2016 - 2017 Security Overview

Background

Handshake, a leading career management platform headquartered in San Fransisco, securely powers career centers at over 180 institutions including Stanford, Princeton, University of California Berkeley, Princeton, and the University of Michigan. Handshake powers campus recruiting at over 80% of the Fortune 500.

This document is for universities considering the deploying Handshake on campus and is designed to outline Handshake's security practices. Handshake has been thoroughly vetted by the nation's top institutions and independent security firms.

Amazon

128bit SSL

Encryption at rest

Data stored in US

PCI Compliant

Security by Design

Handshake's entire platform was built with security in mind. From server to end user Handshake uses industry standard security practices.

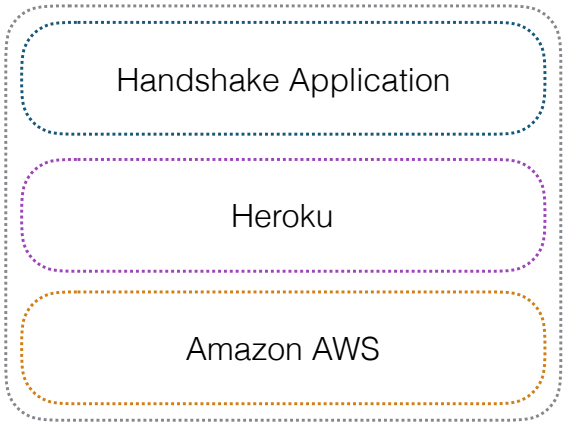
Handshake is built atop Amazon's secure AWS infrastructure. AWS is trusted by companies around the globe ranging from Netflix to the United States Government.

All data in Handshake is encrypted at rest using AES encryption and in transmission using 128bit TLS.

Handshake only uses data centers located in the United States. No University data is ever stored abroad.

FERPA and Handshake

Handshake was designed with the security required to protect sensitive student information. From end-to-end encryption to strict access controls and internal policies your student records are safe with Handshake.



Amazon Web Services: Provides data storage and servers that power Handshake. AWS also stores system backups.

Heroku: Provides a management layer atop of Amazon web services. Heroku provides server management and orchestration across the Handshake AWS instance.

Handshake Application Layer: Handshake's software layer is built for security and is tested against a database of known threats upon each build.

Continued on the next page

Heroku Security

Handshake uses Heroku to assist with infrastructure management, scaling, and security. Heroku is a cloud application platform used by organizations of all sizes to deploy and operate applications throughout the world. Heroku is designed to protect from threats by applying security controls at every layer from physical to application, isolating customer applications and data, and with its ability to rapidly deploy security updates without customer interaction or service interruption.

Heroku and the AWS infrastructure powering Heroku is compliant with the following certifications:

- ISO 27001
- SOC 1 and SOC 2/SSAE 16/ISAE 3402 (Previously SAS 70 Type II)
- PCI Level 1
- FISMA Moderate
- Sarbanes-Oxley (SOX)
- PCI Compliant
- Sarbanes Oxley

Details on Heroku's security can be found here: https://www.heroku.com/policy/security. Please note that Heroku security documents may require an NDA between Heroku and the University.

Heroku also provides the following threat management tools:

- Firewalls
- DDoS Mitigation
- Spoofing and Sniffing Protections
- Porting Scanning

A security white paper on Heroku is available upon request.

Our Infrastructure

Handshake Security

Handshake's application layer is designed with security in mind. Our engineering and security teams ensure that Handshake is the most secure Career Management platform available today.

All data in Handshake is encrypted at rest using AES encryption. Data in transmission is encrypted using TLS. Non-secure connections are not allowed.

Before deploying every change must be signed off on by our VP of Engineering and our the head of quality assurance. These changes are audited for proper access control, coding best practices, and adherence to the Handshake privacy policy.

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, denial of service and many other potential security concerns.

Handshake's security team audits the security of all external libraries quarterly and apply security updates as they are released. Handshake's third party security assessments cover all areas of the platform including testing for OWASP Top 10 web application vulnerabilities and customer application isolation.

Handshake is a multi-tenant system. All data in Handshake is controlled through a strict access control layer ensuring that users can only see data that they have permission to access.

Data Retention

Handshake's contract outlines data use and ownership policies. Handshake will store de-identified aggregated data derived from system usage indefinitely. This information is used to power Handshake's job recommendation engines and enables the delivery of personalized content to end users.

Upon the request of the data owner Handshake will purge identifiable and personal information from the database. User data may still exist in backups even after removal from the primary data stores.

Third Parties

Handshake's platform is built with third party providers. Handshake's security and legal teams vet all third party providers against a stringent set of security standards. Providers used in Handshake have passed a Handshake security audit and meet or exceed the security standards set by Handshake. Services that are driven by third parties in Handshake include:

- Hardware and server infrastructure
- Mass email management
- Customer service integrations
- Issue tracking and reporting

Third parties may gain access to Handshake data in accordance with the Handshake MSLA.

Data Ownership and Transfer

Data ownership is dictated by the Handshake MSLA signed by your University.

Amazon Security

Amazon is one of the most trusted hosting providers in the world. Amazon maintains a series of security certifications including:

- ISO 27001
- PCI Compliance (Level 1)
- AICPA and SOC
- HIPAA

AWS environments are continuously audited, with certifications from accreditation bodies across the globe.

Amazon provides all server management for Heroku and Handshake. Handshake is hosted in the US-EAST Amazon data center.

Details on Amazon's compliance can be found here: https://aws.amazon.com/compliance/ please note that many documents are only available by signing an NDA with Amazon.

Data Security

Customer data is stored in an access-controlled database. Customer data is not shared or made available to anyone outside of the organization. Access to the data is limited to access controlled API keys and through the Handshake UI.

Financial Security & PCI Compliance

Handshake does not handle, process, store, or transmit sensitive financial data through our servers. Handshake uses Stripe to process financial data through a security point-to-point tunnel.

In 2015 an independent third party security consulting firm, the NCC Group (link), deemed Handshake as a merchant under the PCI guidelines. the NCC group found Handshake to be in full compliance with PCI guidelines.

For more details on Handshake's PCI compliance please request the PCI report document from your assigned Handshake team member.

Incident Handling

Handshake uses extensive security monitoring tools to monitor for breaches or potential vulnerabilities. Any indication of a breach or security vulnerability are flagged to the Director of Product and the Director of Engineering. A team of engineers will then review each breach.

If an incident is determined to have resulted in a breach of Handshake data the data breach policy will be invoked (see attached). If the incident did not result in a data breach or was caused by an internal user the incident will be handled at the discretion of the product team.

Operational Security

Handshake takes great pride in the security measures that are embedded into our technology. Equally as important is the human component of security. We take access to Handshake data seriously and have strict policies in place to ensure your data stays safe.

Security Training

All Handshake employees go through security training. This training covers security best practices covering topics like: password management, data deletion policies, access controls, use of physical media, and more. During these trainings all employees are issued company secured and encrypted laptops.

Security refresher courses are given annually and periodic security checks are done with Handshake staff to ensure compliance. Handshake team members also undergo FERPA training during the on-boarding process.

Data Ownership

Data ownership is dictated by the Handshake MSLA signed by your University. Handshake claims no ownership over data imported by the University that has not otherwise been claimed by a student.

Summary

Handshake prides itself on security. Our security team comes from some of the most advanced security organizations in the world and are accustomed to working with top-secret government datasets. These same principles have been applied to Handshake to create the most secure career center management software available.