and configuration.

External penetration tests are performed annually by an accredited third-party.

Threat modeling is incorporated into our SDLC to ensure that security requirements are integrated into the development process from the outset.

Key Survey adheres to the best practices and guidelines provided by OWASP to enhance application security.

System Stability, Assessment & Monitoring

All our systems are monitored for performance, security, traffic, and other parameters on a 24/7 basis using various automated monitoring and alerting tools.

Our clients are contractually guaranteed 99% uptime.

Privacy Compliance

The Company has developed and implemented a privacy program that is necessary and appropriate to meet its obligations under applicable state and federal laws, including but not limited to: General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), CPRA, Virginia Consumer Data Protection Act, Utah Consumer Privacy Act, Colorado Privacy Act, Connecticut Data Privacy Act and other state privacy laws, UK Data Protection Act 2018, UK GDPR, Health Insurance Portability and Accountability Act (HIPAA), Gramm Leach Bliley Act (GLBA) and Massachusetts Regulation 201 CMR 17.00 (MA Reg)



Key Survey passes annual checks by TrustArc as part of the Company's TRUSTe's Privacy Seal certification, signifying that our privacy statement and practices have been reviewed for compliance with the TRUSTe program.

Employees undergo criminal background checks and reference checks as permitted by the applicable law.

The Company has implemented the required processes to ensure the Key Survey platform is in compliance with the GDPR:

- We incorporated the data protection clauses of the GDPR into our contract templates.
- We implemented strong technical and organizational measures for data protection during transfers.
- We are an active participant of the EU-U.S. Data Privacy Framework.
- We provide our customers with safe and legitimate means for personal data transfer.
- We refreshed our Privacy Policy to establish the necessary changes implemented by the GDPR and UK GDPR.
- We created policies and procedures to adequately address and limit, to the maximum extent possible, public authorities' ability to request or access the personal data.
- It is our policy not to create any programming or technology that would allow third parties, including authorities, to access our systems or personal data stored on those systems.
- We developed policies and procedures to address data subjects' requests.
- We keep the data processing records required by the GDPR and UK GDPR.
- We appointed a Data Protection Officer to ensure well-defined data protection control.
- We have offices in UK and EU for fast assistance in data protection matters.
- We conduct GDPR compliance training for the individuals who are authorized to process personal data within the Company.
- We have a well-established mechanism of regular policies review to guarantee compliance with the data protection legislation.
- The processes within the Company allow us to restore data availability and access in a timely manner.
- We are constantly implementing additional technical and administrative measures to secure personal data.

