

# QUALITY & SERVICE DELIVERY POLICY

## BLUE MOON MTC LTDA

Corporate Governance & Compliance Pack 2026

|                |                                                                             |
|----------------|-----------------------------------------------------------------------------|
| Document ID    | BM-COMP-006                                                                 |
| Version        | 1.0                                                                         |
| Effective Date | 01 October 2026                                                             |
| Document Owner | Management - BLUE MOON MTC LTDA                                             |
| Approved By    | Managing Director / Sole Shareholder                                        |
| Review Cycle   | Annual, or earlier upon material service, customer, risk or business change |

### 1. Purpose and Quality Commitment

BLUE MOON MTC LTDA ("BLUE MOON" or "the Company") is committed to delivering network, infrastructure and security services with professional care, technical discipline, traceability and accountability.

This Policy establishes minimum quality and service-delivery requirements from initial scope through implementation, validation, evidence, handover and post-change support where applicable. Detailed technical procedures may define additional controls for specific technologies, customers or services.

### 2. Scope

This Policy applies to BLUE MOON management, employees, contractors and authorized subcontractors involved in technical projects, implementations, changes, migrations, upgrades, network-security activities, firewall services, segmentation, secure connectivity, B2B VPNs, troubleshooting and related service delivery.

Customer-specific procedures, change-management requirements, maintenance windows, approval flows and evidence requirements must also be followed when applicable.

### 3. Service Delivery Principles

BLUE MOON service delivery is guided by the following principles:

- Perform only authorized work within an understood scope.
- Use personnel with competence appropriate to the assigned activity.
- Assess technical risk before material change.
- Preserve service availability and security through appropriate planning.
- Maintain a viable rollback or recovery approach when the change risk requires it.
- Validate outcomes rather than assuming successful implementation.
- Maintain accurate evidence and communicate material deviations.
- Protect customer information and access throughout the service lifecycle.
- Apply lessons learned and continuous improvement.

### 4. Scope and Requirements

Before technical work begins, BLUE MOON will seek to establish the objective, affected environment, expected outcome, responsibilities, relevant dependencies and customer requirements at a level proportionate to the work.

Ambiguous or materially incomplete requirements that could affect security, availability or implementation outcome must be clarified before execution where reasonably possible. BLUE MOON will not knowingly implement a material security or infrastructure change based solely on assumptions when required information or authorization is missing.

## 5. Authorization and Change Control

Changes to customer environments must be performed only with appropriate authorization. Where the customer operates a formal change-management process, BLUE MOON will follow the applicable ticket, approval, maintenance-window and implementation requirements.

Emergency changes may use an expedited process when authorized by the customer, but urgency does not eliminate the need for accountability, evidence and post-change review.

## 6. Planning and Risk Assessment

Material technical changes must be planned at a level appropriate to their complexity and risk. Planning may include affected devices and services, dependencies, implementation sequence, expected impact, security considerations, validation criteria, communication requirements and rollback or recovery actions.

Risks that could materially affect customer security, connectivity, production availability or data must be raised before implementation when identified.

## 7. Pre-Implementation Checks

Where relevant, BLUE MOON will perform or confirm pre-implementation checks sufficient to establish the initial state and readiness for the planned work.

Pre-checks may include device or service health, high-availability state, routing, interfaces, VPN status, policy deployment state, relevant traffic or logging, configuration availability, dependencies, backups and other conditions appropriate to the planned change.

The exact pre-check is determined by the technology, scope, customer procedure and risk; this Policy does not require unnecessary checks unrelated to the activity.

## 8. Implementation Standards

Technical implementation must follow the approved scope and applicable procedure. Personnel must avoid unrelated changes and must stop or escalate when unexpected conditions materially alter the risk or invalidate the approved plan.

Configuration changes should be performed in a controlled sequence that supports validation and recovery. Credentials, customer data and technical evidence must remain protected throughout implementation.

## 9. Firewall and Network Security Changes

Firewall rules, access-control policies, NAT, routing, VPNs, segmentation, security zones and related controls must be implemented according to the authorized requirement and customer security process.

Rule changes should apply the principle of least privilege and should avoid unnecessarily broad source, destination, service or application access where the approved requirement permits a more specific control.

Temporary access, temporary rules and time-limited exceptions must be identified and managed so that they can be reviewed or removed when their authorized purpose expires.

## 10. Rollback and Recovery

For material changes where rollback is technically applicable, the implementation plan must define a reasonable method to restore or recover the prior working state if acceptance criteria are not met or material impact occurs.

A rollback decision must consider customer authorization, current system state, business impact and the risk of continuing versus reverting. Rollback mechanisms must not be assumed to be available without verification where their absence could materially increase change risk.

## 11. Validation and Post-Implementation Checks

Completion of implementation does not by itself constitute successful delivery. BLUE MOON will perform or support post-implementation validation appropriate to the change.

Validation may include policy deployment status, connectivity, expected traffic behavior, routing, VPN establishment, service reachability, high-availability health, logs, security events and other acceptance criteria relevant to the scope.

Material unexpected results must be investigated, corrected, rolled back or formally accepted by the appropriate customer authority.

