INFORMATION SECURITY POLICY

Vendor Management Policy

Crystalline Logistics Platform

Crystalline Supply Chain Solutions Ltd
Registered in Scotland · Company No. SC900213
Summit House, 4-5 Mitchell Street, Edinburgh EH6 7BD

Document ref: CRYS-POL-VM-01
Version 0.1 · Draft
Issued: 27 August 2026

Owner: Lewis · Lewis@crystalline-solutions.com

Vendor Management Policy

This policy defines how the third-party providers underpinning the Crystalline Logistics platform are selected, assessed and managed, so that client data remains protected across the supply chain.

1 Purpose & Scope

The platform is built on a small number of established third-party providers. This policy ensures those providers are chosen with care, meet appropriate security standards, and are reviewed periodically. It applies to all providers that store or process client data, or that are essential to operating the platform.

2 Provider Categories

FUNCTION	ROLE IN THE PLATFORM
Data platform	Holds the structured operational and contact data
Automation platform	Runs the automated processes that generate documents and move data
Document storage	Stores generated documents
Email / communication	Sends outbound documents and notifications
Document generation	Renders documents to their final format

> Where a client prefers, the platform can interface with the client's own equivalent systems (for example their own storage or email environment) in place of the default providers.

3 Selection & Due Diligence

- Providers are selected on the basis of their security posture, reliability and suitability for the function.
- Preference is given to established providers that publish security and compliance information and that maintain recognised certifications.
- The data each provider will hold or process is considered before adoption, and providers are given access only to what their function requires.

4 Data Handling by Providers

- Providers are used in line with their own terms and data protection commitments.
- Access to providers is authenticated and, where supported, protected by multi-factor authentication and scoped credentials.
- Credentials and tokens for providers are stored securely and rotated periodically.

5 Ongoing Management

- The set of providers in use is reviewed periodically to confirm each remains necessary and appropriate.
- Material changes to a provider's terms or security position are assessed for impact.
- A provider is replaced where it no longer meets the required standard.

ACTIVITY	FREQUENCY
Provider review	At least annually
Credential / token rotation	Periodically, and immediately on suspected exposure
Assessment of provider changes	As changes arise

6 Client Assurance

On request, a client can be provided with the list of providers used to deliver their service and the function each performs, to support the client's own vendor and data-policy assessments.

7 Responsibilities & Review

The Administrator is responsible for selecting, assessing and reviewing providers in line with this policy. This policy is reviewed at least annually, or sooner following any significant change to the providers used.

CRYSTALLINE

The third-party providers underpinning the platform are chosen with care, used securely, and reviewed regularly to keep client data protected across the supply chain.

Crystalline Supply Chain Solutions Ltd
Registered in Scotland · Company No. SC900213
Lewis@crystalline-solutions.com
Document ref: CRYS-POL-VM-01 · v0.1