MAGELLANX

Enabling Sustainability

SOL-X

Data Privacy & Security Policy

December 2022

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 developed a symbiotic relationship in 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 Magellan X we are committed to safeguarding the privacy and security of data belonging to our customers and the users of our products. This Data Privacy & Security Policy document will help you understand how Magellan 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

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

Physical Security

For the Software as a Service (SaaS) Cloud model, Magellan X and our secure cloud service provider have in place physical site security and site access controls.

Cloud Based Security and Reliability

- SOL-X uses world class secure cloud service providers such as Microsoft Azure and Google Cloud Platform.
- Data collected through SOL-X will be stored with our secure cloud service provider, which has implemented comprehensive security measures to ensure and maintain the security of its infrastructure, and has committed to adhering to rigorous security and compliance standards.
- The Cloud based architecture enables Magellan X to collaborate closely with our secure cloud service provider to handle data, allowing us to stay as up-to-date as possible with our security practices across the system.
- The Cloud based architecture also allows us flexibility to designate geo-localized server locations as necessary for compliance with applicable 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.

Network Security

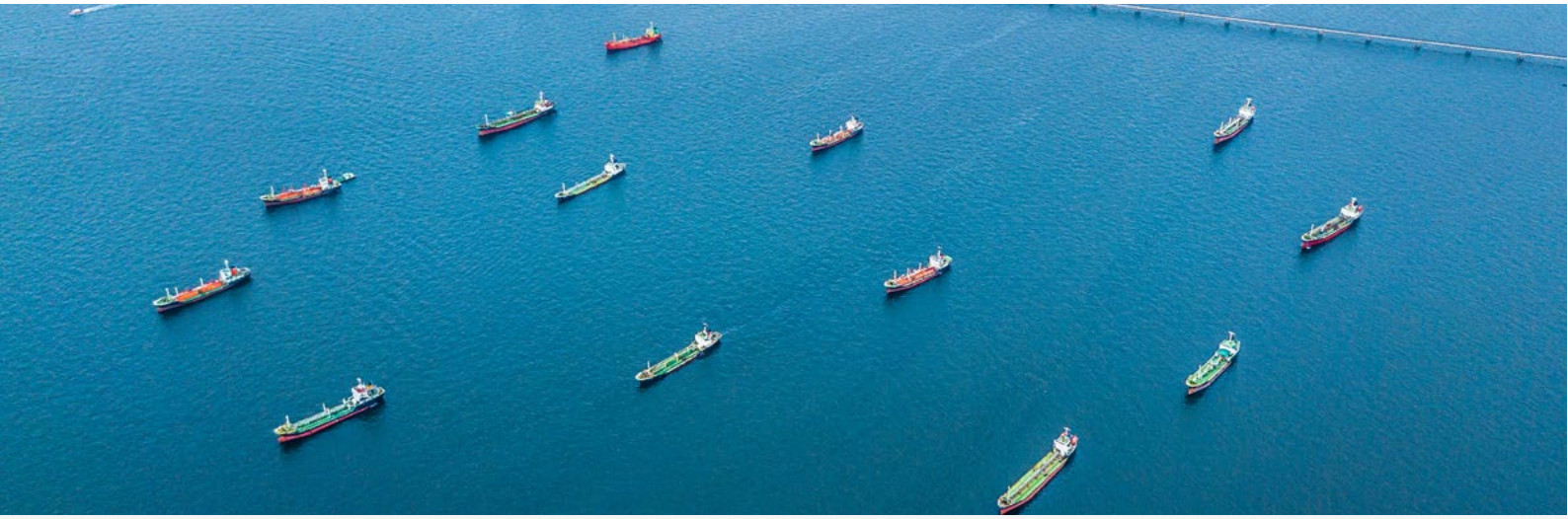
- Strong passwords, encrypted channel communications and layer security authorizations protect client data from unauthorized access.
- Network access to perform operations within the SOL-X platform is subject to credentialing, permitted access rosters, and user access audit logging.
- Our Edge Server, 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, the SOL-X solution relies on customer ship's satellite connectivity and all data transmission is TLS encrypted.
- Remote access to the vessel's on-premise system is performed through TLS based SSH encrypted connection.
- SOL-X 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.

Application Security

- Security and penetration testing by CREST certified security providers are performed for all relevant components of the SOL-X application, including the SOL-X Database, SOL-X Administration Portals, SOL-X Office Portal, Edge Server and SSH Reverse Proxy.
- Only a small number of pre-authorized Magellan 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 is secured through the requirement of unique PIN for each individual crew member. 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.

