



Purpose

This document summarises the technical and organisational measures used to protect Customer Data and Service Data in the Senso.cloud platform, based on the Senso Security Datasheet, Privacy Notice, Business Continuity & Disaster Recovery document and Supplier Security Assessment.

Control area	Measures
Encryption and transmission security	Industry-standard protocols for data in transit between devices and Microsoft datacentres; SSL/TLS, IPsec and AES referenced in the Security Datasheet; encryption for data, files, applications, services, communications and drives.
Data at rest	Azure Storage encryption at rest; archived data stored as JSON in Azure Blob Storage and encrypted at rest.
Identity and access management	Backend Azure configuration/tenancy protected by two-factor authentication; time-limited, authorised access; least privilege.
Customer support access	Access to customer portals by Senso support requires explicit customer permission, is just-in-time, logged and audited, and is revoked after the engagement.
Microsoft support access	Microsoft Azure support access to stored data requires explicit Senso.cloud permission and is just-in-time, logged and audited, then revoked.
Database controls	Databases are IP restricted to physical offices; auditing enabled; Microsoft Threat Detection enabled.
No master accounts	There are no Senso staff master accounts capable of accessing all customer accounts.
Module integrity	Senso modules are hashed and only modules with the correct hash are allowed to run.
Device control	Devices require approval before they are shown in the Senso portal.
Vulnerability management	Azure vulnerability assessment on databases and web servers, plus third-party scanning, as stated in the supplier security assessment.
Monitoring and audit	Technical controls include IP restrictions, matched credentials, intrusion detection and auditing, supported by database auditing and Microsoft Threat Detection.
Training and awareness	Employees receive data privacy and security training through Improve.online and professional development processes.
Availability and resilience	Azure hosting, modular architecture, deployment slots, rollback ability, full/differential/transaction backups and geo-replication.

Secure disposal	Microsoft datacentres support secure disposal; office-based drives are destroyed using KillDisk Ultimate to industry standards.
Shared responsibility	Customers must implement security best practices, educate users and can use Microsoft/Google account protections and console restrictions by public IP, day and time.

Source basis

- Business Continuity & Disaster Recovery, revised 17 May 2019
- Senso Security Datasheet, revised 17 June 2024
- Supplier Data Security Assessment Questionnaire, completed 10 May 2023