Green Park House

London, W1J 8LQ

MARCENA CAPITAL LTD | OPERATIONAL RESILIENCE & COMPLIANCE

Business Continuity Plan (BCP)

DOCUMENT GOVERNANCE

Plan Owner & Approver: Dhruv Sharma (CEO)

Deputy Invoker & Coordinator: Lucy Morrisey (Managing Director)

Regulatory Framework: FCA SYSC 4.1, SYSC 15A, SUP 15.3

Review Cycle: Quarterly Review / Annual Full Test

PREMISES & VERSION CONTROL | 2026

Primary Office: 15 Stratton Street, London, W1J 8LQ

Fallback Site: 210 Euston Road, London, NW1 2BE

Document Version: v2.0 (2026 Annual Review)

Classification: Internal & Regulatory Compliance

1. Purpose and Scope

The purpose of this Business Continuity Plan (**"BCP"**) is to ensure Marcena Capital Ltd (**"Marcena Capital"**) can continue operating or recover within an acceptable timeframe in the event of a critical incident or operational disruption, and to meet the Financial Conduct Authority's (**"FCA"**) expectations under **SYSC 4.1** and, where applicable, the operational resilience rules in **SYSC 15A** regarding continuity of regulated activities, protection of client and investor interests, and market integrity.

The scope of this document is to establish:

- The critical operational scenarios that require Marcena Capital to invoke the BCP.
- The Important Business Services that must be protected, together with the maximum tolerable level of disruption (impact tolerance) for each.
- The governance structure, mitigating actions, and recovery strategies required to restore normal business operations rapidly and safely.

1.1 In-Scope Scenarios

- **Natural and environmental disasters:** flooding, severe weather events, or public health emergencies (epidemics/pandemics).
- **Wilful or malicious disruption:** terrorism, civil disorder, internal or external strike action/work stoppage, cyberattack, ransomware, unauthorised system intrusion, or arson.
- **Accidental or infrastructure damage:** power outage, gas leaks, fire, building structural damage, or heating, ventilation, and air conditioning (HVAC) failure affecting primary premises.
- **Third-party and supply chain disruption:** failure or service degradation of a critical third-party provider (direct or indirect) to deliver agreed service levels.
- **Loss of key personnel:** incapacity, sudden departure, or unavailability of the CEO or other senior individuals holding essential institutional knowledge or invocation authority.

2. Important Business Services and Business Impact Analysis (BIA)

To prioritise recovery actions effectively, Marcena Capital identifies the Important Business Services whose disruption would pose a risk of intolerable harm to clients, limited partners (LPs), general partners (GPs), or market

counterparties, along with the Recovery Time Objective (**RTO**) and Recovery Point Objective (**RPO**) for each. This Business Impact Analysis is reviewed and formally re-approved by the CEO at least annually or following any material change to Marcena Capital's business model.

Important Business Service	Impact on Clients / LPs / GPs	Recovery Time Objective (RTO)	Recovery Point Objective (RPO)	Service Owner
Client / LP / GP Communications (Telephony, Email, Portal)	Duty of care, fiduciary transparency, and timely counterparty reassurance during disruption.	4 hours (initial contact via out-of-band mobile/email if primary portal is unavailable)	1 hour (for electronic messages and portal logs)	Dhruv Sharma (CEO)
Access to Core IT Systems and Cloud Data (via OVHcloud)	Underpins all investment, reporting, compliance, and operational workflows.	8 hours	1 hour (maximum data loss window)	Lucy Morrisey (MD)
LP / GP Investor Reporting and Capital Calls	Contractual LPA commitments, capital deployment schedules, and investor trust.	24 hours	1 hour (cloud system data) / End of prior business day (offline working files)	Dhruv Sharma (CEO)
Deal Execution and Portfolio Company Support	Time-sensitive transactions, financing milestones, and board governance obligations.	48 hours	1 hour (cloud system data) / End of prior business day (offline working files)	Dhruv Sharma (CEO)
Regulatory Reporting to the FCA & Statutory Filings	Compliance with statutory and FCA Handbook obligations (SUP 15 / GABRIEL / RegData).	Within statutory deadline (minimum 24 hours' advance notice to FCA if delayed)	1 hour (underlying compliance records)	Dhruv Sharma (CEO)
Payroll and Staff Welfare Administration	Employee wellbeing, contractual obligations, and statutory payroll compliance.	5 business days	End of prior payroll cycle	Lucy Morrisey (MD)

