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.

This Security Statement is aimed at being transparent about our security infrastructure and practices, to help reassure you that your data is appropriately protected.

Data which we hold on your behalf is always stored within the UK. Some of our data processing activities are carried out by sub-processors located outside of the UK. Permitted under the Data Protection Act 2018 when subject to appropriate safeguards, iHasco's international sub-processors are subject to Standard Contractual Clauses.

Application and User Security

- **SSL/TLS Encryption:** All communications with the iHasco Application take place over a TLS 1.2 connection. Transport Layer Security (TLS) technology (the successor technology to SSL) protects 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. LMS users login to the application with a unique username and password. 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:** LMS user passwords have minimum complexity requirements (between 8 and 20 chars in length, at least one lowercase, at least one uppercase, at least one number, at least one special character). 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. This includes; how we use your data, who we share it with, and how long we retain it for.
- **Encryption:** All data is encrypted at rest using AES-256 encryption. We utilise TLS for in transit encryption.

Data Centre

- **Data Centres:** Our information system's infrastructure (servers, networking equipment, etc.) is collocated at a third party ISO/IEC **27001:2013**, **27017:2015**, **27018:2019**, and ISO/IEC **9001:2015** certified data centre managed by our partner, Amazon Web Services (AWS).
- **Security:** CCTV covering all physical access points. Physical access is controlled at building ingress points, using surveillance, detection systems and electronic means. MFA is required to access data centres. All entrances to server rooms are secured with alarmed devices to initiate an incident response should a door be forced or held open. Electronic intrusion detection systems are installed within the data layers to monitor, detect and automatically alert appropriate personnel of security incidents. Monitored 24/7 via AWS Security operation centres.
- **Environmental Controls:** AWS monitors electrical and mechanical systems and equipment to enable immediate identification of issues. This is carried out by utilising continuous audit tools and information provided through our Building Management and Electrical Monitoring Systems. Preventative maintenance is performed to maintain the continued operability of equipment.
  They're also equipped with automatic fire detection and suppression equipment. Fire detection systems utilise smoke detection sensors within networking, mechanical, and infrastructure spaces. These areas are also protected by suppression systems.
- **Location:** All user data is stored on servers located in the UK.
- **Availability:** AWS has identified critical system components required to maintain the availability of our system and recover service in the event of outage. Critical system components are backed up across multiple, isolated locations known as Availability

Zones. Each Availability Zone is engineered to operate independently with high reliability. Availability Zones are connected to enable you to easily architect applications that automatically fail-over between Availability Zones without interruption. Highly resilient systems, and therefore service availability, is a function of the system design. Through the use of Availability Zones and data replication, we can achieve extremely short recovery time and recovery point objectives, as well as the highest levels of service availability.

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 Detectify.
- **Testing:** Application functionality and design changes are verified in a test environment using test data prior to deployment to the production environment.
- **Access Control:** Secure authentication utilising 2FA and role-based access is enforced for application management by authorised engineering staff.
- **Penetration Testing:** Annual penetration tests are performed by an external Crest certified provider.

Backups

- **Backup Frequency:** Backups occur on a nightly basis, to an S3 bucket stored on AWS. This is then also backed up to a local storage server on site. Both storage locations are encrypted utilising AES-256.
- **Backup Retention:** We retain rolling daily backups for 180 days.
- **Server Snapshots:** All servers are created via IAC (Infrastructure as Code) and can be easily re-created and configured within 15 minutes. All servers that are currently running are created from an image, which is stored in Amazon. We retain server images for the previous 15 successful deployments.

Organisational & Administrative Security

- **Employee Screening:** We perform basic employment screening on all employees.
- **Training:** We provide Cyber Security and GDPR training for all employees.
- **Service Providers and Sub-processors:** We screen our service providers and sub-processors 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 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) and are currently working on achieving ISO 27001 Certification.

Software Development Practices

- **Stack:** Our application is developed using an established open source framework based on a recognised set of programming and database languages.
- **Coding Practices:** Our engineers use best 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.