Security Overview

A Guide for Customers

Published December 2, 2022

Contents

EHS Insight Security Overview

Our Company and Product

EHS Insight is the world's leading Environmental, Health and Safety solution platform. Since 2009, StarTex Software has been on a mission to make the world a safer place to live and work. Today, hundreds of thousands of users in more than 45 countries use our software, services, and support to transform the way they manage, perform, and improve. Our EHS software, EHS Insight, is ranked #1 by GetApp, Capterra, and G2Crowd.

The EHS Insight platform includes Aspects and Impacts, Audit Management, Corrective Actions, Chemical Inventory, Claims Management, Compliance Tasks, Hazard and Risk, Health Encounter, Incident Management, Industrial Hygiene, Job Safety Analysis, Journey Management, Lessons Learned, Man-hours, Management of Change, Objectives, Onboarding, Performance Management, Permitted Work, Quality Management, Safety Drill, Safety Meetings, SDS Management, Skills Management, Sustainability, Training Management, Vendor Management, Waste Management, and Work Observations.

Our customers can configure their preferred solution by subscribing to various modules.

EHS Insight Security and Risk Governance

EHS Insight's primary security focus is to safeguard our customers' and users' data. This is the reason that we have invested in the appropriate resources and controls to protect and service our customers. This investment includes the implementation of a robust Information Security Management System that conforms to and has been certified to be compliant with ISO 27001:2013.

We are focused on defining new and refining existing controls, implementing and managing the EHS Insight security framework as well as providing a support structure to facilitate effective risk management.

Our Security and Risk Management Objectives

We have developed our security framework using best practices in the SaaS industry. Our key objectives include:

- Customer Trust and Protection – consistently deliver superior product and service to our customers while protecting the privacy and confidentiality of their information.

- Availability and Continuity of Service – ensure ongoing availability of the service and data to all authorized individuals and proactively minimize the security risks threatening service continuity.
- Information and Service Integrity – ensure that customer information is never corrupted or altered inappropriately.
- Compliance with Standards – implement process and controls to align with current international regulatory and industry best practice guidance.

We have designed our security program around best-of-breed guidelines for cloud security. In particular, we leverage standards like ISO 27001:2013, ISO 27017:2015, and NIST SP 800-53. We also align our practices with those defined in OWASP, COBIT, and Cloud Security Alliance CCM.

EHS Insight Security Controls

In order to ensure we protect data entrusted to us, we implemented an array of security controls. Our security controls are designed to allow for a high level of employee efficiency without artificial roadblocks, while minimizing risk. The following sections describe a subset of controls. For more information, visit https://www.ehsinsight.com/content/ehs-management-software/cloud-security.

EHS Insight Product Infrastructure

Data Center Security

EHS Insight outsources hosting of its product infrastructure to leading cloud infrastructure providers. We leverage Amazon Web Services (AWS) for infrastructure hosting and Google Cloud Platform (GCP) as a backup host. These solutions provide high levels of physical and network security and well as hosting provider vendor diversity. Our primary AWS cloud server instances and GCP cloud instances reside in US locations. Both providers maintain an audited security program, including SOC 2 and ISO 27001 compliance. EHS Insight does not host any product systems within its corporate offices. Beginning in 2022 we offer EU hosting service. For customers selecting this service, all data will be hosted in Ireland.

These world-class infrastructure providers leverage the most advanced facilities infrastructure such as power, networking, and security. Facilities uptime is guaranteed between 99.95% and 100%, and the facilities ensure a minimum of N+1 redundancy to all power, network, and HVAC services. Access to these providers' sites is highly restricted to both physical access as well as electronic access through public (internet) and private (intranet) networks in order to eliminate any unwanted interruptions in our service to our customers.

The physical, environmental, and infrastructure security protections, including continuity and recovery plans, have been independently validated as part of their SOC 2 Type II and ISO 27001 certifications. Certificates are available at the AWS compliance site and Google Cloud Platform security site.

Network Security and Perimeter Protection

The EHS Insight product infrastructure is built with internet-scale security protections in mind. In particular, network security protections are designed to prevent unauthorized network access to and within the internal product infrastructure. These security controls include enterprise-grade routing and network access control lists (firewalling).

Network-level access control lists are implemented in AWS Virtual Private Cloud (VPC) security groups or GCP firewall rules, which applies port- and address-level protections to each of the server instances in the infrastructure. These firewalling technologies deny unintended traffic by default, and all network traffic is logged and used to inform our monitoring systems (more about that in Alerting and Monitoring below). These network access rules allow for finely grained control of network traffic from a public network as well as between server instances on the interior of the infrastructure. Within the infrastructure, internal network restrictions allow a many-tiered approach to ensuring only the appropriate types of devices can communicate.

