

INFORMATION SECURITY POLICY

BLUE MOON MTC LTDA

Corporate Governance & Compliance Pack 2026

Document ID	BM-COMP-004
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 security, legal, contractual or business change

1. Purpose and Security Commitment

BLUE MOON MTC LTDA ("BLUE MOON" or "the Company") is committed to protecting the confidentiality, integrity and availability of Company and customer information, systems and technology resources. Information security is a core business responsibility and an essential element of the network and security services delivered by BLUE MOON.

This Policy establishes the Company's minimum information-security requirements. Supporting standards, procedures and technical controls may define more detailed implementation requirements.

2. Scope

This Policy applies to BLUE MOON management, employees, contractors, subcontractors where applicable, Company-owned or Company-managed devices, cloud services, accounts, applications, networks, information repositories and any authorized access to customer systems or data.

Customer-specific security requirements and contractual controls must also be followed when they apply to an engagement.

3. Security Principles

BLUE MOON applies security controls proportionate to business risk, customer requirements and the sensitivity of information. The following principles guide the security program:

- Least privilege and need-to-know access.
- Strong identity verification and individual accountability.
- Defense in depth and secure configuration.
- Separation of customer and Company information where appropriate.
- Controlled and auditable technical change.
- Prompt identification, escalation and containment of security events.
- Protection of information throughout its lifecycle.
- Continuous improvement based on risk, incidents, technology changes and customer requirements.

4. Information Classification and Handling

Information must be handled according to its sensitivity and contractual requirements. BLUE MOON recognizes, at minimum, public information, internal business information, confidential information and highly sensitive security or customer information.

Customer network diagrams, firewall configurations, access-control policies, credentials, security logs, vulnerability information, technical evidence and other security-sensitive data must be treated as confidential or more restrictive when required by the customer.

Sensitive information must not be transferred to unauthorized personal accounts, consumer storage services, unapproved messaging channels or other locations outside the authorized business purpose.

5. Identity and Access Management

Access to BLUE MOON and customer resources must be individually attributable, authorized and limited to the minimum privileges required for the assigned role or task.

- Shared user accounts should be avoided where individual accounts are technically available.
- Multi-factor authentication must be used for privileged, administrative, remote and cloud access where supported and must be enabled for critical Company services.
- Access rights must be reviewed when responsibilities change and removed promptly when access is no longer required.
- Authentication credentials must not be shared, reused inappropriately or stored in insecure locations.
- Administrative access must be separated from ordinary user activity where practical and appropriate to the environment.

6. Privileged Access and Customer Environments

Privileged access to customer firewalls, security platforms, network infrastructure, management systems and related services carries heightened responsibility. Such access may only be used for authorized work within the approved scope.

BLUE MOON personnel must follow the customer's access, change, logging, maintenance-window and approval processes. Privileged credentials, API tokens, certificates, recovery codes and similar secrets must receive appropriate protection.

Access to a customer environment must never be used to inspect, modify, extract or retain information unrelated to the authorized technical purpose.

7. Endpoint and Device Security

Devices used to access BLUE MOON or customer information must be appropriately secured for their intended use. Security controls will be applied according to risk and technical capability and should include supported operating systems, timely security updates, endpoint protection, screen locking, secure authentication and encryption for portable devices storing sensitive information.

Unmanaged or personally owned devices must not be used for customer access when prohibited by customer requirements or when adequate security controls cannot be applied.

8. Network and Remote Access Security

Remote connectivity to Company or customer resources must use authorized secure methods. Where BLUE MOON controls the environment, remote administrative access must use encrypted protocols and appropriate authentication.

Network exposure must be minimized to required services. Firewalls, access controls, VPNs, secure remote-access mechanisms and segmentation should be applied according to the risk and architecture of the environment.

Customer B2B VPNs and other trusted connectivity must be implemented only under authorized designs and with documented technical parameters and ownership.

9. Encryption and Secrets

Sensitive information must be protected in transit using appropriate encrypted protocols where technically supported and required by risk or contract. Sensitive data stored on portable devices or other higher-risk locations must be protected through suitable encryption or equivalent controls.

Passwords, private keys, API secrets, tokens and certificates must not be embedded in public repositories, exposed in documentation without protection or transmitted through unauthorized channels.

10. Secure Configuration and Vulnerability Management

BLUE MOON will use secure configuration practices appropriate to the systems it manages. Unnecessary services, accounts and exposure should be removed or disabled where operationally feasible.

Security patches and known vulnerabilities must be assessed according to risk, exposure, vendor guidance, customer requirements and operational impact. Critical or actively exploited vulnerabilities affecting systems under BLUE MOON's control require prioritized assessment and remediation or documented risk treatment.

Customer-managed systems remain subject to the customer's authority and change processes; BLUE MOON will not make unauthorized remediation changes.

