DATASHEET

Privacy and Security

HSI EHS, SaaS System, ensures data privacy and security in compliance with global industry standards. We host our system components within the robust Amazon Web Services (AWS) computing cloud, leveraging different AWS services to guarantee our infrastructure's stability and security. Our organization is ISO 27001 certified, and SOC 2 compliant.

Security Infrastructure

HSI ensures data isolation for each customer by setting up dedicated Virtual Private Clouds (VPCs) and utilizing separate schemas in PostgreSQL for database-level segregation. Traffic filtering is handled through AWS Web Application Firewall (WAF), while data exchange is secured using the industry-standard SFTP protocol.

HSI EHS System components:

- **Application Server:** Hybrid Ruby on Rails backend and VueJS frontend, built on AWS ECS containers, backed by EC2 instances.
- **Data Storage:** PostgreSQL database with schema-based multitenancy. Running in AWS RDS.
- **Caching:** AWS Elasticache representing Redis cache.
- **Data Exchange:** SFTP gateway storing data in AWS S3 using AWS Transfer.
- **Load Balancing:** SSL/TLS termination by AWS application load balancers, while SFTP traffic goes through AWS network load balancers.

HSI EHS uses open-source software like PostgreSQL, Redis, Docker, S3 SFTP gateway, and HashiCorp Vault. We follow industry standard practices for data encryption both in transit (SSL 256-bit encryption) and at rest using the /contrib function library pgcypto.

The HSI Difference

Access Control and Single Sign-On: Users access our system through individual usernames and passwords, with configurable password complexity requirements. We offer support for Two-Factor Authentication and IP whitelisting.

We support integration with customers' Single Sign-On solutions, including ADFS 3.0, SAML 2.0, and Okta.

Administrative access to systems infrastructure requires individual and segregated AWS logins, and MFA with a hardware key. Remote access to sensitive data is protected through JIT access controls and an SSL VPN. All privileged access is limited to authorized personnel, and this access is reviewed regularly.

Data Loss Prevention: Our hosting environment includes a Data Loss Prevention system and leverages AWS Security and incident management reporting tools. We maintain real-time audit logs of all activities, notifying customers of any unauthorized changes within 24 hours.

SIEM implementation with the audit trails can track down and revert any unauthorized changes made. For customers on a dedicated instance, we offer the ability to export logs to a 3rd party system like Splunk or Graylog, enabling customers to utilize their existing SIEM for audit log management.

Data Backup and Business Continuity: Data stored within HSI EHS is protected by 35 days of hot backups with 5 minutes time resolution. Weekly backups are stored for 90 days. Monthly backups are stored indefinitely in AWS Glacier. Our RDS configuration includes a read-replica which can be promoted should the master fail, aiming to restore services (RTO) within four hours and recover data (RPO) as of five minutes before a disaster.

HSI EHS also maintains a Business Continuity Management framework that includes project management, risk analysis and review, business continuity and impact analysis, and recovery strategy development.

Incident Response and Support: Our Incident Management Policy outlines strategies and procedures for handling security incidents, enabling 24/7 response to critical availability or security incidents. Customers can initiate support tickets, chat live, or call 800-447-3177 to speak with Technical Support.

Compliance and Certifications: HSI EHS is a SOC2 Compliant solution and is ISO 27001 certified, validating our commitment to quality and information security management.

HSI EHS utilizes AWS as our hosting provider. AWS maintains an extensive security and compliance program including SOC1, SOC2, and ISO 27001 compliance. HSI monitors all key vendors through our third-party risk assessment program, including annual validation and re-review of security and compliance.

Cross-Platform Compatibility: The app runs smoothly on various devices and operating systems, ensuring a consistent user experience whether on Android, iOS, or desktop environments.

Integration: We support integration with external and third-party applications, managing both live feeds and batch-based capabilities for data importing and exporting. Clients can use our well-documented API or perform batch imports/exports using SFTP.

Data Privacy: HSI EHS maintains a robust data privacy policy and does not share, sell, rent, or trade personally identifiable information with third parties for promotional purposes. Customers' data is fully accessible and usable for reporting and transition purposes. We are compliant with GDPR and CCPA requirements. For more detailed information, please view here for our full Privacy Policy.

Audit Trails and Logs: All activities within our EHS System are logged and monitored. These audit trails support regulatory compliance and investigation of security incidents.