Handshake Security & Privacy 2023

At Handshake, data and information security & privacy is of the highest importance for us. In this document, you will find a comprehensive overview and description of the measures we undertake to ensure the integrity and security of the Handshake platform.

Handshake is a leading company that connects students and universities with top employers across the globe. As a company that handles sensitive personal data and information, Handshake has made it a priority to protect their clients' data from any potential security breaches. To achieve this, the company has implemented a number of security measures, including encryption and access controls, to ensure that all client data is kept safe and secure.

Handshake conducts regular security audits to identify and mitigate any potential vulnerabilities in their system. Additionally, the company complies with all relevant data protection regulations, such as the General Data Protection Regulation (GDPR), to ensure that client data is handled in a lawful and ethical manner.

With these measures in place, Handshake provides their clients with the peace of mind that their personal information is secure and protected. Handshake employs fully dedicated security and privacy teams. These teams are constantly focused on ensuring that Handshake leads the industry in data security and privacy as well as building a culture of security at Handshake

Our data security and privacy teams are composed of senior engineering leaders, attorneys with a focus on user privacy best practices, and representatives from the Handshake executive leadership team.

All of our best-in-class security services listed below are included in the Handshake subscription. Handshake is the only career services management platform in the industry that offers all of these at no additional charge.

Platform Security

This section describes the security measures relative to the Handshake platform.

Access Control

Access Control Policy

Access to data within the Handshake platform is governed by tight access controls. Handshake has various permission levels for users (career services, students, employers) that encompass different data access rights.

Handshake's approach for defining access privileges and roles is to provide predefined roles with the appropriate permissions covering the most common use cases and best practices. As such, it is easy to understand for administrators (either career services, employers, or Handshake's staff) who are responsible for giving access privileges to other users. This ensures that the appropriate roles are given to users that fits their needs, enabling them to follow the least-privilege principle.

Secure single sign-on

Handshake supports modern single sign-on (SSO) options, to ensure your students can enjoy safe, simple access to the platform from any secure identity or device. Our authentication process supports the following SSO protocols, among others: SAML, SAML 2.0, Shibboleth, LDAP, CAS, and TFA.

User Access Provisioning and Deprovisioning

The career service and employer interface allows organizers to configure users according to roles they need to attribute to others.Access to administration interfaces are encrypted via industry best-practices HTTPS and TLS1.3.

Handshake administrators handle user registration and de-registration.

Administration Interfaces Access

Cryptography

Data in Transit

Handshake uses modern and industry best practices encryption schemes (HTTPS and TLS1.3) to encrypt data in transit and communications between the platform users (students, employers, career services or Handshake staff). Handshake only supports TLS 1.3 and 1.2 in favor of deprecated protocols like TLS 1.1.

A few communications are sent via email and are inherently less protected. Only public information transits through this method of communication.

Data at Rest

The Google Cloud Platform infrastructure ensures encryption at rest of all data-stores containing non-public information using an industry-standard AES-256 encryption algorithm.

Physical and Environmental Security

Physical Perimeters and Location

Our platform is hosted in Google Cloud Platform (GCP) facilities in the US Data Region. GCP data centers are housed in nondescript facilities. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff.

Physical Access Control

The GCP data center facilities feature a secured perimeter with multi-level security zones, 24/7 manned security, CCTV video surveillance, multi-factor identification, physical locks, and security breach alarms.

GCP only provides data center access and information to employees and contractors who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if they continue to be an employee of Google or Google Cloud Platform. All physical access to data centers by GCP employees is logged and audited routinely.

Protecting Against External and Environmental Threats

Fire Detection and Suppression

Automatic fire detection and suppression equipment have been installed to reduce risk. The fire detection system utilizes smoke detection sensors in all data center environments, mechanical and electrical infrastructure spaces, chiller rooms and generator equipment rooms. These areas are protected by either wet-pipe, double-interlocked pre-action, or gaseous sprinkler systems.

Power

The data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day, and seven days a week. Uninterruptible Power Supply (UPS) units provide back-up power in the event of an electrical failure for critical and essential loads in the facility. Data centers use generators to provide backup power for the entire facility.