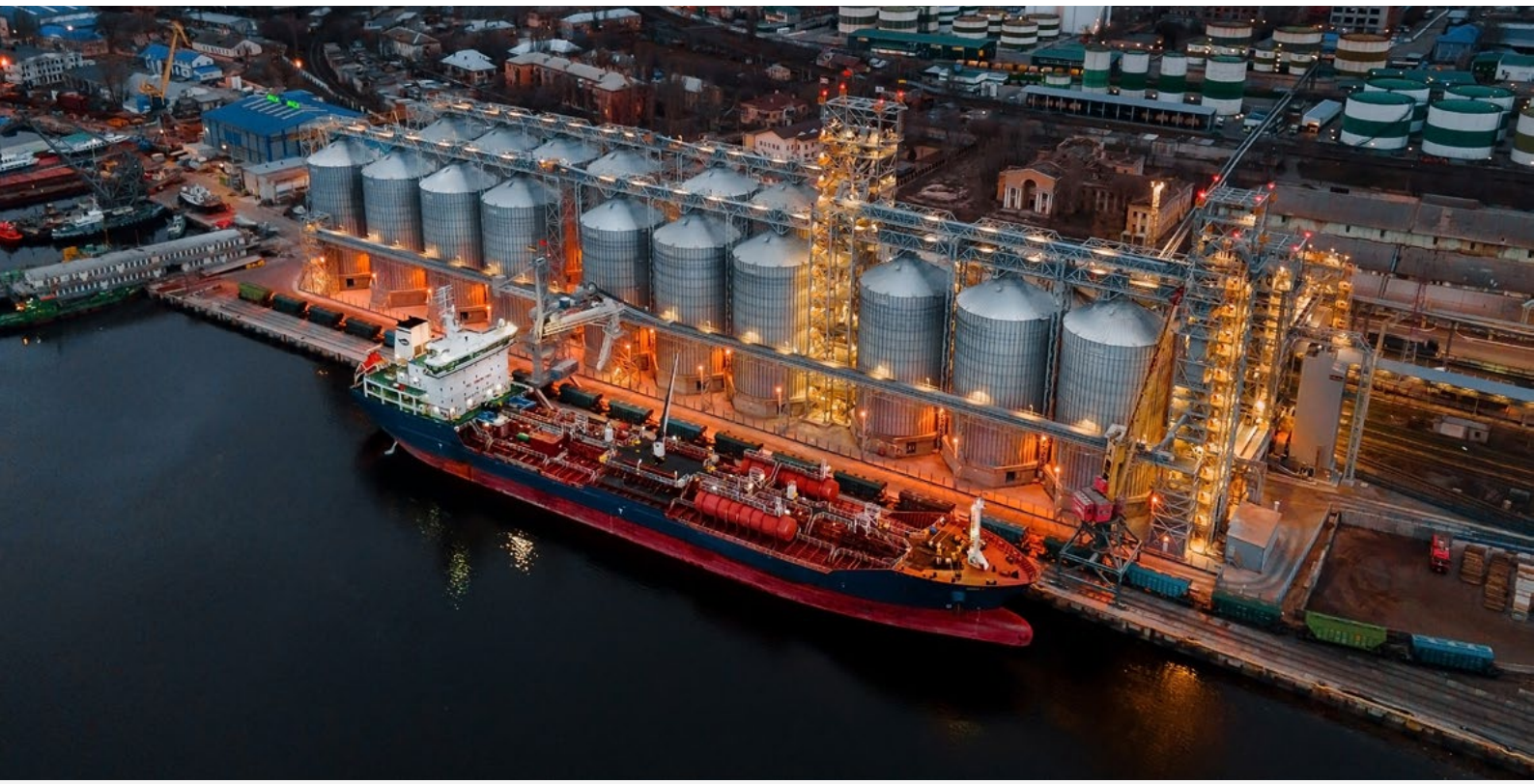


How We Use Your Personal Data

- SOL-X 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 SOL-X, creating new features, conducting research and developing new products and services, including reports based on analytics associated with SOL-X. 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

- Magellan X has taken great care to implement an integrated data security and management system to provide adequate control, visibility, actionable insights in relation to the collection, processing, transmission and storage of personal data.
- Magellan 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 solx.support@magellanx.co.
- In instances of service termination, customers may request for the removal of their identifiable data from Magellan X's system.



MAGELLANX

Enabling Sustainability