Changes in the network security model are actively monitored and controlled by standard change control processes. All existing rules and changes are evaluated for security risk and captured appropriately.

Configuration Management

Automation drives our ability to scale with our customers' needs. The product infrastructure is a highly automated environment that flexibly expands capacity and capability as needed. Server instances are fully templated and configuration management is fully automated, meaning that any server's configuration is tightly controlled from creation through deprovisioning.

Changes to the configuration and standard images are managed through a controlled change management process. Each component is based on a hardened configuration. Patch management and configuration control is typically handled by removing server instances that are no longer compliant with the expected baseline and provisioning a replacement instance in its place. Rigorous and automated configuration management is baked into our day-to-day infrastructure processing.

Alerting and Monitoring

Not only do we fully automate our build procedures, we invest heavily in automated monitoring, alerting and response technologies to continuously address potential issues. The EHS Insight product infrastructure is instrumented to alert engineers and administrators when anomalies occur. This includes error rates, abuse scenarios, application attacks, and other anomalies trigger automatic responses and alerts to the appropriate teams for response, investigation, and correction. As unexpected or malicious activities occur, systems bring in the right people to ensure that the issue is rapidly addressed.

Many automated triggers are also designed into the system to immediately respond to foreseen situations. Traffic blocking, quarantine, process termination, and similar functions kick in at pre-defined thresholds to ensure that the EHS Insight platform can protect itself against a wide variety of undesirable situations.

The power behind our ability to detect and respond to anomalies is our 24x7x365 monitoring program and extensive logging. Our systems capture and store logs that include all the technologies that comprise our products. At the application layer, all logins, page views, modifications, and other access to EHS Insight instances are also logged. In the infrastructure back-end, we log authentication attempts, horizontal and vertical permission changes, infrastructure health, and requests performed among many other commands and transactions. Logs and events are monitored in real time and events are escalated immediately at any hour of the day to developers, security professionals, and engineers to take appropriate action.

Infrastructure Access

Entire categories of potential security events are prevented with a stringent, consistent, and well-designed access control model. Along those lines, access to EHS Insight production systems is strictly controlled. Employees are granted access to resources and assets based on their jobs, using a role-based access control model. More information about our RBAC model across the company is available in Customer Data Protection section below.

For access to infrastructure tools, servers, and similar services, access is minimized to only the individuals whose jobs require it. For emergency access necessary in certain situations, our personnel use a Just-In-Time-Access (JITA) model in which certain employees can request access to certain privileged functions for a limited duration. The request is logged and logs are continuously monitored for suspicious requests. Access to the privileged function is granted, and the person can go about his or her work.

Additionally, direct network connections to product infrastructure devices over SSH or similar protocols is prohibited, and engineers are required to authenticate first through a bastion host or "jump box" before accessing QA or production environments.

Application Protection

Web Application Defenses

As part of its commitment to protecting customer data and websites, EHS Insight utilizes an industry recognized Web Application Firewall (WAF). The WAF automatically identifies and protects against attacks aimed at EHS Insight products and services. The WAF protects platform access (e.g., the features you can access by browsing to the EHS Insight website, integrating with APIs, or the endpoints used by the native applications). Additionally, all Customer Data hosted on the platform is also automatically protected. The rules used to detect and block malicious traffic are aligned to the best practice guidelines documented by the Open Web Application Security Project (OWASP) in the OWASP Top 10 and similar recommendations. Protections from Distributed Denial of Service (DDoS) attacks are also incorporated, helping to ensure that customer access to EHS Insight products are available continuously.

The WAF is configured with a combination of industry standard and custom rules that are capable of automatically enabling and disabling of appropriate controls to best protect our customers. These tools actively monitor real-time traffic at the application layer with ability to alert or deny malicious behavior based on behavior type and rate.

Development and Release Management

One of EHS Insight's greatest advantages is a rapidly evolving feature set, and we provide constantly improved products through a modern continuous delivery approach to software development. Code reviews and quality assurance are performed on every line of code as it is checked in. Once approved, code is automatically submitted to our continuous integration environment where compilation, packaging and unit testing occur. If all passes, the new code can be deployed across the appropriate tier.

