SOL-X DATA PRIVACY & SECURITY POLICY

DATA PRIVACY & SECURITY POLICY

As the world becomes digitally enabled and as Industry 4.0 trends start to take hold, data tied to individuals and the collective enterprise has increasingly become a symbiotic relationship towards building a sustainable workforce of the future. In the safety and risk management space, the power of data can be used to discover important new details for improving human behaviour and elevating health and safety standards.

At SOL-X, we are committed to safeguarding the privacy and security of data belonging to users of our products and customers who have engaged our company to provide products and services. This Data Privacy & Security Policy document will help you understand how SOL-X collects, uses and processes your personal data and informs you about your privacy rights.

SOL-X PRIVACY AND SECURITY VALUES

SOL-X recognizes the importance of information security and client confidentiality as a foundation of the company's activities and is dedicated to setting the highest standards necessary to protect our customers' data and our own software assets.

HOW WE PROTECT YOUR DATA

SAFEVUE.ai by SOL-X is delivered to our customers through a Software as a Service (SaaS) Cloud model and an On-Premise Edge Server model.

CLOUD BASED SECURITY AND RELIABILITY

Cloud Based Security and Reliability
SAFEVUE.ai uses world class secure cloud service providers such as Microsoft Azure and Google Cloud Platform.

Data collected through SAFEVUE.ai will be stored with our secure cloud service provider, equipped with leading security standards and compliant with data privacy regulations.

The Cloud based architecture provides many advantages, including enabling an important data handling collaboration with our secure cloud service provider so we can stay as up-to-date as possible with our security practices across the system.

The Cloud based architecture also allows us flexibility, such as to designate geo-localized server locations as necessary for compliance to regulations.

Disaster Recovery is performed via common industry practices including rolling backups and geographically segregated data centres.

Our secure cloud services conform to global security certification requirements.

PHYSICAL SECURITY

For the Software as a Service (SaaS) Cloud model, physical site security and site access control are in place both within the SOL-X organization that supports and administers the SAFEVUE.ai solution and our secure cloud services partner.

APPLICATION SECURITY

Security and penetration testing by CREST certified security providers are performed for all relevant components of the SAFEVUE.ai application, including the SAFEVUE.ai Database, SAFEVUE.ai Administration Portals, SAFEVUE.ai Office Portal, Edge Server and SSH Reverse Proxy.

Only a small number of pre-authorized SOL-X administrators can access customer and user data for customer support purposes.

VESSEL ON-PREMISE SECURITY AND RELIABILITY

Edge Servers on the vessel are to be installed in a secured server room by the customer. Edge Servers are password protected to prevent unauthorized access by the crew. There is no direct remote access to the onboard Edge Servers and access is only available via secured and encrypted connection from a designed SSH Reverse Proxy server.

Access to hardware devices (personnel devices, tablets, touchscreen dashboard) onboard the vessel are secured through individualized crew pin identification. All relevant data from mobile devices is synced to the secured Edge Server.

The secured Edge server is implemented with SSD RAID drives to provide additional local reliability. In addition, data replication to the Cloud occurs on a regular basis when satellite connectivity is available.

NETWORK SECURITY

- Strong passwords, encrypted channel communications and layer security authorizations protect client data from unauthorized access.
- Network access to perform operations within the SAFEVUE.ai platform is subject to credentialing, permitted access rosters, and user access audit logging.
- Our Edge Server, Reverse Proxy and Cloud based services have been extensively tested for penetration by CREST certified security testing vendor.
- Onboard the vessel, the SOL-X local Wi-Fi network, access points and routers are password protected. To complete the Ship-to-Shore data communication, SAFEVUE.ai solution relies on customer ship's satellite connectivity and all data transmission is TLS encrypted.
- Remote access to the vessel on-premise system is performed through TLS based SSH encrypted connection.
- SAFEVUE.ai customer data uses hardware encryption at the device level, TLS 1.2 over HTTPS for data in transit, and AES 256-bit encryption for data in storage.

HOW WE USE YOUR PERSONAL DATA

SAFEVUE.ai is an integrated safety and risk management solution which consists of various functions and features. SOL-X will collect, process and store user personal data for the following purposes including:

- To verify the identity of user for activities such as access management and personalized user experience.
- To fulfill core functionalities of the product features, including integrated Permits To Work ("PTW"), Crew Finder, Crew Assist and Work and Rest hours management.
- To aggregate, mine and analyze data for the purposes of improving SAFEVUE.ai, creating new features, conducting research and developing new products and services, including reports based on analytics associated with SAFEVUE.ai. User data will be anonymized and de-identified such that the data or aggregated data will not enable each unique user to be identified.
- To communicate any product announcement, software updates, changes to the product and features and changes to the terms and conditions.

DATA GOVERNANCE AND SUPPORT

SOL-X has taken great care to lay down an integrated data security and management system to provide adequate control, visibility, actionable insights and compliance throughout the data collection, processing, transmission and storage journey.

SOL-X has an IT data access and governance policy. Procedures are in place to quickly respond to any data incidents.

To ensure integrity and security of user personal information, our privacy and security guidelines are communicated to all employees and strictly enforced within the company.

Technical support can be reached by calling +65-67203020

Users can also request support via email at support@sol-x.co.

In instances of service termination, customers may request removal of their identifiable data from the system, consistent with contractual terms.