INFORMATION SECURITY POLICY

Access 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-AM-01
Version 0.1 · Draft
Issued: 27 August 2026

Owner: Lewis · Lewis@crystalline-solutions.com

Access Management Policy

CRYS-POL-AM-01
v0.1 · Draft

This policy defines how user access to the Crystalline Logistics platform and its underlying systems is granted, controlled, reviewed and revoked. It applies to all individuals with access to client data held within the platform.

1 Purpose & Scope

The purpose of this policy is to ensure that access to client data is limited to authorised individuals, that the level of access granted is appropriate to each person's role, and that access is removed promptly when no longer required.

This policy covers all systems used to operate the Crystalline Logistics platform, including the Airtable data layer, the Make.com automation layer, document storage, and the email environment used for outbound communication.

2 Roles & Access Levels

Access is granted on a least-privilege basis. Each individual is assigned the lowest level of access required to perform their role.

ROLE	ACCESS GRANTED	TYPICAL HOLDER
Administrator	Full configuration, user management, schema and automation control	Platform owner
Editor	Create and edit operational records; generate documents	Operational users
Viewer / Read-only	View records and generated documents; no edit rights	Wider stakeholders as required
System / Service	Automated access via API tokens for integration tasks	Automation and document generation

> Editing access is restricted to named operational users on a per-project basis. Each live project is provisioned with its own access boundaries.

3 Provisioning & Deprovisioning

Granting access

- Access requests are approved by the Administrator before any account is created or invited.
- Each user is provisioned with a named individual account. Shared logins are not permitted.
- The access level granted is recorded against the user at the point of provisioning.

Removing access

- Access is revoked promptly when a user changes role or leaves, targeted within one working day of notification.
- Associated API tokens or service credentials tied to a departing user are rotated.

- Removal is recorded against the user.

Access Management Policy

4 Authentication

Credentials

- Users authenticate with a unique email identity and a password meeting the platform provider's complexity requirements.
- Passwords are not shared, reused across systems, or stored in plain text.

Multi-Factor Authentication (MFA)

Multi-factor authentication is enabled on all individual accounts with access to client data, using a time-based one-time passcode (TOTP) authenticator application as the second factor.

CONTROL	POSITION
MFA on individual accounts	Enabled for all users with data access
Org-wide enforced MFA	Available where a client data policy requires central enforcement (subject to platform plan tier)
Single Sign-On (SSO / SAML)	Available where a client requires identity brokered through their own provider (subject to platform plan tier)

> Where a client's data policy requires centrally enforced MFA or SSO that cannot be bypassed by the individual user, this can be provisioned on the platform's enterprise tier. This is arranged on a per-client basis.

5 Access Reviews

- A review of all active users and their access levels is carried out at least every six months.
- Each review confirms that every account is still required and that its access level remains appropriate.
- Any account no longer required is removed; any over-provisioned account is corrected.
- The date and outcome of each review is recorded.

6 Service & API Credentials

- Automated integrations authenticate using scoped API tokens rather than user passwords.
- Tokens are granted the minimum scope required for their function.
- Tokens are stored within the connection configuration of the relevant platform and are not exposed in plain text within scripts or documents.
- Tokens are rotated periodically and immediately if exposure is suspected.

7 Integration with Client Systems

The platform is designed to interface with a client's own systems where required, so that data storage and communication can align with a client's existing environment and data policy.

CAPABILITY	POSITION
Document storage	Provided via a managed storage layer by default; can interface with a client's own storage provider (for example Egnyte, SharePoint or equivalent) where required
Email / communication	Provided via a managed mailbox by default; can interface with a client's own Microsoft 365 or email environment where required
Identity	Can interface with a client's own identity provider for authentication where required (subject to platform plan tier)

> Where integration with a client's own systems is used, access to those systems is governed by the client's own access policies in addition to this policy.

8 Responsibilities

PARTY	RESPONSIBILITY
Administrator	Approving access, provisioning/deprovisioning, conducting reviews, maintaining records
All users	Protecting their own credentials, enabling MFA, reporting suspected compromise

9 Review of This Policy

This policy is reviewed at least annually, or sooner following any significant change to the platform, its systems, or applicable client requirements.

Access to client data is granted on a least-privilege basis, protected by multi-factor authentication, and reviewed regularly to ensure it remains appropriate.

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