3. Responsibilities and Governance

Clear accountability is maintained to ensure rapid decision-making during an operational incident:

BCP Role	Designated Individual	Core Responsibilities
BCP Owner & Primary Invoker	Dhruv Sharma (Chief Executive Officer)	Overall ownership of the BCP; sole authority to approve new versions; primary authority to invoke the BCP; leads regulatory notifications (FCA/ICO) and key LP/GP communications.
Deputy Invoker	Lucy Morrisey (Managing Director)	Authorised to invoke the BCP if the CEO is unreachable or personally incapacitated by the incident for more than 1 hour; assumes overall incident command in the CEO's absence.
Business Continuity Coordinator	Lucy Morrisey (Managing Director)	Maintains the register of critical third-party contacts (Appendix A), executes the first-hour invocation checklist, coordinates the incident conference bridge, and logs actions for the post-incident review.

All Staff & Representatives	All Marcena Capital Personnel	Maintain familiarity with their responsibilities under the BCP, adhere to remote-working and information security protocols, and remain reachable via secondary communication channels (SMS / WhatsApp).

4. Plan Invocation

The BCP will be formally invoked by the CEO, or by the Deputy Invoker if the CEO is unreachable within 1 hour, where one or more in-scope scenarios cause any of the following triggers:

- Important Business Services provided by Marcena Capital to its clients, LPs, or GPs are materially disrupted or unavailable.
- Marcena Capital's primary premises at **15 Stratton Street, London, W1J 8LQ** become wholly or partially inaccessible or unsafe.
- Personnel lose access to core cloud IT systems, data repositories, or primary communications.
- A critical third-party supplier fails to deliver services within agreed service levels or experiences a security compromise.
- A severe incident at an indirect counterparty or infrastructure provider materially affects Marcena Capital or its clients.

4.1 First-Hour Invocation Checklist

1. **Confirm Scenario & Severity:** Assess the operational impact against the BIA impact tolerances and RTO/RPO metrics in Section 2.
2. **Activate Communications Bridge:** The Business Continuity Coordinator convenes the emergency stakeholder bridge (Section 6.2) and accounts for all personnel.
3. **Execute Recovery Strategy:** Initiate the relevant operational recovery workstream under Section 5 (Premises, IT/Cyber, Personnel, or Staff Welfare).
4. **Assess Regulatory Notification Obligations:** Evaluate whether immediate or preliminary notification is required to the FCA (under Principle 11 / SUP 15.3) or the ICO (within 72 hours for a qualifying personal data breach).
5. **Maintain Incident Log:** Record the incident start time, key decisions taken, systems affected, and personnel involved for the post-incident report (Appendix D).

5. Recovery Strategies

5.1 Loss of Premises

If Marcena Capital's primary office at **15 Stratton Street, London, W1J 8LQ** is unavailable or inaccessible, all personnel will transition immediately to secure remote working using encrypted company laptops and cloud-hosted systems (via OVHcloud). Where a physical meeting or operational base is required, **210 Euston Road, London, NW1 2BE** is designated as the temporary fallback location.

5.2 Loss of IT Systems / Cyber Incident

If core IT systems or data are disrupted by a cyberattack, ransomware event, unauthorised intrusion, or technical failure:

- **Containment & Isolation:** Immediately isolate affected systems and revoke compromised credentials in coordination with OVHcloud's incident response team and IT support.
- **Forensic Preservation:** Preserve system logs, audit trails, and forensic evidence prior to remediation.

- **Backup Verification:** Assess data integrity and verify the last clean, uncompromised backup point against the 1-hour RPO target in Section 2. Systems must not be restored from backup until the root cause and attack vector are fully contained.
- **Regulatory & Data Breach Notification:** Determine whether personal data or confidential client data has been compromised. Where a personal data breach poses a risk to individuals' rights and freedoms, notify the Information Commissioner's Office (**ICO**) within the statutory **72-hour window** and notify affected data subjects where required. Notify the **FCA** without undue delay under Principle 11 / SUP 15.3.