Climate and Temperature

Climate control is required to maintain a constant operating temperature for servers and other hardware, which prevents overheating and reduces the possibility of service outages. Data centers are conditioned to maintain atmospheric conditions at optimal levels. Personnel and systems monitor and control temperature and humidity at appropriate levels.

Management

GCP monitors electrical, mechanical, and life support systems and equipment so that any issues are immediately identified. Preventative maintenance is performed to maintain the continued operability of equipment.

Storage Device Decommissioning

When a storage device has reached the end of its useful life, GCP procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. GCP uses the techniques detailed in NIST 800-88 (“Guidelines for Media Sanitization”) as part of the decommissioning process.

Operations Security

Change Management

Handshake's development cycle is based on the scrum framework, specifically Agile. Agile is a project management approach that breaks projects into short, iterative cycles called “sprints”. At its core, Agile is based on the assumption that circumstances change as a project develops. That’s why, in an Agile project, the planning, design, development, and testing cycles are never done. They continue to change as the project takes form. Change management is directly integrated within the process.

Development Process

Handshake maintains an industry leading secure software development lifecycle program. All code is subject to review and approval via the change management process that includes separation of duties and approvals. Code security and dependency checks are performed before every deployment. Furthermore, the access to source code is heavily restricted, and a Version Control tracks all changes to source code.

Technical-operational Measures

Environment Separation

Development, testing and pre-production environments are divided logically from the production environment via Virtual Private Clouds. Production data is never used in lower environments.

Protection from Malware

All endpoints are subject to anti-malware measures including Endpoint Protection via Crowdstrike Falcon and anti-virus software.

Backup

Our backup policy guarantees that platform data on Handshake is replicated in several geographical locations. The replication instances are configured and reliant. Our production databases are backed up and versioned every day. Those backups are kept for seven days. Backups are encrypted at the whole disk level.

Log Management

Logging and Monitoring

Handshake uses application server logs which contain all user actions that prompt an HTTP request to the application (e.g. loading a page, submitting a form, triggering background HTTP requests etc.), as well as some associated data.

These logs include actions performed by administrative accounts.

Logs Protection

Access to the logs is restricted to certain members of the technical team.

Technical Vulnerability Management

Vulnerability Scanning

An automated Web Scanning appliance is deployed on the Handshake platform pre-production. It sends alerts on vulnerabilities found before the platform is deployed. The security team then ensures that the vulnerabilities are prioritized and subsequently corrected. Vulnerability scans are performed quarterly.

Static Code Analysis

We're using an automated service to monitor code quality, reliability and security, automatically detecting bugs, vulnerabilities, code smells and other issues in our codebase.

Penetration Testing

Handshake contracts a leading third-party security firm to perform external penetration tests of different scopes of our platform and applications at least annually.. The full scope of our public-facing products is tested and reviewed at least once a year.

Communications Security

Network Security Organisation

Architecture

Our network security architecture is built upon multiple security zones. Sensitive systems, like database servers, are protected in the most trusted zones, where only traffic coming from the internal network is authorized. Traffic between different zones is filtered using firewalls.

Segregation in Networks

Our GCP infrastructure utilizes several GCP network security features to isolate our infrastructure from external traffic and filter any unauthorized traffic (GCP VPC - Virtual Private Cloud - and Security Groups - virtual stateful firewalls).

Logical Access

Access to the Handshake production infrastructure is restricted to specific members of the Handshake technical team, following the least-privilege principle. By default, members of the technical team do not have access and have to request access during a certain time frame.

Network Monitoring

Network monitoring on our GCP infrastructure is managed through our global infrastructure monitoring. All logs are sent to a centralized logging service for monitoring, analysis, and alerting.

System Acquisition, Development and Maintenance

Secure Development

Secure Development Awareness

Handshake strongly encourages security awareness in its technical team through regular communications and staff awareness programs.

Members of the technical team meet monthly to discuss and share best practices, information and resources, and identify security actions that need to be taken. Security articles and presentations are regularly shared within the team through internal communication channels and regular training sessions.

Secure Development Training

Handshake currently conducts secure code trainings, covering the OWASP Top 10 and other common attack vectors.

