Information Security Statement

Our clients trust iHasco with their data, and we make it a priority to take our clients' security and privacy concerns seriously. We strive to ensure that user data is retained securely, and that we collect only as much personal data as is required to provide our services to clients in an efficient, lawful and effective manner.

iHasco uses advanced technology for Internet security that is commercially available today. This Security Statement is aimed at being transparent about our security infrastructure and practices, to help reassure you that your data is appropriately protected.

Some of the data we hold on your behalf is stored and processed within the UK, Ireland and the US. In all cases the processors are GDPR compliant or are certified to the EU-U.S. and Swiss-U.S. Privacy Shield Framework.

Application and User Security

- SSL/TLS Encryption: All communications with the iHasco Application occur over SSL/TLS connections. Secure Sockets Layer (SSL) and Transport Layer Security (TLS) technology (the successor technology to SSL) protect communications by using both server authentication and data encryption. This ensures that user data in transit is safe, secure, and available only to intended recipients.
- User Authentication: User data on our database is logically segregated by account-based access rules. Clients can opt to enforce that users login to their training suite with a unique username and password via their LMS. The iHasco Application issues a session cookie only to record encrypted authentication information for the duration of a specific session. The session cookie does not include the password of the user.
- User Passwords: If enabled via the LMS user passwords have minimum complexity requirements. Passwords are individually salted and hashed.
- Data Portability: iHasco facilitates the export of user and results data from our application in CSV format so that you can back it up, or use it with other applications. Additionally you can use our API to extract your data and integrate with other third party applications.

- Privacy: We have a comprehensive privacy policy that provides a very transparent view of how we handle your data, including how we use your data, who we share it with, and how long we retain it.

Data Centre Security

- Data Centres: Our information system's infrastructure (servers, networking equipment, etc.) is collocated at a third party ISO 27001:2013 certified data centre managed by our partner, Memset.
- Data Centre Security: The Memset data centre is monitored by CCTV with footage retained for 90 days. Access is limited to specific necessary personal and entry is by Biometric and/or RFID badges.
- Environmental Controls: The Memset data centre has continuous environmental monitoring and is fitted with a FM-200 fire suppression system.
- Location: All user data is stored on servers located in the UK or Ireland.

Data Centre Availability

- Power: Servers have redundant internal and external power supplies. Data centre has backup power supplies.
- Uptime: Continuous uptime monitoring, with escalation to iHasco staff for any downtime.

Application Security

- Uptime/Performance: Continuous uptime and performance/error monitoring, with escalation to iHasco staff for any downtime.
- Third Party Scans: Weekly vulnerability/security scans are performed on the production server by Nessus.
- Testing: Application functionality and design changes are verified in a test environment prior to deployment to the production server.
- Access Control: Secure authentication, and role-based access is enforced for application management by authorized engineering staff.

Storage Backup

- Local Backup Frequency: Backups occur on a nightly basis to a local drive on the application server and then subsequently in an encrypted form to a RAID based external drive within the Memset data centre.
- Remote Backup Frequency: On a daily basis the most recent backup is transferred from the Memset data centre to a remote storage facility based in Ireland which is provided by Amazon.
- Backup Retention: We retain 5 daily backups, 4 weekly backups and 6 monthly backups at both our local and remote backup facilities.
- Server Snapshots: We retain regular snapshots of our server infrastructure in order that we can re-provision servers with minimal downtime should they suffer from catastrophic failure.

Organizational & Administrative Security

- Employee Screening: We perform background screening on all employees.
- Training: We provide security and technology use training for employees.
- Service Providers: We screen our service providers and bind them under contract to appropriate confidentiality obligations if they deal with any user data.
- Access: Access controls to sensitive data in our application, systems and environments are set on a need-to-know / least privilege necessary basis.
- Information Security Policies: We maintain internal information security policies, including incident response plans, and regularly review and update them.
- Accreditations: We have been accredited by APMG for Cyber Essentials Certification (Certificate #CES/00656).

Software Development Practices

- Stack: Our application is developed using an established open source framework based on recognised set of programming and database languages.

- Coding Practices: Our engineers use good practice and follow industry-standard coding guidelines. The application code base is hosted within an environment which provides version control and a complete audit trail of changes.

Handling of Security Breaches

Despite best efforts, no method of transmission over the Internet and no method of electronic storage is perfectly secure. We cannot guarantee absolute security. However, if iHasco learns of a security breach, we will notify the ICO in accordance with the Data Protection Act 2018 and, if required by law, any affected parties within 48 hours of us becoming aware of said breach.

Your Responsibilities

Keeping your data secure also depends on you ensuring that you maintain the security of your account by using sufficiently complicated passwords and storing them safely. You should also ensure that you have sufficient security on your own systems, to keep any user and/or results data (which you download via CSV or extract via our API) away from individuals without access permission.