MAGELLANX

Enabling Sustainability

SOL-X

# Data Privacy & Security Policy

May 2023

# 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 work force of the future. In the safety and risk management space, the power of data is used to discover important added 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 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 Magellan X collects, uses, and processes your personal data and informs you about your privacy rights.

## Magellan X Privacy and Security Values

Magellan 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 optionally through On-Premise Edge Server model.

We are committed to protecting personal data and ensuring users privacy. We act appropriately to ensure the security and confidentiality of user's personal data.

SOL-X data is stored locally within the SOL-X application & devices and can only be accessed by the SOL-X application.

User data is protected by removing personal identifiers by encryption.

## Cloud Base Security and Reliability

- SOL-X uses worldclass secure cloud service providers such as Microsoft Azure.
- Data collected through SOL-X 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 data handling collaboration with our secure cloud service provider for us to stay up to date as much 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 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.
- Our Cloud server and Cloud hosted edge servers can be enabled with Cloud Service Provider's DDoS protection service.

## Physical Site Security

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

## On-Premise Security and Reliability

- Edge Servers at the customer location are to be installed in a secured server room by the customer. Edge Servers are password protected to prevent unauthorized access. 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 customer site are secured through individualised PIN identification. All relevant data from mobile devices is synchronised 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 connectivity is available.

## Physical Device Security

- SOL-X Smart devices such as watches and tablets are intrinsically safe, explosion proof IOT (Internet of Things) devices which are also secured against data security attacks at the device level.
- Data from SOL-X devices are sent to local edge server and to cloud server via Client's secured infrastructure and firewalls. Data sent from edge server to cloud server is encrypted.
- SOL-X IOT devices are protected using Device Management and are updated using OTA (Over-The-Air). New devices connecting to network or application servers are automatically detected.

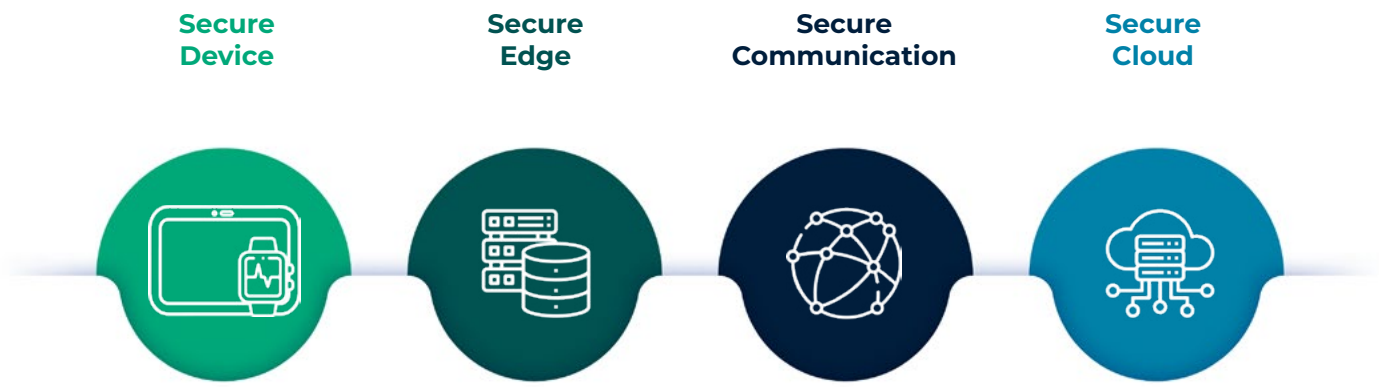
## Application Security

- Security and penetration testing by CREST certified security providers are performed for all relevant components of the SOL-X application, including the Database, Administration Portals, Office Portal, Edge Server and SSH Reverse Proxy.
- Only pre-authorised SOL-X administrators can access customer and user data for customer support purposes.

# 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 routers, and user access audit logging.
- Our Edge Server, Reverse Proxy and Cloud based services have been extensively tested for penetration by a Crest certified security testing vendor.
- Onboard the Customer site, the SOL-X local Wi-Fi network, access points and routers are password protected. To complete the Edge-to-Cloud data communication, SOL-X solution relies on customer site connectivity and all data transmission is TLS encrypted.
- Remote access to the customer 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.