All code deployments create archives of existing production-grade code in case failures are detected post-deployment. The deploying team manages notifications regarding the health of their applications. If a failure occurs, rollback is immediately engaged. As part of the continuous deployment model, we use extensive software gating and traffic management to control features based on customer preferences (private beta, public beta, full launch). Major feature changes are communicated through in-app messages and/or product update posts.

Newly developed, built code is first deployed to the dedicated and separate QA environment for the last stage of testing before being promoted to production. Network-level segmentation prevents unauthorized and undesirable access between QA and production environments. Customer data is never used in the QA environment, nor does any other testing use customer data.

Vulnerability Scanning, Penetration Testing, and Responsible Disclosure

The EHS Insight team manages a multi-layered approach to vulnerability scanning, using a variety of industry-recognized tools to ensure comprehensive coverage of our technology stack. We perform vulnerability scanning and penetration testing activities against ourselves on a continuous basis. Static code analysis automatically reviews the most current code to detect potential security flaws early in the development lifecycle.

Continually running scans, adaptive scanning inclusion lists, and continuously updating vulnerability signatures help us stay ahead of many security threats. To get a second opinion about our ability to identify and respond to security risks, we bring in industry-recognized third parties to perform annual penetration and web application tests. The goal of these programs is to iteratively identify flaws that present security risk and rapidly address any issues. Penetration tests are performed against the application layers and network layers of our technology stack, and penetration testers are given internal access to the product and/or corporate networks in order to maximize the kinds of potential vectors that should be evaluated.

In addition to internal vulnerability scanning and independent penetration testing, StarTex Software manages a bug bounty program. Independent security researchers are invited to participate in identifying security flaws in EHS Insight and are rewarded for their submissions. Security community members and customers are welcome to perform security testing against trial sites. Information about the Responsible Disclosure is available at https://www.ehsinsight.com/responsible-disclosure.

Customer Data Protection

Confidential Information in EHS Insight

EHS Insight is a comprehensive environmental, health and safety solution platform. The information collected in our product is data gathered through customer end user interaction. This often includes sensitive information. Although our customers are in control of what data will be collected, we treat the Customer Data as private and take precautions to appropriately protect it.

Credit Card Information Protection

Many EHS Insight customers pay for the service by credit card. EHS Insight does not store, process or collect credit card information submitted to us by customers. We leverage trusted and PCI-compliant payment vendors to ensure that customers' credit card information is processed securely and according to appropriate regulation and industry standards.

Encryption In-Transit and At-Rest

All interactions with EHS Insight (e.g., API calls, login, authenticated sessions to the customer's instance, etc.) are encrypted in-transit with at least TLS 1.2 including 2048-bit keys or better.

EHS Insight leverages several technologies to ensure stored data is encrypted at rest. The physical and virtualized hard drives used by EHS Insight product server instances as well as long-term storage solutions like AWS S3 use AES-256 encryption. Additionally, certain databases or field-level information is encrypted at rest. For instance, user passwords are hashed.

Encryption keys for both in-transit and at-rest encryption are securely managed by the EHS Insight platform. TLS private keys for in-transit encryption are managed through our content delivery partner. Volume and field-level encryption keys for at-rest encryption are stored in a hardened Key Management System (KMS). Keys are rotated, and the frequency varies by the type of key and the sensitivity of the key and the data it protects; in general, TLS certificates expire every two years.

User Login Protections

EHS Insight users may login to their accounts using built-in EHS Insight login, or by using one of the many supported Single Sign On providers. The built-in login enforces a uniform password policy which requires a minimum of 8 characters and include at least 1 special character, at least 1 number, and a combination of lower- and upper-case letters.

Customers who use a Single Sign On (SSO) provider can set up SSO-based login for their users. Depending on their identity provider, customers may have many options to control password complexity and reuse, as well as IP restrictions.

User and API Authorization

Customers can assign finely grained permissions for their accounts and limit access to their data features. For more information about user roles, please see the EHS Insight Knowledge Base. Application programming interface (API) access is enabled through an API key authorization. Customers have API keys for read-only access and full access.

EHS Insight Employee Access

EHS Insight controls individual access to data within its production and corporate environment. A very small subset of our employees are granted access to production data based on their role in the company through role based access controls (RBAC) or on an as-needed basis referred to as JITA (just in time access).

The Product Development team members are not granted access to production environments.

may be granted access to various production systems, as a function of their role. Common access needs include alert responses and troubleshooting, as well as to analyze information for product investment decisions as well as product support. Access to the product infrastructure is limited by network access and user authentication and authorization controls. Access to networking functions is strictly limited to individuals whose jobs require that access, and access is reviewed on a continual basis.

