workable

Security at Workable

Workable helps companies find and hire great people — and protects the data you collect and create along the way. Applying a combination of industry standards and our own ever-evolving best practices, our robust and rigorous controls ensure your organizational and candidate data is kept safe. We focus on security, so you can focus on finding the best person for the job.

We understand and appreciate that candidates must be able to trust you with their data. And that you must trust the tools and technology you use with yours. That's why we take information security seriously and aim to be clear and transparent about the measures and approaches we use. Keep reading to learn more.

Security culture

Awareness

At Workable, we believe every employee plays an important role in maintaining security — and that it's our responsibility to provide them with the knowledge and tools they need to do so. That's why, starting from onboarding and continuing through their time with Workable, we strengthen employees' security prowess with regular security training, phishing campaigns, technical events, Q&A sessions and more.

Additionally, all employees are required to sign and follow our comprehensive Acceptable Use policy, which depicts our Information Security Management System.

Security team

Workable employs a dedicated, full-time security team to manage and continuously improve our organizational, engineering and compliance security. The team protects Workable, our data and the data of our customers by conducting activities such as red teaming (vulnerability assessments, source code review, penetration tests), blue teaming (monitoring and alerting, infrastructure hardening), and governance and compliance (internal audits, risk assessments, business continuity plan).

Data encryption

Workable data is encrypted in transit using security best practices (i.e. HSTS) and the latest recommended secure cipher suites and protocols whenever supported by clients. All personally identifying information (PII) is encrypted at rest while passwords are stored using irreversible encryption (hash function + salt) to ensure their confidentiality. Appropriate safeguards have been implemented to protect the creation, storage, retrieval, and destruction of secrets. We implement best practices as they evolve and respond promptly to cryptographic weaknesses as they're discovered.

Application, systems and network security

In addition to the security components provided by our top-level cloud providers (Google and AWS), Workable maintains its own dedicated controls by leveraging key industry security vendors and open source projects. These controls cover the entire TCP/IP stack, including DNSSEC, DDoS protection and a dedicated web application firewall, as well as network firewall fine grained rules configured according to the highest industry standards.

WAF

Our dedicated web application firewall acts as a strong barrier to protect Workable application and microservices. It enforces security controls such as hardened TLS configuration (HSTS, strong encryption and hashing algorithms), strong authentication mechanisms (preventing password guessing attacks), overall protection against malicious activity (bad IP reputation detection, browser integrity checks, WAF rules, etc.) and specific rate limiting rules.

Authentication

Workable provides an additional level of security during application authentication by offering single sign-on (SSO) which integrates with services that support Security Assertion Markup Language (SAML).

Availability and disaster recovery

To ensure Workable is available when you need it (we guarantee an uptime of 99.8%), our infrastructure and data are stored redundantly in multiple locations in our hosting and data storage providers. In the unlikely event of a major disaster, our Business Continuity Plan (BCP) guarantees a smooth and organized transition towards a full recovery.

Logging and monitoring

We maintain an extensive, centralized logging environment in our production environment. It contains information pertaining to security, monitoring, availability, and access, as well as other metrics about our application ecosystem and its microservices.

These logs are analyzed for security events and abnormalities via logical and technical controls. Further, alerts and monitors automatically notify the appropriate internal teams to ensure visibility and responsiveness.

Incident response

Workable's incident management policy and procedures are designed to quickly and effectively handle any disruption to our data availability, integrity or confidentiality. Should a situation arise, we'll notify the affected customers and any applicable regulator according to our privacy policy.

Security assessments

3rd-party audits

We've been working with private bug bounty programs since the very beginning to ensure continuous independent penetration testing of our application and microservices. On top of that, Workable invests in technical security assessments (web application penetration testing, manual source code review, configuration audit, etc.) performed by 3rd-party security experts to bring context, expertise and in-depth testing together in one place and achieve an overall stronger security level.

Internal red teaming activities

In parallel with 3rd-party audits, our security team performs red teaming activities such as web application penetration tests, system/network vulnerability assessments and static code reviews on a regular basis. The outcomes are evaluated and action plans are dispatched across affected teams in order to mitigate all potential vulnerabilities according to their severity.

Compliance

ISO 27001

Workable is ISO 27001:2013 certified, which means we meet the highest worldwide security standards. In other words, we have powerful processes and policies in place to ensure the confidentiality, integrity and availability of our data. An external audit is performed every six months by a qualified 3rd party to assess our organizational compliance and information security risk.

View our ISO certificate, or request a detailed scope of applicability (SoA), including our documentation framework summary per control, from your account manager.

VIEW ISO CERTIFICATE

GDPR

Workable provides features which enable customers who collect and process EU data to maintain GDPR compliance, and is itself GDPR compliant. However, it is our customers' responsibility to comply with GDPR requirements from the perspective of a 'Data controller'. Read more in our Privacy policy.

CCPA

Workable is compliant with the California Consumer Privacy Act of 2018 (CCPA). However, it is our customers responsibility to comply with CCPA requirements from the perspective of a "Business". Read more in our Privacy policy.

EU-U.S. Privacy Shield

Workable complies with the EU-U.S. Privacy Shield Framework and Swiss-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use and retention of personal information transferred from the European Union and Switzerland to the United States.

3rd-party data centers and services

The environment that hosts our services (Google and AWS) maintains multiple certifications for its data centers, including SOC 1 and SOC 2/SSAE 16/ISAE 3402, PCI Level 1, FISMA Moderate, and Sarbanes-Oxley (SOX). Learn more: AWS, Google.