INFORMATION SECURITY POLICY

Incident Response 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-IR-01
Version 0.1 · Draft
Issued: 27 August 2026

Owner: Lewis · Lewis@crystalline-solutions.com

Incident Response Policy

CRYS-POL-IR-01
v0.1 · Draft

This policy defines how security incidents affecting the Crystalline Logistics platform or the client data it holds are identified, contained, investigated, resolved and reported.

1 Purpose & Scope

The purpose of this policy is to ensure that any security incident is handled promptly and consistently, that affected clients are informed in a timely manner, and that lessons are captured to reduce the likelihood of recurrence.

This policy applies to all systems used to operate the platform and to all individuals with access to client data. It covers events affecting the confidentiality, integrity or availability of that data.

2 What Counts as an Incident

A security incident is any event that compromises, or threatens to compromise, the confidentiality, integrity or availability of client data or the platform. Examples include:

- Unauthorised access to an account or to client data
- Loss, theft or exposure of credentials or API tokens
- Accidental disclosure of data to an unintended recipient
- Loss of data integrity through corruption or erroneous processing
- Loss of platform availability beyond a routine service interruption
- Suspected malicious activity within any connected system

3 Severity Classification

On identification, each incident is assigned a severity level that determines the response pace and the level of client communication.

SEVERITY	DEFINITION	INITIAL RESPONSE TARGET
Critical	Confirmed exposure of client data, or total loss of platform availability	Immediate; within 4 hours
High	Suspected data exposure, or significant degradation of service	Within 1 working day
Medium	Contained issue with no confirmed data impact	Within 2 working days
Low	Minor issue, no data or availability impact	Within 5 working days

4 Response Process

Identify

The incident is logged with the time identified, how it was detected, and an initial description. A severity level is assigned.

Contain

- Immediate action is taken to limit further impact, for example revoking affected credentials, rotating tokens, or suspending an affected account or integration.
- Where appropriate, affected systems are isolated to prevent spread.

Investigate

- The cause, scope and data affected are established as far as is reasonably possible.
- Evidence relevant to the incident is preserved.

Resolve & Recover

- The underlying cause is remediated and normal service restored.
- Restoration from backup is used where data integrity or availability has been affected.

Close

The incident is formally closed once resolved, with the resolution and any follow-up actions recorded.

5 Client Notification

Where an incident affects, or is reasonably likely to have affected, a client's data, that client is notified without undue delay.

TRIGGER	NOTIFICATION
Confirmed or likely exposure of client data	Affected client notified without undue delay, with the facts known at the time
Personal data breach (where applicable)	Handled in line with applicable data protection law, including any regulatory notification obligations
Service availability incident	Affected clients informed of impact and expected restoration

> Notification is made with the information available at the time and updated as the investigation progresses. Initial notification is not delayed pending full root-cause analysis.

6 Post-Incident Review

- Following any Critical or High incident, a review is carried out to confirm the cause and identify preventive measures.
- Actions arising are tracked to completion.
- This policy and related controls are updated where the review identifies a gap.

7 Responsibilities

PARTY	RESPONSIBILITY
Administrator	Coordinating response, classifying severity, deciding containment, leading client notification and review
All users	Reporting suspected incidents promptly and not attempting to resolve them unaided where data may be affected

8 Review of This Policy

This policy is reviewed at least annually, or sooner following any significant incident or change to the platform.

CRYSTALLINE

Security incidents are contained quickly, investigated thoroughly, and affected clients are notified without undue delay.

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