Customer Success, support, and other customer engagement staff with a need-to-know may request just in time access to customer portals on a time-limited basis. However, our normal procedure is to request our customers to invite the support staff into their instance, so they may manage access on their own. Requests for access are limited to their work responsibilities associated with supporting and servicing our customers. The requests are limited to just-in-time access to a specific customer's portal. All access requests, logins, queries, page views and similar information are logged.

All employee access to both corporate and product resources is subject to daily automated review and at least semi-annual manual recertification to ensure the granted authorization is appropriate for an employee's role and job needs.

Privacy

The privacy of our customers' data is one of our primary considerations. As described in our Privacy Policy, we never sell your Personal data to any third parties. The protections described in this document and other protections that we have been implemented are designed to ensure that your data stays private and unaltered. EHS Insight is designed and built with customer needs and privacy considerations in the forefront. Our privacy program incorporates best practices and regulatory requirements.

Along those lines, EHS Insight is certified under the EU-US and Swiss-US Privacy Shield Frameworks. More information about our certification is available on the Privacy Shield site.

Data Retention Policy

Customer data is retained for as long as you remain an active customer. The EHS Insight platform provides active customers with the tools to delete their data, as they see fit. Former customers' data is removed from live databases upon a customer's written request or after an established period following the termination of the customer agreements. Former paying customers' data is purged 90 days after customer relationships are terminated. Information stored in replicas, snapshots, and backups is not actively purged but instead naturally ages itself from the repositories as the data lifecycle occurs, which also takes about 90 days. EHS Insight retains certain data like logs and related metadata in order to address security, compliance, or statutory needs.

Privacy Program Management

The EHS Insight team collaborates to ensure an effective and consistently implemented privacy program. Information about our commitment to the privacy of your data is described in greater detail in our Privacy Policy and the Data Processing Agreement available on our GDPR site.

Business Continuity and Disaster Recovery

EHS Insight maintains business continuity and disaster recovery plans focusing both on preventing outage through redundancy of telecommunications, systems and business operations, and on rapid recovery strategies in the event of an availability or performance issue. Whenever customer-impacting situations occur, our goal is to quickly and transparently isolate and address the issue. Identified issues are published on the EHS Insight status site and are subsequently updated until the issue is resolved.

Backup Strategy

EHS Insight ensures data is replicated and backed up in multiple durable data-stores. The retention period of backups depends on the nature of the data. Data is also replicated across availability zones and infrastructure locations/providers in order to provide fault-tolerance as well as scalability and responsive recovery, when necessary.

Customer (production) data is backed up leveraging multiple online replicas of data for immediate data protection. Production databases are fully backed up everyday and incrementally every 15 minutes. Three copies of each backup file are maintained:

1. On the instance,
2. within the VPC, and
3. within another provider's network.

A minimum of thirty days' worth of backups are kept for any database in a way that ensures restoration can occur easily. Snapshots are taken and stored to a secondary

service no less often than daily and where practicable, real time replication is used. All production data sets are stored on a distributed file storage facility such as Amazon's S3.

Because we leverage private cloud services for hosting, backup and recovery, EHS Insight does not implement physical infrastructure or physical storage media within its products. EHS Insight does also not generally produce or use other kinds of hard copy media (e.g., paper, tape, etc.) as part of making our services available to customers.

By default, all backups are protected through access control restrictions on our production infrastructure networks, access control lists on the file systems storing the backup files and/or through database security protections.

For customers who would additionally like to back up their data, the EHS Insight platform provides many ways of making sure you have what you need. Many of the features within your instance contain export features, and the EHS Insight library of APIs can be used to synchronize your data with other systems. For the details about backing up your data, please check out our Knowledge Base article about exporting your content.

StarTex Software Corporate Security

Employee Authentication and Authorization

StarTex Software enforces an industry-standard corporate password policy. That policy requires changing passwords at least every 90 days. It also requires a minimum password length of 8 characters and complexity requirements including special characters, upper- and lower-case characters, and numbers. StarTex Software prohibits account and password sharing by multiple employees. Additionally, production infrastructure access requires multi-factor authentication or are protected by single-sign on solutions that enforce multi-factor authentication.

Access Management

StarTex Software has regimented and automated authentication and authorization procedures for employee access to StarTex Software systems. All access is logged. Most frequently, access is granted based on a role-based access control model. Just in time access is built into automated procedures around a set of rigorous authorization mechanisms.

