LEGAL CENTER

Data Ownership & Security Policy

Who owns your data, how it is isolated per client, and the controls we use to protect it.

Document	Version	Effective date	Last updated
Data Ownership & Security Policy	1.0	August 1, 2026	July 28, 2026

This is the current published version. It is incorporated into the Master Services Agreement and supplements the Privacy Policy. Questions: dougc@charb-tech.com.

This Data Ownership & Security Policy (the "**Policy**") describes how Charbonneau Technologies (the "**Company**," "**we**," "**us**," or "**our**") treats ownership of, and protects, the data our clients entrust to us within the Services. It is incorporated into the Master Services Agreement and supplements the Privacy Policy.

1. Purpose & Scope

This Policy applies to Client Data processed within the Services, including the BusinessSystem application and the CT Monitoring service. It describes our commitments regarding data ownership and the administrative, technical, and physical safeguards we use to protect Client Data. It does not modify any more specific data or security terms agreed in a signed Order.

2. Data Ownership

Client Data belongs to the Client. As between the Parties, the Client retains all right, title, and interest in and to Client Data. We claim no ownership of Client Data and process it only to provide and support the Services, as directed by the Client, and as permitted by the applicable agreement and law. We do not use Client Data to advertise to the Client's customers, and we do not sell Client Data. We may generate aggregated, de-identified operational metrics (for example, system health and performance statistics) that do not identify the Client or any individual, to operate and improve the Services.

3. Data Classification

We handle information according to its sensitivity. Client Data typically includes business-operational records such as quotes, jobs, purchase orders, inventory, and related documents, and may include contact information for the Client's personnel, customers, and vendors. We treat all Client Data as confidential under the Master Services Agreement and apply controls appropriate to its sensitivity. The Client is responsible for determining whether to place particularly sensitive categories of data into the Services and for any consents required to do so.

4. Tenant Isolation & Architecture

The Services use a **dedicated, single-tenant architecture**. Each Client is provisioned with its own Deployment — a separate application instance and its own database — rather than sharing a common multi-tenant database with other clients. This means:

- Client Data is isolated at the application and database level by design, not solely by access rules within a shared store;
- One Client's Deployment does not have access to another Client's Deployment or data; and
- Configuration, updates, and data handling can be managed per Client.

The CT Monitoring service receives operational signals (such as heartbeats, error events, integration status, and daily metrics) from each Deployment to support availability and reliability, and is operated so that monitoring information is handled consistent with this Policy.

---

5. Access Controls

We restrict access to Client Data to authorized personnel who need it to deliver and support the Services, following the principle of least privilege. Controls include:

- Authenticated user access to the Services, with role-based permissions within the application;
- Administrative access to systems limited to authorized Company personnel;
- Multi-factor authentication on administrative and hosting (Azure) accounts; and
- Prompt review and removal of access when it is no longer required.

The Client is responsible for managing its own users' access within the Services and for safeguarding user credentials.

---

6. Encryption

We use encryption to protect Client Data:

- **In transit.** Access to the Services is protected using industry-standard transport encryption (TLS/HTTPS).
- **At rest.** Client Data is encrypted at rest using Azure's platform-managed, infrastructure-level storage encryption (256-bit AES).

---

7. Backups & Recovery

We perform regular backups of Client Deployments to support recovery in the event of data loss or system failure. Unless otherwise stated in an Order:

- Backups are performed on at least a daily basis;
- Backups are retained for 30 days;
- Our target recovery point objective (RPO) is 24 hours and target recovery time objective (RTO) is 24 hours; and
- We periodically verify that backups can be restored.

These objectives are targets based on our standard practices and may be tailored for a specific Client in an Order.

---

8. Infrastructure & Hosting

The Services are hosted on Microsoft Azure infrastructure in the Central US region. Our hosting providers maintain physical and environmental security controls for their data centers. We configure and maintain the application, operating system, and database layers, apply updates and security patches on a reasonable schedule, and monitor Deployments through the CT Monitoring service.

---

9. Incident Response

We maintain processes to detect, investigate, and respond to security incidents affecting Client Data. If we become aware of a security incident that has compromised, or is reasonably likely to have compromised, a Client's Client Data, we will:

- Take reasonable steps to contain and remediate the incident;
- Notify the affected Client without undue delay, within 72 hours of confirmation; and
- Provide information reasonably available to us about the nature of the incident and the measures taken, and cooperate with the Client's reasonable requests, including to help the Client meet its own legal obligations.

10. Data Portability & Return

During an active engagement, the Client may request an export of its Client Data in a commonly used format. On termination or expiration of the applicable Order, we will, on the Client's request made within thirty (30) days, make Client Data available for export, after which we will delete or de-identify Client Data in our production systems within 60 days, except for copies retained in routine backups (which are deleted on the backup cycle) or as required by law. We will confirm deletion on the Client's reasonable request.

11. Sub-processors

We may engage third-party service providers ("sub-processors") to help deliver the Services, such as cloud hosting and infrastructure providers. We enter into agreements with sub-processors that require appropriate confidentiality and security protections and use of the data only to provide services to us. Integrations that the Client chooses to enable — such as QuickBooks Online and Microsoft Office 365 / Microsoft Graph — involve the Client's own third-party accounts and are governed by those providers' terms. On request, we will provide information about the categories of sub-processors we use.

12. Contact

Questions about this Policy, or requests relating to data security and ownership, can be directed to Charbonneau Technologies at dougc@charb-tech.com or 678-387-7659.

Questions about this document? Email dougc@charb-tech.com or call 678-387-7659.