INFORMATION MANAGEMENT & CYBERSECURITY POLICY

1. Introduction

Apex Coco operates an integrated ecosystem spanning manufacturing, procurement, warehousing, distribution, and digital customer portals. Our information and technology estate underpins day-to-day operations, innovation, and competitive differentiation. As our digital footprint grows across IT and operational technology (OT), safeguarding information assets and critical systems becomes essential to business resilience, stakeholder trust, and regulatory compliance. This Policy defines Apex Coco's management principles and governance expectations for information management and cybersecurity across all information and technology assets.

2. Scope and Applicability

This Policy applies to all individuals who access Apex Coco information or networks, including full-time employees, fixed-term employees, trainees and apprentices, contractors, consultants, interns, and temporary staff engaged via third parties. It also extends to subsidiary personnel, system vendors, outsourcing partners, and any entity processing Apex information under contract. The Policy covers all information, computing, and communications systems owned or licensed by Apex, including data in electronic and non-electronic forms, voice, images, and telemetry across offices, plants, warehouses, and remote work environments.

3. Objectives

The objectives of this Policy are to establish baseline requirements for a robust security posture; reduce exposure of Apex assets to threats; prevent unauthorized access, loss, alteration, or leakage of information; and foster cyber-safe, privacy-aware behavior across the workforce. Apex will uphold confidentiality, integrity, and availability of information and services, and will embed information management controls into processes, technologies, and third-party relationships.

4. Policy Commitment

Apex Coco will maintain a secure, reliable, and resilient environment to safeguard employees, business partners, and customers by implementing a defense-in-depth cybersecurity and information management framework aligned to recognized standards such as ISO/IEC 27001. Apex shall adopt and continually improve controls to protect critical infrastructure and information assets, ensuring confidentiality, integrity, and availability.

All Apex information and technology assets must conform to the policies and procedures outlined below.

4.a Policy Framework

The cybersecurity and information governance team shall issue policies, standards, and procedures that define responsibilities and segregation of duties. Standard Operating Procedures for security operations shall be documented and communicated. Roles and accountability will be assigned based on organizational needs and risk.

4.b Protection of Information Assets

All information assets—including hardware, software, data repositories, records, and documents—shall be protected to uphold confidentiality, integrity, and availability. Apex shall maintain an up-to-date inventory of information assets and apply appropriate safeguards. Intellectual property will be protected using suitable mechanisms and contractual controls.

4.c Protection of Critical Infrastructure Assets

Technology assets across IT and OT, including plant systems and IIoT components, shall be safeguarded to maintain control, availability, integrity, and confidentiality. Apex shall maintain a current inventory of technology assets and implement layered protections proportionate to business risk.

4.d Management of Customer and Personal Data

Customer information and personal data shall be collected, processed, stored, retained, and disposed of in accordance with applicable laws and Apex policies. Unless otherwise agreed contractually, customer data shall be managed under Apex's information security and privacy requirements, with privacy preserved throughout its lifecycle. Apex will define retention timelines, secondary use controls, and third-party disclosure practices and provide mechanisms for individuals or customers to manage their data preferences where applicable.

4.e Regulatory Compliance

Information and technology assets will be used in compliance with applicable laws, regulations, and sectoral guidance. The security team will maintain engagement with regulators, industry bodies, and threat-intelligence forums to monitor external changes.

Prepared By

Coco and Solar Energy Authorized Signatory

Approved By

When using third-party products and services, Apex shall respect and protect intellectual property rights and contractual obligations.

4.f External Engagements and Threat Intelligence

Apex will maintain relationships with relevant authorities, industry groups, and information-sharing forums to obtain threat intelligence and updates on emerging risks, and will incorporate such insights into its control environment.

4.g Acceptable Use

All users must use Apex information and technology assets responsibly, respect the rights of other users, protect system confidentiality and integrity, and comply with applicable laws and company policies. Acceptable use expectations shall be published and enforced.

4.h Information Governance in Projects

Security and privacy requirements shall be embedded into all new IT and OT projects from initiation through design and delivery. Project plans must evidence the incorporation of appropriate controls and will be subject to design reviews prior to deployment.

4.i Business Continuity and Backup

Business continuity planning shall be maintained for critical information and technology assets to enable timely recovery from adverse events. Backup strategies and recovery objectives shall be documented, tested, and integrated with information security requirements.

4.j Ownership of Information

Information residing on Apex information and technology assets that is not explicitly identified as belonging to another party shall be treated as Apex property. Ownership and stewardship roles shall be documented to ensure accountability for protection and quality.

