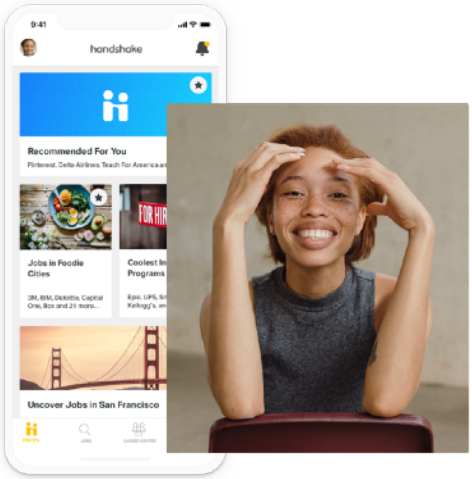


Data Security and Privacy at Handshake

Introduction

Handshake was founded in 2014 with the mission to democratize access to opportunity for every student, regardless of their socioeconomic background, who they know, or where they go to school.

Today, Handshake is the leading career management platform in the United States. Trusted by over 70% of the Nation's top Universities, Handshake provides a platform that connects 700+ Universities, 10M+ students, and 220K+ employers.

Universities career centers trust Handshake to manage back office operations including tracking event attendance, managing on-campus interviews for employers, tracking advising appointments, and more.

Students use Handshake to build a professional profile, manage resumes and covers letters, and to apply to jobs posted by employers through the system. Students can choose to have their Handshake profiles visible to employers - enabling employers to proactively reach out to them with job and internship offers.

Employers use Handshake to manage their college recruiting across over 700 Universities. Handshake is a core part of the recruiting process for over 220,000 organizations globally, including 100% of the Fortune 500.

A Culture of Security

At Handshake a culture of security is created throughout the organization. An emphasis on security is embedded throughout our hiring and on-boarding processes and re-enforced through frequent company-wide trainings.

Employee Background Checks

Before they join Handshake, our team verifies an individual's education and previous employment, and perform internal and external reference checks. Where local labor law or statutory regulations permit, Handshake may also conduct criminal, credit, immigration, and security checks. The extent of these background checks is dependent on the desired position.

Dedicated Security and Privacy Teams

Handshake employs dedicated security and privacy teams. These teams are constantly focused on ensuring 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 comprised of senior engineering leaders, attorneys with a focus on user privacy best practices, and representatives from the Handshake executive leadership team.

Ongoing Team Training

All new Handshake employees must go through security training as a early part of the on-boarding process. During on-boarding employees set up key security safeguards such as two-factor authentication on all sensitive systems. As a part of on boarding all team members also go through detailed FERPA training.

Handshake's Security and Privacy team also lead company wide refresher trainings throughout the year. These trainings are often times combined with security tests - including vulnerability test for things like spear-phishing attacks.

Compliance

FERPA

Handshake is designed to enable complete FERPA compliance. When a University launches Handshake the career center, in partnership with the IT organization on campus, upload FERPA protected information to Handshake. This data is used by the career center for purposes of tracking engagement, maintaining counseling notes, and other key functions allowed by the system. This data transfer is permitted by FERPA under the service provider exception.

When a student logs in to Handshake they "claim their account" and are in full control over how their information is shared with third parties on the system (employers. The Handshake agreement defines this transition as a "Claimed Account".

Handshake's opt-in process is designed to ensure students are in full control of their information at all times. No student information is visible to others on the system unless that student has explicitly opted to share that data. These decisions are reportable for purposes of compliance.

Handshake has been vetted by Universities across the country and found to be 100% inline with the FERPA legislation. Handshake retains FERPA experts and incorporates FERPA training into the employee on-boarding process.

GDPR

Europe's new General Data Protection Regulation (GDPR) is one of the most comprehensive and important changes in data privacy regulation in recent years. Handshake has made updates to further strengthen our commitment to Student privacy and to ensure compliance with GDPR.

Handshake will be fully compliant with GDPR by its effective date of May 25, 2018. As outlined in the GDPR legislation, Handshake is defined as a “Data Processor” and the University the “Data Controller”.

Handshake has a draft “Data Processing Agreement” on file for all third party technologies employed in the Handshake platform and has a draft agreement on file for use by Universities. DPAs can be requested by emailing Handshake’s privacy team at privacy@joinhandshake.com.