Background Checks

StarTex Software employees undergo an extensive 3rd party background check prior to beginning employment with us, wherever local regulations and employment standards allow. In particular, employment, education, and criminal checks are performed for potential employees. Reference verification is performed at the hiring manager's

discretion. All employees must comply with Non-Disclosure Agreements and Acceptable Use Policy as part of access to corporate and production networks.

Corporate Physical Security

StarTex Software adopted a 100% remote workforce in 2020. Although over 50% of our company was already remote, we relinquished our corporate office and went all-in. However, we do utilize co-working spaces, which are shared office environments which also feature a small private space. These offices are secured in multiple ways. Security guards are employed at location to help create a safe environment for employees. Door access is controlled using RFID tokens tied to individuals, which are automatically deprovisioned if lost or when no longer needed (e.g., employee termination). Video surveillance, and many other protective measures are implemented across these offices including the private office areas/corridors.

Vendor and Supplier Management

We maintain a vendor management program to ensure that appropriate security and privacy controls are in place. The program includes inventorying, tracking, and reviewing the security programs of the vendors who support EHS Insight.

Appropriate safeguards are assessed relative to the service being provided and the type of data being exchanged. Ongoing compliance with expected protections is managed as part of our contractual relationship with them.

Security Awareness and Security Policies

To help keep all our engineering, support, and other employees on the same page with regard to protecting your data, we developed and maintain an Information Security Policy. The policy covers data handling requirements, privacy considerations, and responses to violations, among many other topics.

With this policy and the myriad protections and standards in place, we also ensure employees are well-trained for their roles. Multiple levels of security training are provided to employees, based on their roles and resulting access. General security awareness training is offered to all new employees and covers security requirements of our policies and systems. After initial training, different training tracks are available based on an employee's role. Developer-specific training is provided by and tailored to our engineering teams.

Incident Management

EHS Insight implements 24x7x365 coverage to respond quickly to all security and privacy events. Our rapid incident response program is responsive and repeatable. Pre-defined incident types, based on historical trending, are created in order to facilitate timely incident

tracking, consistent task assignment, escalation, and communication. Many automated processes feed into the incident response process, including malicious activity or anomaly alerts, vendor alerts, customer requests, privacy events, and others.

In responding to any incident, we first determine the exposure of the information and determine the source of the security problem, if possible. We communicate back to the customer (and any other affected customers) via email or phone (if email is not sufficient). We provide periodic updates as needed to ensure appropriate resolution of the incident.

Our Chief Technology Officer reviews all relevant security-related incidents, either suspected or proven, and we coordinate with affected customers using the most appropriate means, depending on the nature of the incident.

Product Security Features

StarTex Software's security program is designed to protect EHS Insight and Customer Data entrusted to us. We take advantage of common application development security best practices as well as infrastructure security and high availability configurations.

We work hard to maintain the privacy of data you entrust with us. Data you store in EHS Insight is yours. We put our security program in place to protect it and use it only to provide the service to you. We never share your data across customers and never sell it.

EHS Insight infrastructure is hosted in Amazon Web Services and Google Cloud Platform. Our hosting strategy enables additional redundancy capabilities, architecture flexibility, and infrastructure responsiveness. Our deployment processes leverage network security, server security, and availability features described above.

EHS Insight leverages the protections of a world-class Web Application Firewall (WAF). By default, your instance is protected from state-of-the-art Distributed Denial of Service (DDoS) and other web application attacks. When security events occur, our Security Operations and DevOps teams take immediate action to ensure that your data are protected continuously 24x7x365.

Compliance

StarTex Software maintains compliance with the EU-US Privacy Shield as mentioned in our Privacy Policy. The EHS Insight platform also contains features that enable our customers to easily achieve and maintain their General Data Processing Regulation (GDPR) compliance requirements. More information about privacy compliance and EHS Insight are available in our GPDR compliance content and the DPA located there.

EHS Insight is hosted within world-class cloud infrastructure providers Amazon Web Services and Google Cloud Platform. EHS Insight infrastructure providers are SOC 2 Type II and ISO 27001 certified and maintain facilities secured against electronic and physical intrusion.

Document Scope and Use

StarTex Software values transparency in the ways we provide solutions to our customers. This document is designed with that transparency in mind. We are continuously improving the protections that have been implemented and, along those lines, the information and data in this document (including any related communications) are not intended to create a binding or contractual obligation between StarTex Software and any parties, or to amend, alter or revise any existing agreements between the parties.