Harbr_

DATA SHEET

Harbr Security Posture

Harbr exists to help organizations unlock the full value of their data. By making us part of your data strategy, you are instilling a level of trust in Harbr to protect your valuable data assets. We take that responsibility very seriously and put security at the forefront of our product design, operations and customer engagement.

Securing Your Data Exchange

Data Centers

Your data exchange is hosted within an Amazon Web Services (AWS), Google Cloud or Microsoft Azure (coming soon) data center of your choice. Each cloud provider employs a robust physical security program with multiple certifications, including SSAE 16 certification.

Backup and Disaster Recovery

Your data is held in a relational database and encrypted cloud data repository across multiple availability zones within a region. The database is replicated synchronously so that we can quickly recover from a database failure. Your data is backed up to a separate data center of your choosing to ensure the data exchange can be restored in the event of a regional failure. Your data exchange has no single points of failure and will autoscale to support your growth.

Network Protection

Multiple layers of security controls protect access to and within your environment. Virtual air gapped networks are created for each service via the use of internal firewalls (security groups), internal route tables and roles, based on the principle of least privileged access control. Tight network routing controls within your data exchange allow close route monitoring and network traffic anomaly detection as each subnet/service has a very clear behavioral pattern.

Encryption

We encrypt all data in transit, using industry-standard TLS (Transport Layer Security), and at rest. Our platform forces all requests over HTTPS, ensuring all traffic is secured in transit and protecting against protocol downgrade attacks.

Authentication

Users access your data exchange using a unique email address and password. All passwords are salted and hashed using bcrypt and never stored in the clear.

Access Control

Your data exchange administrator is in complete control of the organizations and individuals invited to join your data exchange and their entitlements within it. The administrators for each organization within the data exchange are in control of who can join that specific organization and the roles of each of its users.

Entitlements

Anyone who publishes data and models to your data exchange maintains custody of those data products and controls who is entitled to use them and for what purpose. Even our support staff cannot access these artifacts unless they are entitled to do so.

Maintenance and Support

Your data exchange is continuously monitored for service impacting alarms, event logs, notifications and alerts. Security and anti-malware patches are applied automatically to ensure your data exchange is always up to date.

Only approved Harbr staff with temporarily elevated privileges can access your data exchange infrastructure via secure VPN connection, requiring multi-factor authentication and SSH public key authentication. All operational support activity is logged.

Harbr Security Priorities

Security Accreditations

We are both Cyber Essentials and ISO/IEC 27001 certified, which validate our high standards in provisioning and supporting the security, availability and confidentiality of your data exchange. We regularly undertake internal and external audits to make sure we adhere to the security controls we have implemented to achieve these accreditations.

SECURITY CERTIFICATIONS

Information Security Management ISO 27001 Certified

CYBER ESSENTIALS

IASME Consortium ®

Self-certified | Company GDPR

Employee Security
We evaluate new employees for security risks and require every employee to sign a contract that binds them to our information security and data confidentiality policies. Access rights are based on the employee's job function and are reviewed regularly. All staff obtain regular briefings to maintain awareness of security in all work environments.

Mobile devices are regularly audited against our secure configuration requirements, which include full disk encryption, configured firewalls, use of anti-malware and construction of strong passwords. Removable media is prohibited and all network connections are via a secure VPN.

Software Delivery
Security is the first principle against which our product design is measured, and we implement it from the ground up. Our code is developed following industry-standard secure coding guidelines and is automatically inspected to detect bugs, code smells and security vulnerabilities. All changes are version controlled via a Git repository and secured across multiple clouds.

A suite of automated tests is run to further test the code prior to each release, and we periodically invite external security consultants to scrutinize our approach and to challenge our security controls.

We follow the agile development methodology and features are approved and released via our secure, continuous delivery pipeline.

Data Privacy and GDPR
We only store personal information that is absolutely necessary and follow the principles of the European Union (EU) General Data Protection Regulation (GDPR) of May 2018. Our core compliance with the act means we:

- Have full awareness of where any of your data is being held, and when outside the EU, ensuring a
- Appropriate compliance is in place.
- Ensure that only those who require access to your data have it and implement the highest level of protection against unauthorised access.
- Ensure you have the right to view, amend, export or delete any information that we hold on your behalf, including anything held by 3rd-party services.
- Ensure that consent is given during the sign up process for all users of your data exchange and allowing you to withdraw this at anytime

Our Data Protection Officer and Privacy Policy govern our data privacy guidelines and are available should you have any questions or concerns.

Harbr_