Handshake’s product and security teams have continue their commitment to ensure GDPR’s best practices for informed consent are incorporated into the Handshake product.

Handshake allows Universities to sync in the GDPR protections status of students using the “‘eu-gdpr-subject’” flag in the data sync.

Security Architecture

Handshake is built atop industry leading cloud infrastructure. Our development team incorporates test for known security vulnerabilities into each build. Quarterly third party scans ensure Handshake is safe and secure.

Handshake Security Standards

All data stored and processed through the Handshake platform is:

- ☑ Encrypted in transmission using TLS 1.1 or above
- ☑ Encrypted at rest using AES 128 or above
- ☑ Stored in the United States

Cloud Infrastructure

Handshake uses Google Cloud to host the Handshake application.

Google Cloud

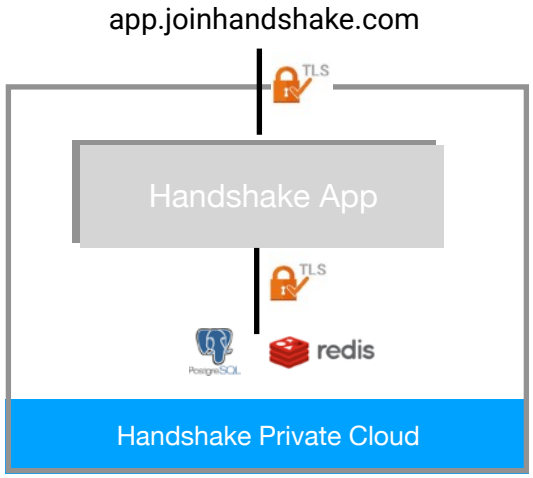
Handshake uses Google cloud to manage data storage, system back-ups, server management, and cloud management tools.

Google cloud is an industry leader in data security. You can learn more about the work Google is doing to ensure protection here: https://cloud.google.com/security/

Google’s infrastructure has been vetted for compliance against industry standards. Specifically, Google’s infrastructure has been vetted under:

✓ ISO 27001	✓ SOC 2	✓ CSA STAR	✓ ISE
✓ ISO 27017	✓ SOC 3	✓ FedRAMP	✓ MPAA
✓ ISO 27018	✓ PCI DSS	✓ COPPA	✓ NIST 800-53
✓ SOC 1	✓ HIPPA	✓ FERPA	✓ SOX

Architecture Diagram



Security in the Development Process

Every build of Handshake is tested for security vulnerabilities. Tests include checks against: SQL Injections, cross-site request forgery, session vulnerabilities, cross site scripting, file access, authentication, and many other potential security concerns. Each change to the Handshake codebase is peer reviewed by a qualified engineer.

Handshake continuously uses security assessments to examine the platform and tests for known web application vulnerabilities (e.g. OWASP Top 10).

Third Party Audits

Handshake partners with third party agencies to verify the security of the Handshake platform.

External scans are done of the Handshake system quarterly through Trustwave. In the event that any vulnerabilities are discovered they are prioritized by our security team and addressed in accordance with their severity.

Handshake contacts with a third party security firm to do a full penetration test of the Handshake system annually.

Financial Security and PCI Compliance

Handshake does not handle, process, store, or transmit sensitive financial data through Handshake servers.

Handshake offers integration to third party credit card processors that can be used by the University for the purposes of collecting payments for career fairs, events, and interview schedules. Currently supported third parties include: Stripe, CashNet, and TouchNet.

Handshake maintains applicable PCI compliance as a merchant. Handshake runs quarterly scans for security compliance and uses a fully PCI compliant infrastructure stack. An AOC can be provided upon request.

Data Ownership

Data ownership and protections for University data are addressed in depth in the Handshake agreement, the Handshake Terms of Service (linked here), and the Handshake Privacy Policy (linked here).

Universities retain full ownership to University Data. Upon contract termination, this data is returned to the University in a mutually agreeable format and deleted from Handshake servers.

Reliability and Uptime

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

Conclusion

Handshake prides itself on security and operational excellence. We're proud to lead the industry in data security and privacy and are committed to protecting University information.