4.k Information Classification, Labelling, and Secure Transfer

Information shall be classified and labelled by data owners according to Apex's classification scheme. Unclassified information shall be treated as Internal unless designated for public release. Transfers of information to external parties must use secure channels and be authorized in accordance with policy.

4.l Identity and Access Management

Identity lifecycle management shall control creation, modification, and revocation of access to information and technology assets. Access rights will be granted based on business need and security requirements and reviewed periodically for appropriateness.

4.m Authentication, Authorization, and Accounting

Only authorized individuals shall access Apex assets. Strong authentication will be required for access, authorization will be enforced according to policy rules, and access activities on critical assets shall be monitored and reviewed on a periodic basis.

4.n Use of Personally Owned Devices (BYOD)

Where personally owned devices interface with Apex information or systems, such devices must comply with Apex security requirements, including configuration, encryption, and monitoring controls, as applicable.

4.o Cyber Risk Management and Governance

Risk analysis shall be performed for projects and operations, and identified risks shall be addressed using appropriate technical and administrative controls. Residual risks shall be accepted through documented governance.

4.p Security in Supply Chain and Supplier Relationships

Supplier agreements shall include security requirements commensurate with the nature of the relationship, data sensitivity, and service criticality. Cybersecurity risks in the supply chain shall be addressed in technical specifications and contracts, and supplier services shall be monitored and reviewed for compliance.

4.q Cloud Services Security

Security and privacy requirements shall be incorporated during acquisition, onboarding, operation, and exit from cloud services, covering data residency, encryption, identity management, logging, and incident handling.

4.r Incident Management

Information security incidents shall be triaged and managed through a formal process to minimize business impact and protect assets, processes, and reputation. Evidence shall be collected and preserved in line with legal requirements. Lessons learned will inform continuous improvement of controls.

4.s Audits and Assessments

Independent reviews of Apex's security implementation across critical IT and OT systems shall be conducted at least annually to verify effectiveness and alignment with industry standards. Periodic third-party audits will validate compliance with privacy and regulatory requirements, and internal audits will assess adherence to policies and identify opportunities for improvement.

4.t Physical Security of Information and Technology Assets

Information and technology assets shall be protected from physical and environmental threats. Critical assets will be housed in secure locations with access controls and monitoring to deter and detect unauthorized physical access. Asset returns at off-boarding and secure disposal at end-of-life shall be enforced.

4.u HR Hiring and Contracting Controls

Pre-employment or onboarding checks shall be performed as permitted by law. Employment agreements shall include confidentiality obligations that survive termination. Contractors and third-party personnel shall be bound by equivalent obligations via contract.

4.v Training and Awareness

Apex will continually improve its information management and cybersecurity program and will communicate this Policy to all personnel. Mandatory training and awareness shall cover acceptable use, classification, access control, incident reporting, privacy, and digital conduct.

4.w Monitoring and Privacy Governance

Activities on or through Apex information assets may be monitored for security and business purposes in accordance with law and policy. The cybersecurity function shall oversee data protection and privacy matters in coordination with relevant stakeholders.

4.x Incident Reporting

Employees and partners must promptly report events that could adversely affect Apex's security posture using prescribed channels. Timely reporting enables swift containment and remediation.

Prepared By

Approved By

4.y Disciplinary Measures

Violations of security policies or procedures may result in disciplinary action under Apex's HR policies, up to and including termination of employment or contract, depending on severity and circumstances.

4.z Technical Controls

Security and stakeholder teams shall design, implement, and operate technical controls appropriate to the risk profile of information and technology assets, including but not limited to endpoint protection, network security, encryption, logging, vulnerability management, and secure configuration.

5. Exceptions and Limitations

Exceptions may be granted where risks are mitigated through compensating controls or where the residual risk is low and business justifications are documented. Exceptions must comply with minimum security requirements and shall not conflict with legal or regulatory obligations.

6. Policy Non-Compliance

Breaches of this Policy will be addressed in accordance with organizational procedures. Non-compliance by third-party personnel shall be referred to the relevant business or functional head for contractual action under procurement or legal processes, as applicable.

7. Review and Maintenance

This Policy shall be reviewed at least annually, or upon significant changes in technology, organizational structure, regulatory requirements, or risk levels that could affect Apex's business environment. Document version control will be updated upon content changes, with appropriate approvals recorded. The effective date shall reflect the approval date.

Coco and Solar Energy Authorized Signatory

Prepared By

Approved By