5.3 Loss of Key Personnel

If the CEO or another individual holding critical institutional knowledge becomes incapacitated or unavailable, the Deputy Invoker (**Lucy Morrisey**) assumes invocation and operational authority. Continuity of LP/GP relationships, active transactions, and regulatory obligations is maintained using documented handover registers and transaction logs, which are refreshed quarterly.

5.4 Staff Welfare and Life Safety

During any incident affecting physical safety or health (including fire, civil disorder, extreme weather, or public health emergencies), the immediate priority is life safety and staff welfare. This includes immediate headcount verification, compliance with building evacuation procedures, and continuity of payroll and employee assistance arrangements. Staff safety takes absolute precedence over commercial service recovery.

6. Communications

6.1 Critical Third-Party Suppliers

Marcena Capital maintains a Critical Supplier Register (Appendix A) containing:

- Primary and 24/7 emergency escalation contact details (including mobile numbers independent of landline telephony) and the designated Marcena Capital individuals authorised to engage each supplier during a BCP invocation.
- Copies or summaries of each critical supplier's own business continuity and disaster recovery assurances.

Marcena Capital's primary technology infrastructure provider is **OVHcloud (OVH Cloud Solutions)**, which hosts core systems and data repositories supporting the Important Business Services in Section 2 (excluding the public corporate website, which is classified as non-critical). The Critical Supplier Register in Appendix A also encompasses key professional and operational counterparties, including compliance advisers, legal counsel, auditors, and banking/custody institutions.

6.2 Internal Communications

- **Primary Channel:** Microsoft Teams emergency conference bridge for all stakeholders to confirm headcount, share situational updates, and coordinate mitigation steps.
- **Secondary / Backup Conferencing:** If Microsoft Teams is unavailable, stakeholders convene via the designated Zoom fallback bridge or mobile teleconference.
- **On-Site & Remote Coordination:** Where premises remain safe and operational, on-site personnel coordinate in person while remote personnel join via Microsoft Teams (or Zoom backup).
- **Out-of-Band Fallback:** If both corporate email and internet conferencing are unavailable, internal communications fall back immediately to direct mobile voice calls, SMS text messaging, and the closed Marcena Capital WhatsApp incident group (Appendix B).

6.3 External & Regulatory Communications

- **Direct Client, LP, and GP Outreach:** In keeping with Marcena Capital's institutional operating model, affected clients, LPs, GPs, and corporate finance counterparties are contacted directly by the CEO or Managing Director via email, telephone, or secure investor portal notices within the 4-hour initial contact target.

- **Inbound Telephony & Email Routing:** Where primary office telephony is disrupted, inbound calls are diverted to designated mobile numbers or answered with an institutional voicemail notice providing alternative contact details and expected resolution timeframes.
- **Corporate Website & Public Channels:** Where appropriate for a prolonged infrastructure outage, a concise status notice may be placed on www.marcenacapital.com. Operational incident details are not broadcast on public social media unless specifically approved by the CEO.
- **Regulatory Notification (FCA & ICO):** The CEO (or Deputy Invoker in the CEO's absence) will assess without undue delay whether the incident constitutes a notifiable event under **FCA Principle 11 / SUP 15.3** or the **UK GDPR / Data Protection Act 2018**. Where required, Marcena Capital will notify the FCA and/or ICO promptly, detailing the nature of the incident, impact on clients, remedial actions taken, and estimated resolution time (logged in Appendix E).

7. Testing, Review, and Continuous Improvement

- **Quarterly Review & Change Management:** This BCP is reviewed quarterly and reassessed whenever a new business service, system, or critical third-party supplier is onboarded or materially modified.
- **Annual Full Desktop & Operational Exercise:** A comprehensive test of the BCP—covering plan invocation, internal fallback communications, remote system recovery, and third-party escalation—is conducted at least annually, supplemented by quarterly scenario walk-throughs.
- **Remote & Alternate Site Verification:** Periodic practical tests are conducted to verify that remote working access via OVHcloud and out-of-band communication trees operate within target RTOs.
- **Post-Test & Post-Incident Action Tracking:** Following every test or live invocation, the Business Continuity Coordinator completes a Post-Incident / Test Report (Appendix D) evaluating performance against the Section 2 RTO/RPO targets and assigning owned remediation actions with binding due dates.

