Service Robot Co.

DATA SECURITY

Your systems. Your data. Your control.

Every Service Robot Co. deployment is designed around customer-controlled data, documented access, and a clear operating boundary.

XENGINEERING, LLC
team@servicerobotco.com
(650) 362-8736
servicerobotco.com

Company-Wide Data Commitments

These standards apply to every product and system we choose to deploy, regardless of industry or use case.

Customer-controlled architecture

The customer approves where operational data is stored and which systems may receive it. For data-sensitive use cases, we select only products and architectures that can satisfy the agreed customer-controlled or on-premises boundary.

Documented data flows

Before deployment, we document what data is collected, where it goes, who can access it, and which external services or subcontractors are involved.

Controlled access

Every proposed system documents how named users, roles, permissions, and administrator ownership work. Customer administrators retain control of accounts and permissions wherever the selected product supports that model.

Customer-set retention

Retention, export, and deletion requirements are agreed before product selection. A vendor default is not accepted when it conflicts with the customer's documented boundary.

No secondary use

We document whether the product vendor, cloud provider, or support system has any right to use customer data. Products that permit sale or unapproved model training are not selected for the deployment. Diagnostic or support access is limited to the agreed purpose.

Permissioned support

Remote support connections and vendor dependencies are documented before deployment. Support access is customer-approved and time-bound where the selected architecture supports it.

Common Questions

Where is customer data stored?

Data storage location is set during system design. Options include on-premises servers, customer-controlled cloud, or OEM cloud — depending on the product selected and the customer's requirements. We do not default to any single architecture.

Can video and operational data stay on premises?

Yes, when the deployment requires it. We select products and architectures that support locally stored video, edge analytics, and on-premises management. Some systems may still require external connections for firmware updates, license checks, or telemetry — these are documented before deployment.

Who has access to system data?

Access is role-based and documented. Customer administrators control user accounts and permissions. SRCo support access is permissioned, time-bound, and recorded where the selected product supports it.

How long is data retained?

Retention periods are set by the customer before deployment. We configure the system to the agreed schedule and document the export and deletion process.

Does SRCo or any vendor use customer data for training, analytics, or resale?

No. We verify each product vendor's data-use terms before selection. Products that permit secondary use, model training, or data resale without the customer's explicit consent are not deployed.

What about drone telemetry and flight data?

Drone telemetry, flight-control links, and dock or cloud dependencies are documented in the product-specific data sheet. Storage location and access controls follow the same customer-controlled standard as any other system.

How are firmware updates and remote support handled?

Vendor firmware, update, diagnostic, and support connections are documented before deployment. Remote support sessions are customer-approved and, where the architecture supports it, time-bound with audit records.

Does SRCo hold SOC 2, ISO 27001, CJIS, or similar certifications?

We do not place generic certification claims on our materials. When a specific product, service, or scope holds a current certification, we document it with the exact certificate and scope. Our operating standard is the set of commitments described above — not an unsupported certification wall.

Product-Specific Data Sheet

Every proposed system receives a product-specific data sheet before purchase. The sheet covers:

Required Documentation

- Data collected
- Analytics and event metadata
- Local vs. cloud processing
- Drone telemetry and dock dependencies
- User roles and permissions
- Remote support access
- Incident escalation procedures
- Video and audio captured
- Storage location
- External connections
- Administrator ownership
- Retention and deletion
- Vendor update and diagnostic connections
- Backup and recovery

If a product cannot satisfy the deployment's required data boundary, access model, retention controls, or support process, it is not offered for that use case.

Important: This sheet describes SRCo's operating standard for data security across all deployments. It is not a compliance certification. Product-specific certifications, standards conformity, and regulatory applicability are documented per-deployment with the exact scope and evidence.
