BUSINESS CONTINUITY MANAGEMENT POLICY

Coastal Logistics Ltd

Document Ref: CLL-BCM-POL-001 | Version: 1.4 | Classification: CONFIDENTIAL

Version Control

Version	Date	Author	Description	Status
1.0	14 Feb 2019	R. Walsh (Ops Director)	Initial policy.	Approved
1.1	22 Aug 2019	R. Walsh (Ops Director)	Added port operations scope.	Approved
1.2	30 Jan 2020	R. Walsh (Ops Director)	Updated exercise requirements following tabletop.	Approved
1.3	17 Nov 2020	R. Walsh (Ops Director)	Crisis comms section added post-COVID disruption.	Approved
1.4	04 Sep 2021	R. Walsh (Ops Director)	Minor updates post-ransomware incident. ERP not yet reflected.	Approved

Approval and Sign-Off

Role	Name	Signature	Date
Board of Directors (Chair)	H. Fitzgerald	_____	04 Sep 2021
Operations Director	R. Walsh	_____	04 Sep 2021
Chief Financial Officer	M. O'Brien	_____	04 Sep 2021
Head of IT		_____	
HR Director	C. Ryan	_____	04 Sep 2021
Insurance Representative		_____	

GAPS: (1) Head of IT sign-off is absent — the IT Director responsible for technology recovery has not approved the BCP. (2) Insurance Representative column is blank — business interruption insurance requirements have not been validated against BCP recovery capabilities. (3) This policy was approved September 2021. The ransomware incident cost £3.2M and occurred 18 months after this approval — the policy has not been re-approved following the most significant continuity event in company history.

1. Purpose

This policy establishes the framework for Business Continuity Management (BCM) at Coastal Logistics Ltd ("Coastal" or "the Company"), ensuring the Organisation can maintain critical operations during and after a significant disruption. This policy was substantially developed following the ransomware incident of 2021 and is intended to address gaps identified in the post-incident review.

> **AUDIT NOTE — DELIBERATE GAP**
> *PURPOSE GAP: The policy references the ransomware incident as the impetus for this version, but the post-incident review's specific recommendations have not been documented as requirements within this policy. It is therefore impossible to verify whether all post-incident action items have been embedded into the BCM framework.*

2. Scope

This policy applies to all Coastal Logistics operations including:

- Head Office — Southampton
- Warehouse operations — Bristol, Felixstowe, Tilbury
- Port operations — 6 ports (Southampton, Felixstowe, Liverpool, Hull, Grangemouth, Belfast)
- All IT systems supporting logistics operations
- Third-party logistics partners with critical dependencies

> **AUDIT NOTE — DELIBERATE GAP**
> *SCOPE GAP: The new ERP system deployed 8 months ago is not listed as an in-scope system. A business continuity audit must assess whether critical systems deployed after the last policy review are captured in BIA assessments and BCPs.*

3. Business Impact Analysis

3.1 BIA Requirement

A Business Impact Analysis (BIA) must be conducted to identify critical business processes, their Maximum Tolerable Downtime (MTD), Recovery Time Objectives (RTO), and Recovery Point Objectives (RPO). The BIA must be reviewed and updated when significant organisational changes occur.

> **AUDIT NOTE — DELIBERATE GAP**
> *BIA GAPS: (1) No annual review frequency is defined — "when significant organisational changes occur" is insufficient. ISO 22301:2019 requires BIA reviews at planned intervals. (2) "Significant organisational changes" is not defined — the ERP deployment 8 months ago and acquisition of 2 new facilities have not triggered a BIA review. (3) No process exists for business process owners to validate or challenge MTD values. IT-declared RTOs and business-declared MTDs are not cross-validated. (4) No requirement to assess the financial, legal, reputational, and regulatory impacts of disruption separately.*

3.2 Process Classification

Processes must be classified as:

Tier 1 (Critical): MTD < 4 hours — immediate recovery required. Failure threatens life safety, regulatory compliance, or major financial loss.

