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 our measures and approaches.

Security culture

Awareness

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 we constantly strengthen employees' security prowess through regular security training, hands-on sessions, internal phishing campaigns and security Q&A events.

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 security. The team protects Workable's infrastructure, network and data (including the data of our customers) in three ways:

- **Assess:** Perform security audits and simulate malicious behavior in order to evaluate our security posture and identify areas for improvement
- **Defend:** Implement and maintain controls in order to prevent and mitigate threats
- **Comply:** Create policies and procedures in order to establish a high and consistent security level across the organization's Information Security Management System

Product Security

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

Web Application Firewall

Our dedicated web application firewall acts as a strong barrier to protect Workable's application and microservices. It enforces security controls such as hardened TLS configuration (HSTS, strong encryption and hashing algorithms), overall protection against malicious activity (bad IP reputation detection, browser integrity checks, WAF rules) and multiple rate-limiting rules that prevent automated form submission on critical endpoints (password guessing attacks).

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 2.0).

Data encryption

Workable data is encrypted in transit using security best practices and the latest recommended secure cipher suites and protocols, whenever supported by clients. All data is also 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.

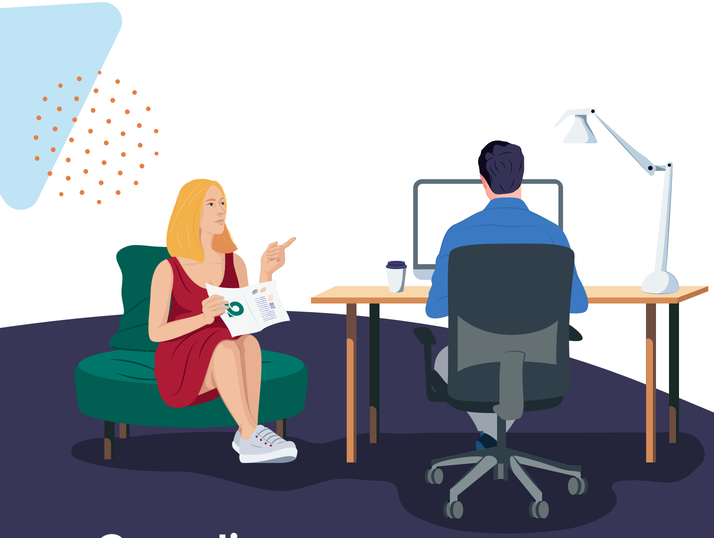
Logging and monitoring

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 appropriate internal teams 24/7/365 to ensure visibility and responsiveness.

Incident response

Workable’s incident management policy and procedures are designed to quickly and effectively handle any event which may impact our data availability, integrity or confidentiality. Should a situation arise, we notify affected customers and any applicable regulator according to our privacy policy.



Availability and disaster recovery

To ensure Workable is available when you need it, our infrastructure is hosted in a multi-zone architecture and its critical data storage has an independent synchronous replica in a different availability zone. Automatic backups are performed at regular intervals. The backup frequency depends on the data types and occurs hourly, daily, weekly and monthly.

In the unlikely event of a major disaster, our Business Continuity Plan (BCP) guarantees a smooth and organized transition towards a full recovery (ISO 27001, ISO 27017 and SOC 2 requirement).

Up-time

We guarantee 99.8% uptime, excluding scheduled maintenance. You can find live information here: https://status.workable.com

Security assessments

We work with private bug bounty programs to get continuous independent security feedback on our application and microservices. We also invest in technical security assessments performed by 3rd-party experts (penetration tests, source code review, vulnerability assessments) to bring context, expertise and in-depth testing together in one place. Our security team also performs its own security testing on a regular basis.

Vulnerability management

After their identification, all security bugs are validated, evaluated, categorized and prioritized based on severity. An action plan is dispatched across the affected teams in order to mitigate all potential vulnerabilities on time.

Compliance

ISO 27001 and ISO 27017

Workable is ISO 27001:2013 and ISO 27017:2015 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.

SOC 2 and SOC 3

Workable holds a SOC 2 Type II and SOC 3 report. This certifies we have designed appropriate controls to provide reasonable assurance that our service commitments and system requirements were achieved based on the AICPA Trust Services Criteria relevant to Security, Availability, and Confidentiality.

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.

3rd-party data centers and service

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.

For more information visit **workable.com/security**