8. Document Governance and Version History

This BCP is owned by the Chief Executive Officer (**Dhruv Sharma**). Authorised stakeholders may propose amendments to reflect operational or regulatory updates; however, no revised version becomes effective until formally approved by the CEO and recorded in the Version History log below.

Version	Effective Date	Author / Reviewer	Summary of Changes	Approved By
v1.0	2025	Lucy Morrisey (MD)	Legacy Business Continuity Plan adoption.	Dhruv Sharma (CEO)
v2.0	November 2026	Lucy Morrisey (MD)	2026 annual review: aligned RTO/RPO metrics, clarified Deputy Invoker & Coordinator roles, updated institutional communication protocols, and added structured appendices.	Dhruv Sharma (CEO)

9. Appendices & Operational Registers

Appendix A: Critical Supplier Contact Register

Supplier Name	Service Provided	24/7 Incident / Support Contact	Marcena Authorised Contact	BCP Assurance on File
OVHcloud (OVH Cloud Solutions)	Core cloud infrastructure, virtual desktops & data	OVHcloud Enterprise Support Portal /	Lucy Morrisey (MD) Dhruv Sharma	Yes (ISO 27001 / SOC 2 & SLA)

	hosting	Emergency Escalation Line	(CEO)	
Capital Alliance Partners Ltd	Data protection & compliance administration support	Arnaud van der Wyck 46 Great Marlborough St, W1F 7JW	Dhruv Sharma (CEO) Lucy Morrisey (MD)	Yes
Microsoft / Zoom	Cloud collaboration & emergency conference bridge	Service Health Dashboard / Admin Portal	Lucy Morrisey (MD)	Yes (Cloud SLA)

Appendix B: Emergency Staff Contact Tree & Fallback Channels

- **Primary Emergency Bridge:** Microsoft Teams Incident Channel (invoked by Business Continuity Coordinator).
- **Out-of-Band Messaging:** Marcena Capital Closed WhatsApp Group & SMS Broadcast List (maintained on encrypted company devices by Lucy Morrisey).
- **Key Invocation Contacts:** Dhruv Sharma (CEO – Primary Invoker) and Lucy Morrisey (Managing Director – Deputy Invoker & Business Continuity Coordinator).

Appendix C: Alternate Site & Remote Working Access Procedures

- **Primary Registered Office:** 15 Stratton Street, London, W1J 8LQ, United Kingdom.
- **Designated Fallback Physical Office:** 210 Euston Road, London, NW1 2BE, United Kingdom.
- **Remote Access Protocol:** All personnel authenticate to OVHcloud hosted environments via multi-factor authentication (MFA) over encrypted connections using company-issued laptops.

Appendix D: Post-Incident & BCP Testing Report Log

Each BCP desktop test or live invocation must record: (1) Date/Time and Scenario; (2) Invoker and Participating Personnel; (3) Actual Recovery Times vs. Section 2 RTO/RPO Targets; (4) Root Cause Analysis; and (5) Remediation Actions, Owners, and Target Completion Dates.

Appendix E: Regulatory Notification Escalation Summary (FCA & ICO)

Regulator	Applicable Rule / Trigger	Statutory Timeframe	Decision Owner & Contact Method
Financial Conduct Authority (FCA)	Principle 11 / SUP 15.3 (material operational disruption or cyber incident)	Immediate / Without undue delay upon confirming materiality	Dhruv Sharma (CEO) or Lucy Morrisey (Deputy Invoker) via FCA Connect / Supervisory Contact
Information Commissioner's Office (ICO)	UK GDPR Art. 33 (personal data breach posing risk to individuals)	Within 72 hours of becoming aware of the breach	Dhruv Sharma (CEO) / Data Protection Contact via https://ico.org.uk (0303 123 1113)