Tier 2 (Important): MTD 4–24 hours — urgent recovery required. Failure causes significant operational disruption.

Tier 3 (Standard): MTD > 24 hours — planned recovery acceptable.

4. Business Continuity Plans

4.1 Plan Development

A BCP must be developed for each Tier 1 and Tier 2 process. Plans must include: activation criteria, step-by-step recovery procedures, named roles and responsibilities, contact lists (internal and external), and supplier/vendor dependencies.

> **AUDIT NOTE — DELIBERATE GAP**
> *PLAN DEVELOPMENT GAP: No minimum standard for BCP content is defined in this policy. Plans vary significantly in quality and completeness across business units. Some plans reference decommissioned systems (e.g. Legacy TMS v4.2) that no longer exist.*

4.2 Plan Ownership

Each BCP must have a named Plan Owner responsible for maintaining, testing, and executing the plan. Plan Owners must be trained on their plan responsibilities upon appointment.

> **AUDIT NOTE — DELIBERATE GAP**
> *OWNERSHIP GAPS: (1) No requirement to update Plan Owner records when the named owner leaves the Organisation. (2) No succession planning — if a Plan Owner is unavailable during an incident, there is no designated backup. (3) No requirement for Plan Owners to confirm annually that they have read and understood their plan. (4) No central register of BCPs and their owners maintained by the Operations Director.*

4.3 Plan Review

BCPs must be reviewed when significant changes occur to the relevant process or system.

> **AUDIT NOTE — DELIBERATE GAP**
> *REVIEW GAPS: (1) No minimum review frequency is defined. ISO 22301 requires at least annual review. The main warehouse BCP has not been updated in 3 years. (2) The ERP deployment 8 months ago has not triggered a BCP review despite being the primary operational system. (3) No sign-off process exists for post-review approvals — a review may occur without any evidence it was completed.*

5. Testing and Exercises

5.1 Exercise Requirement

BCPs must be tested through exercises to validate their effectiveness. Exercise types include: desktop walkthrough, tabletop exercise, and live simulation.

5.2 Exercise Frequency

Exercises must be conducted when deemed necessary by the Operations Director.

> **AUDIT NOTE — DELIBERATE GAP**
> *EXERCISE GAPS — CRITICAL: (1) "When deemed necessary" provides no minimum frequency commitment. ISO 22301 requires exercises at planned intervals. No exercise may be required for years under this policy. (2) No requirement exists to test the ransomware recovery scenario specifically — the most likely and most costly disruption type. (3) No requirement for lessons learned to be formally captured, assigned to owners, and tracked to closure. (4) No requirement for independent observers or post-exercise reports. An exercise may be conducted and declared successful with no objective evidence.*

6. Crisis Communications

Coastal maintains a Crisis Communications Plan identifying spokespersons for internal and external communications during a disruption.

Role	Responsibility	Named Individual	Backup
CEO	External media spokesperson	T. McGrath	Unassigned
Operations Director	Internal communications lead	R. Walsh	Unassigned
IT Director	Technical incident communications	[VACANT]	Unassigned
HR Director	Staff communications	C. Ryan	Unassigned
Legal Counsel	Regulatory notifications	External firm	Unassigned

AUDIT NOTE — DELIBERATE GAP

CRISIS COMMS GAPS: (1) IT Director role is VACANT — the primary technical communications spokesperson does not exist. (2) No backup is assigned for any role — if the CEO or Operations Director is unavailable, there is no designated escalation. (3) No social media crisis communications policy exists. (4) No template holding statements have been pre-approved for common disruption scenarios.

7. Policy Review

This policy is owned by the Operations Director and reviewed annually. Last reviewed: September 2021. Next review due: September 2022.

AUDIT NOTE — DELIBERATE GAP

OVERDUE REVIEW — CRITICAL GAP: This policy review is overdue by over 2 years. The policy has not been updated since September 2021 despite: a ransomware incident costing £3.2M, deployment of a new ERP system, and relocation of 2 facilities. A policy not reviewed within 12 months of a significant business continuity event does not meet ISO 22301 requirements.