Disaster Recovery

and Business Continuity Plan

Bank House, Marshall Terrace, Crossgates Leeds LS15 8EA
Tel: 0113 322 3765 Email: contact@lilacalliance.co.uk

Disaster Recovery and Business Continuity Plan

Policy owner: Lilac Alliance Management | Version 1.0 | Date: January 2026 | Next review: January 2027

Purpose

This plan sets out how Lilac Alliance will respond to a disruptive incident affecting our premises, systems, people or suppliers, so that we can continue to support our placed workers and client organisations with minimal interruption, and recover normal operations as quickly as possible.

Scope

This plan covers Lilac Alliance's Head Office at Bank House, Marshall Terrace, Crossgates, Leeds, and applies to all staff, systems and third-party services relied on to deliver our staffing services, including candidate and worker placement, payroll and compliance.

Potential Disruption Scenarios

This plan covers, but is not limited to, the following types of disruption:

- Loss of access to Head Office premises (fire, flood, utility failure, or similar).
- Loss of IT systems, internet connectivity, or key software platforms.
- Loss of key personnel, including sudden unavailability of senior staff.
- Failure or unavailability of a critical third-party supplier (for example, a payroll or shift-management provider).
- Wider public emergency affecting staff, workers or client sites (for example, severe weather or public health incident).

Business-Critical Functions

The functions Lilac Alliance treats as business-critical, in priority order, are:

1. Worker safety checks and shift confirmation for placed workers already on assignment.
2. Payroll processing, to ensure placed workers are paid on time.
3. Client communication, to keep client sites informed of any service impact.
4. Candidate sourcing and placement activity.
5. Back-office administration and reporting.

Key Systems and Data

Lilac Alliance relies on cloud-based platforms for shift management (Plan Day) and for sourcing workers through client procurement portals, including Commensura, Florence and Matrix. As these are cloud-hosted, core operational data remains accessible from any internet-connected location, reducing our reliance on any single office location.

Data backups for locally held records are taken regularly, and access credentials for all business-critical systems are held securely by more than one member of the management team, to avoid a single point of failure.

Response Actions

1. Identify: The person who becomes aware of a disruptive incident notifies a Director immediately.
2. Assess: The Director assesses the scale and likely duration of the disruption, and identifies which business-critical functions are affected.
3. Activate: Where necessary, the Director activates remote working arrangements, redirects phone lines, and notifies staff of revised arrangements.
4. Communicate: Consultants contact any client sites or placed workers affected, to confirm continuity of service or agree interim arrangements.
5. Maintain critical functions: Priority is given to worker safety checks and payroll processing, using remote access to cloud-based systems where office access is unavailable.
6. Recover: Once the disruption is resolved, the Director confirms a return to normal operations and reviews whether any follow-up action or improvement to this plan is required.

Remote Working Arrangements

Because our core systems are cloud-based, staff are able to work remotely using a laptop and internet connection if Head Office premises become unavailable. Staff are encouraged to ensure they can access key systems from home as part of routine good practice, not only during a disruptive incident.

Communication Plan

In the event of a disruption affecting our ability to deliver services, the Director will ensure that affected clients are contacted directly by phone or email at the earliest opportunity, and that placed workers are contacted regarding any impact on shifts, timesheets or payroll. Where a disruption is expected to last more than one working day, clients will be given a realistic

timeframe for resolution and a single point of contact for the duration.

Responsibility For This Plan

Ultimate responsibility for this plan rests with the Company's leadership team. Simon Goddard has primary day-to-day responsibility for maintaining this plan, ensuring staff are aware of it, and leading the response to any disruptive incident.

Testing and Review

This plan is reviewed at least annually, and sooner following any disruptive incident or significant change to our systems, premises or key suppliers. Where practical, key contact details and system access arrangements are checked as part of this review to confirm they remain current.