Secure Development Environment

Platform development is undertaken on the local developer machines. This system is hosted by Github in private repositories. Github guarantees an appropriate level of confidentiality, availability, integrity and traceability.

System Change Control procedures

Web Frameworks Security Controls

Handshake employs modern web frameworks (e.g. React, Ruby on Rails) and continuously applies security assessments to examine the platform and to tests for known web application vulnerabilities (e.g. OWASP Top 10). These include inherent controls that reduce our exposure to Cross Site Scripting (XSS), Cross Site Request Forgery (CSRF), and SQL Injection (SQLi), among others.

Technical Review of Applications after Platform Changes

Each source code change goes through several reviews:

- code review by two other members of the development team;
- functional review and/or non-regression testing by the product manager or QA engineers.

- Security-sensitive changes will get flagged specifically and go through an additional process of review & testing involving senior technology leaders

Vendor Risk Management and Third Party Security

All third-parties used for the Handshake platform and applications have been vetted and approved by Handshake's security team. All third parties are subject to security and privacy controls at least as strict as those imposed on Handshake by its customers. All vendors are subject to confidentiality agreements.

Information Security Incident Management

Responsibilities and Procedures

Security incident management and crisis management is the responsibility of the security team. A security incident is handled as a production incident, and a task force is assigned to fix the issue. In the event that a security incident requiring notification occurs on the platform, Handshake will notify the competent authorities and its affected clients within a reasonable time frame.

Classification of an incident is done by the task force assigned to the incident. Major decisions are approved by the Vice President of Security & IT. All security incidents are recorded and analyzed by the security department. Action plans can result from this analysis.

Business Continuity

Business Continuity Plan

A Business Continuity Plan (BCP) is in place and can be provided upon request. It is reviewed at least annually.

Handshake's continuity plan depends on the availability guaranteed by GCP: All data centers are online and serving customers; no data center is “cold.” In case of failure, automated processes move customer data traffic away from the affected area. Core applications are deployed in an N+1 configuration, so that should a data center failure occur, there is sufficient capacity to enable traffic to be load-balanced to the remaining sites automatically.

RTO< 24 hours

RPO< 6 hours

Implementing Information Security Continuity

Redundancy

Critical components of the infrastructure, such as web servers, application servers and data-stores are clustered and redundancy ensures availability in case of a system failure. Our backup policy guarantees that our platform data is replicated in several geographical locations. Our replicated instances are set up according to our policy and their reliance is assured by GCP.

Disaster Recovery

Handshake undertakes an infrastructure-as-code approach to infrastructure management, thus enabling a faster recovery in the event of a major disaster necessitating re-building the whole infrastructure.

Disaster Recovery Testing

The configuration for the whole platform and all applications is scripted. In the event of a disaster, the technical team will be able to restore the platform by deploying running configuration scripts. Databases are restored automatically from their snapshots to a point in time between zero and five minutes from the time of the disaster. Configurations are used every day, and they are tested all the time.

Availability of Services

Details of the Handshake SLA can be found in the agreement provided to your institution. Handshake guarantees a 99.9% uptime. A Handshake engineer is on call 24/7 and automated monitoring systems are used to alter the on-call engineer of any site issues automatically.

Users can monitor the performance of the Handshake site as well as subscribe to updates by visiting status.joinhandshake.com

Compliance

Security Compliance

GCP Certifications

Handshake uses Google Cloud Platform (GCP) to host the Handshake application and to manage data storage, system back-ups, server management, and cloud management tools. GCP is an industry leader in data security. You can learn more about the work GCP is doing to ensure protection here:

GCP's infrastructure has been vetted for compliance against industry standards.

GCP is compliant with the following certifications:

- ISO 9001:2015
- ISO 27001
- ISO/IEC 27017
- ISO/IEC 27018
- ISO 22301:2019 & BS EN ISO 22301:2019
- ISO 50001:2018
- ISO/IEC 27110
- ISO/IEC 27701
- SOC 1
- SOC 2
- SOC 3
- GDPR

Our platform benefits from those certifications by being hosted in GCP facilities.