BCP

1. **Purpose and Scope**

Define what the plan covers:

- Core business operations (production, sales, dispatch, finance, comms)
- Locations (e.g. warehouse, office, remote operations)
- Critical systems (ERP, MaticTrack, FreePBX, n8n, Graphy, printers, servers)
- Key suppliers and dependencies (power, internet, courier, substrates)

---

2. **Business Impact Analysis (BIA)**

Identify and rank what actually breaks the business if lost:

Function	Max Tolerable Downtime	Dependencies	Impact if Lost
Print production	24h	Colorado, Zünd, RIP PCs	Revenue halt
ERP / MaticTrack	8h	Database, backups, server	Dispatch paralysis
Customer comms	4h	FreePBX, WhatsApp, email	Lost orders
Payments / Banking	24h	Internet, bank access	Cashflow freeze
Premises access	48h	Building, power	Operational stop

---

3. **Risk Assessment**

List threats and the level of disruption they’d cause:

- Fire/flood (site loss)
- Cyber attack / ransomware
- Power or internet outage
- Staff absence (illness, strike, quarantine)
- Supplier failure
- Hardware failure
- Data corruption

- Reputational incident (social or customer backlash)

---

4. **Continuity Strategies**

How each critical function will be maintained:

- **IT & Data:** Full daily backups (local + cloud), tested quarterly; mirrored server or hot-swap VM ready.
- **Communications:** Secondary internet connection, mobile hotspot failover; Rocket.Chat accessible via mobile.
- **Premises:** Temporary production site agreement or pre-arranged outsource network.
- **Staffing:** Cross-training matrix; remote access policies; leadership succession list.
- **Suppliers:** Dual-supplier list for key materials; emergency courier options.

---

5. **Incident Response Procedure**

Step-by-step response to an event:

1. **Detection & Assessment** – who identifies the problem and how it’s logged.
2. **Activation** – who decides to trigger the plan.
3. **Internal Communication** – key staff WhatsApp group, SMS broadcast.
4. **External Communication** – message templates for customers, suppliers, press.
5. **Recovery Actions** – restore data, re-route calls, re-start production.
6. **Post-Incident Review** – what failed, what changes are needed.

---

6. **Roles and Responsibilities**

Define a chain of command:

- **Incident Lead:** Robert McCombe
- **Deputy Lead:** Kelly Power
- **IT & Systems:** Robert McCombe
- **Communications:** Robert McCOmbe
- **Safety & Facilities:** Richard McCombe

Include personal mobiles, secondary emails, and home working access details.

---

7. **Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs)**

Be specific:

- ERP: RTO 8h, RPO 1h
- Email/Comms: RTO 2h, RPO 0h (live failover)
- Print Production: RTO 24h, RPO N/A
- Accounting: RTO 48h, RPO 24h

---

8. **Testing & Maintenance**

- Simulate a disaster every 6–12 months.
- Review after any incident or major system change.
- Document every test result and update gaps.

Revision #1
Created 12 November 2025 10:43:49 by Admin
Updated 12 November 2025 10:45:00 by Admin