workable

Security at Workable

Workable simplifies HR with a suite of products for recruitment and employee management, protecting 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 recruiting and managing your teams.

Organization

Workable's security program is aligned with ISO 27000 and AICPA Trust Service Principles aiming for in-depth defense: securing your data at every layer.

Team

We employ a dedicated, full-time Security Team to manage and continuously improve our controls and initiatives. The team is responsible for protecting the Workable product, its data and underlying infrastructure by focusing on four pillars:

Assess: perform security audits and simulate malicious behavior to evaluate our security posture and identify areas for improvement

Defend: implement and maintain controls to prevent, detect and mitigate threats

Comply: create policies and procedures to establish a high and consistent security level across the organization's Information Security Management System

Train: empower people's security culture and mindset

Training and awareness

We believe every employee plays an important role in Security - and that it's our responsibility to provide them with the knowledge and tools they need to do so. That's why we strengthen employees' security prowess through regular security training, hands-on sessions, lessons-learned events and internal phishing campaigns.

Acceptable Use Policy

All employees commit to confidentiality obligations to protect Wokable information, they sign our comprehensive Acceptable Use Policy, which depicts the key dos and don'ts, and links their role to our Information Security Management System.

Product

In addition to the security components provided by the top-level cloud providers (Google Cloud Platform and AWS), Workable maintains its 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, but not limited to, DNSSEC, DDoS protection, a dedicated web application firewall, as well as fine-grained network firewall rules configured using the highest industry standards.

Web Application Firewall

Our dedicated web application firewall (Cloudflare) acts as a strong barrier to protect Workable application and its 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 anti-bot capabilities (such as rate-limiting capabilities and a captcha solution).

Authentication

Built-in product mechanisms are in place to prevent password-guessing attacks and enforce strong authentication. Workable provides an additional security level through OAuth flows (Google, Linkedin and Microsoft) and offers single sign-on (SSO) which integrates with services that support Security Assertion Markup Language (SAML 2.0).

Encryption

Workable data is encrypted in transit using security best practices and the latest recommended secure cipher suites and protocols, whenever supported by clients. Data is also encrypted at rest, while passwords are stored using irreversible encryption (hash function + salt) to ensure their confidentiality. To further protect certain types of data (e.g.: employee salary), encryption in-use is implemented within the data stores using unique data keys per customer.

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.

Secure by design

Specific and evolving application security requirements are set for new application features to enforce a consistent level across the product. Automated controls are part of our CI/CD pipelines to detect emerging issues such as code dependency vulnerabilities.

Infrastructure

Production, testing and staging environments are segregated while their resources are fenced at the network level to allow access only to authorized employees through a VPN-like solution.

Access control

Workable adheres to role-based permissions and the principles of least privilege to ensure that only authorized personnel have access to systems and data required by their role. Authentication to production resources requires additional controls such as physical hardware keys and client certificates.

Logging and monitoring

We maintain a powerful and centralized logging of all production resources. 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.

Availability, backups 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 storages have independent synchronous replicas in different availability zones. Automatic backups are performed at regular intervals (hourly, daily, or weekly depending on the data type) to allow the restoration of data within a reasonable point in time.

In the unlikely event of a major disaster, our Business Continuity Plan guarantees a smooth and organized transition toward a full recovery.

Assessments

Security feedback can be reported through our public Vulnerability Disclosure Program.

Technical assessments

On top of internal technical audits, we invest in regular security assessments (such as penetration tests and source code reviews) performed by 3rd-party experts to bring independent context, skills and in-depth testing together in one place. Their scope and type are dynamic and based on the previous quarter company roadmap. We have also been working with private bug bounty programs to get continuous security feedback on our product.

Partners' audits

Product partners - including but not limited to Google, Linkedin, ADP and Zoom - perform scoped technical assessments every year.

Vulnerability management

After their identification, all security bugs are collected in a central platform to be validated, triaged, categorized and then prioritized based on their severity. The action plan is drafted and dispatched to the affected teams to mitigate the associated risks based on our predefined timelines. Fixes are retested by the security team before being deployed to production.

IT

On top of strong authentication configuration - such as short session timeout, password complexity requirements and MFA - context-aware access rules are applied to allow only trusted devices to log in to our Identity Provider service.

All employee laptops are centrally managed - hardened, monitored and updated - to ensure data confidentiality. Where required, a password manager service is used to generate and store unique and complex passwords.

Incident response

Workable's incident management policy and procedures are designed to quickly and effectively handle any event that may impact 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.

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 which certify that we have designed and implemented 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 has taken many steps throughout the years to build its internal compliance and align the product with privacy laws, including the General Data Protection Regulation (GDPR and UK GDPR), and relevant decisions of supervisory authorities. Workable provides features that enable customers who collect and process EU data to maintain GDPR compliance. However, it is our customers' responsibility to comply with GDPR requirements from the perspective of a 'Data controller'. Read about how Workable processes data as a 'Data controller' in our privacy policy.

CCPA

Workable is compliant with the California Consumer Privacy Act of 2018 (CCPA) and the California Privacy Rights Act (CPRA). In addition, we incorporate a CPRA Addendum in our Terms. However, it is our customers' responsibility to comply with CCPA requirements from the perspective of a "Business". Read more in our privacy policy.

Third-party data centers and services

The environment that hosts our services (AWS, Google Cloud) 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).

Third-party vendors

Workable carries out due diligence checks of all third parties that act as sub-processors. We have Data Processing Agreements (DPAs) in place with all sub-processors, including Standard Contractual Clauses for transfers from the European Economic Area to non-EEA countries. In addition, we perform Transfer Impact Assessments before we transfer any data outside the EU/UK.

For more information visit our Security page

Version 3.1, last updated August 2024