## SOL-X IIoT & IT Security Features



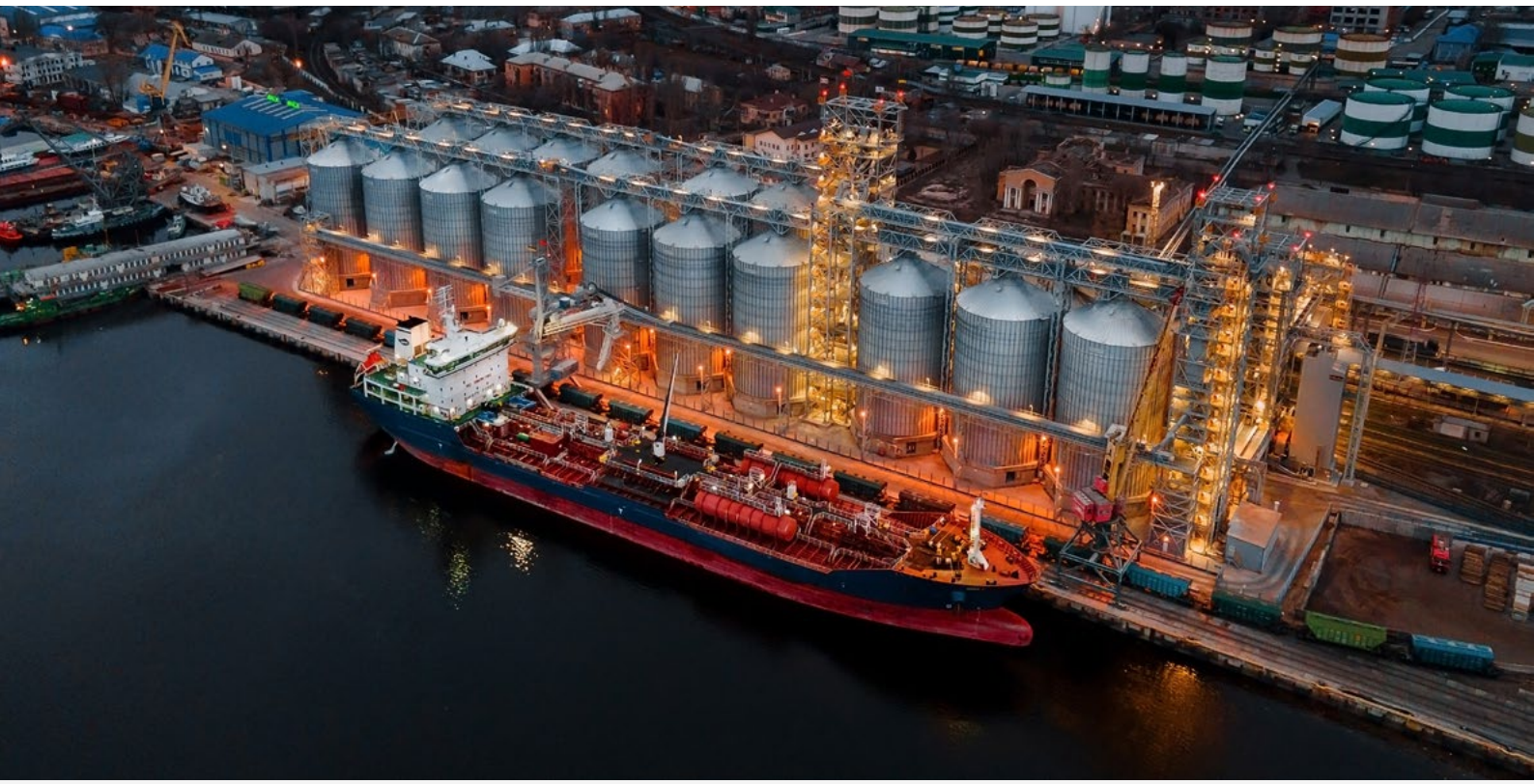
## How We Use Your Personal Data

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 fulfil 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 analyse 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 to remove personal identifiers from the data / aggregated data.
- To communicate any product announcement, software updates, changes to the product and features and changes to the terms and conditions.

## GDPR (General Data Protection Regulation) Compliance

- 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 solx.support@magellanx.co.
- In instances of service termination, customers may request removal of their identifiable data from the system, consistent with contractual terms.



MAGELLANX

Enabling Sustainability