## **12. Evidence and Technical Records**

BLUE MOON will maintain service evidence proportionate to the engagement and customer requirements. Evidence may include change records, approvals, implementation notes, pre/post-check results, configuration references, timestamps, screenshots, logs, validation results and issue records.

Evidence must be accurate, attributable where practical, protected according to information sensitivity and retained only for legitimate business, contractual, security or audit purposes.

## **13. Testing and Acceptance**

Where a service includes defined testing or acceptance criteria, BLUE MOON will evaluate the implemented result against those criteria before considering the activity complete.

Customer acceptance may be explicit or may follow the customer's established process. Open issues, limitations or deviations that materially affect the agreed outcome must be communicated.

## **14. Hypercare and Post-Change Support**

Hypercare or enhanced post-change monitoring may be provided when included in the service scope, required by the customer or appropriate to the risk and criticality of the change.

Where hypercare applies, the expected duration, support model, escalation path and monitoring responsibilities should be understood by the relevant parties. Hypercare is not automatically required for every service or change.

## **15. Incident and Service Issue Escalation**

Material incidents, outages, security events or implementation errors identified during service delivery must be escalated promptly through the applicable BLUE MOON and customer channels.

Personnel must not conceal mistakes or alter evidence to create the appearance of successful delivery. Timely disclosure and technically responsible remediation take priority over avoiding accountability.

## **16. Communication**

Service communications must be clear, professional and proportionate to the activity. Material changes in scope, risk, schedule, impact or outcome must be communicated to the appropriate stakeholders.

Technical information provided to customers must distinguish confirmed facts from assumptions or items still under investigation.

## **17. Technical Competence**

BLUE MOON will assign work to personnel whose knowledge and experience are appropriate to the technology and risk involved. Where additional expertise is required, the Company may use qualified internal resources, approved subcontractors or vendor support as appropriate.

Professional certifications may support evidence of competence but do not replace the obligation to understand the specific environment, scope and customer procedure.

## **18. Customer Security and Confidentiality**

All service delivery must comply with BM-COMP-004 Information Security Policy and BM-COMP-005 Data Privacy & Confidentiality Policy.

Customer configurations, network information, logs, credentials, diagrams and technical evidence must be accessed and retained only as necessary for the authorized work.

## 19. Subcontractors and Third Parties

Subcontractors involved in service delivery must be appropriately authorized, competent for the assigned work and subject to relevant confidentiality, security and quality requirements.

Use of a subcontractor does not remove BLUE MOON's responsibility to manage the quality and scope of the service it has contractually undertaken to provide.

## 20. Nonconformity and Corrective Action

When a material service failure, recurring defect or process deviation is identified, BLUE MOON will assess the cause and determine proportionate corrective action.

Corrective action may include technical remediation, procedure adjustment, additional validation, training, access changes, customer communication or other measures appropriate to prevent recurrence.

## 21. Continuous Improvement

BLUE MOON will use relevant service outcomes, incidents, customer feedback, technical lessons learned and changes in technology or threat conditions to improve its delivery methods and controls.

Process improvement should remain proportionate to Company scale and risk and should focus on measurable operational value rather than unnecessary bureaucracy.

## 22. Customer-Specific Requirements

Where a customer establishes mandatory technical, quality, security, change or documentation procedures, BLUE MOON personnel assigned to that engagement must follow those applicable requirements.

BLUE MOON internal policy does not override a customer's authority over its own environment. Conflicts between requirements must be escalated before proceeding when they could materially affect delivery.

## 23. Metrics and Management Review

BLUE MOON management may use proportionate service metrics to evaluate quality and improvement needs. Depending on the service model, measures may include successful change completion, rollback events, incidents, recurring issues, response performance, customer feedback and completion of required evidence.

Metrics will be introduced and expanded according to operational maturity and customer requirements rather than reported as established measurements before reliable data exists.

## 24. Responsibility and Governance

Overall responsibility for this Policy rests with BLUE MOON management. The Managing Director is accountable for approving the Policy, maintaining an appropriate service-delivery framework, reviewing material quality risks and ensuring that corrective actions are addressed.

Technical personnel are responsible for working within authorized scope, following applicable procedures, maintaining appropriate evidence and escalating material risks, deviations and incidents.

## 25. Related Controlled Documents

This Policy forms part of BLUE MOON's Corporate Governance & Compliance framework and should be read together with:

- BM-COMP-001 Code of Business Conduct & Ethics.
- BM-COMP-004 Information Security Policy.
- BM-COMP-005 Data Privacy & Confidentiality Policy.
- Change Management Procedure.
- Incident Response & Security Incident Management Procedure.
- Access Control & Privileged Access Standard.
- Business Continuity & Disaster Recovery Plan.
- Supplier & Subcontractor Standards.

## 26. Review Cycle

This Policy will be reviewed at least annually and earlier following a material service failure, significant change in service portfolio, material customer requirement, applicable regulatory change or other relevant change in operational risk.

## 27. Approval

This Policy becomes effective upon approval by BLUE MOON MTC LTDA management and remains in force until superseded by a later approved version.

Approved by:

---

**LUCIANO IZAIAS MAGALHAES TYE**

Managing Director / Sole Shareholder

**BLUE MOON MTC LTDA**