11. Firewall, Network Security and Change Management

Changes to firewall rules, network-security controls, routing, VPNs, segmentation or related customer infrastructure must be authorized and performed under the applicable change process.

Where relevant to the engagement, change activity should include a defined scope, implementation plan, validation, rollback considerations and evidence appropriate to the risk and customer procedure.

Temporary rules, emergency access and exceptions must be controlled and removed or reviewed when their authorized purpose expires. BLUE MOON will not bypass customer security controls to accelerate delivery.

12. Logging, Monitoring and Accountability

Security-relevant activity should be logged and monitored at a level appropriate to system risk, customer requirements and available platform capability. Logs used for operational or security evidence must be protected from unauthorized alteration.

Where BLUE MOON is responsible for monitoring, suspicious events and material anomalies must be evaluated and escalated according to the applicable incident or operational process.

13. Data Retention and Secure Disposal

BLUE MOON will retain Company and customer information only for legitimate business, legal, contractual, security or evidentiary purposes. Customer data must not be retained indefinitely merely for convenience.

When information or media is no longer required, it must be securely deleted, destroyed, returned or otherwise handled according to applicable contractual and legal requirements.

14. Backup and Recovery

Business-critical BLUE MOON information and systems must have backup or recovery measures proportionate to their importance and recoverability requirements. Backup copies containing sensitive information must receive appropriate access protection.

Recovery capability should be tested or otherwise validated at intervals appropriate to the system and business risk. Detailed continuity and recovery requirements are maintained in the Business Continuity framework.

15. Security Incident Management

Suspected or confirmed security incidents affecting BLUE MOON or customer information, credentials, systems or access must be reported promptly to BLUE MOON management and handled according to the applicable incident-management procedure.

Response actions may include containment, credential protection, evidence preservation, technical investigation, recovery, corrective action and customer notification when required by contract or law.

Personnel must not conceal material security mistakes or incidents. Timely escalation is required even when the full impact is not yet known.

16. Third-Party and Cloud Security

Third-party and cloud services that store, process or provide access to sensitive BLUE MOON or customer information must be selected and used with consideration of security, confidentiality, access control, data location where relevant, service reliability and contractual requirements.

Subcontractors requiring access to customer systems or information must be authorized and subject to appropriate confidentiality and security obligations.

17. Physical Security

Devices, documents and media containing sensitive information must be protected against unauthorized physical access, theft, loss and casual observation. Personnel working remotely or while traveling must take reasonable measures to protect screens, equipment and confidential conversations.

Loss or theft of a device containing or capable of accessing sensitive Company or customer information must be reported promptly.

18. Personnel Security and Awareness

Individuals with access to BLUE MOON or customer resources must understand their security responsibilities. Security awareness will be provided proportionate to role and risk, with additional guidance for privileged or customer-facing technical activities.

Access must be adjusted or revoked promptly when an individual changes role, leaves the Company or no longer requires the relevant system or customer access.

19. Privacy and Confidentiality

Information security controls must support BLUE MOON's privacy and confidentiality obligations. Personal data must be accessed and processed only for authorized purposes and protected according to applicable law and contractual requirements.

Detailed privacy and confidentiality requirements are maintained in a separate controlled policy.

20. Exceptions and Risk Acceptance

Exceptions to this Policy must not be informal. Where a requirement cannot reasonably be met, the exception must be evaluated based on risk, documented when material, limited in scope and duration where possible, and approved by BLUE MOON management or the applicable customer authority.

An exception approved by BLUE MOON cannot override a customer's mandatory security requirement without that customer's authorization.

21. Compliance, Review and Corrective Action

BLUE MOON may review compliance with this Policy through operational checks, access reviews, configuration review, incident analysis, customer assessments or other proportionate methods.

Material non-compliance must be corrected or formally risk-treated. Repeated or deliberate violations may result in access removal, contractual or disciplinary action, or other appropriate measures.

22. Responsibility and Governance

Overall responsibility for the BLUE MOON information-security framework rests with Company management. The Managing Director is accountable for approving this Policy, ensuring that proportionate security controls are established, reviewing material security risks and incidents, and assigning technical responsibilities as the Company grows.

Technical personnel are responsible for following authorized procedures, protecting credentials and information, maintaining appropriate evidence, and escalating security risks or incidents without undue delay.

23. Related Controlled Documents

This Policy is supported, or will be supported as the BLUE MOON security framework is implemented, by controlled documents including:

- Incident Response & Security Incident Management Procedure.
- Access Control & Privileged Access Standard.
- Change Management Procedure.
- Data Privacy & Confidentiality Policy.
- Business Continuity & Disaster Recovery Plan.
- Backup & Recovery Standard.
- Supplier & Subcontractor Security Requirements.
- Asset & Endpoint Security Standard.

24. Review Cycle

This Policy will be reviewed at least annually and earlier following a material security incident, significant change in services or technology, material customer requirement, applicable legal change or other change to the Company's security risk profile.

25. 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