



EMPOWER CONSULTING LIMITED
EASY SOLUTION

ECL-CMP-003 REV.00

INFORMATION SECURITY POLICY

1. PURPOSE

This Information Security Policy establishes the principles, objectives and commitments through which **Empower Consulting Limited** protects the information and information assets used in the conduct of its business activities.

The Company recognizes that information is one of its most valuable assets and that its protection is essential to ensuring business continuity, service quality, the protection of intellectual property, regulatory compliance and the confidence of clients, business partners and stakeholders.

Empower Consulting Limited considers information security to be an integral part of its corporate governance and management framework, promoting an organizational culture founded on accountability, confidentiality and the responsible management of information.

This Policy forms an integral part of the Company's Corporate Compliance framework and Integrated Management System and shall be read in conjunction with the Code of Ethics and Business Conduct, the Anti-Bribery & Anti-Corruption Policy, the Whistleblowing Policy and all other applicable corporate policies and procedures.

Through this Policy, **Empower Consulting Limited** reaffirms its commitment to implementing organizational and management measures proportionate to the risks associated with its business activities, while promoting the continual improvement of its Information Security Governance Framework.

2. SCOPE

This Information Security Policy applies to all information managed by **Empower Consulting Limited**, regardless of its format, medium or the manner in which it is created, collected, stored, processed, transmitted, shared or disposed of.

This Policy also applies to all of the Company's information assets, including documents, data, records, information systems, electronic devices, digital platforms, communications and any other information processed in connection with the Company's business activities.

The provisions of this Policy are binding upon directors, employees, consultants, contractors, temporary or

seconded personnel, suppliers, subcontractors, business partners and any other individual or organization acting on behalf of the Company or having access to its information assets.

Every recipient is responsible for protecting the information to which they have access in the course of their professional activities and shall conduct themselves in accordance with the principles set out in this Policy, actively contributing to the protection of the Company's information assets.

Empower Consulting Limited further encourages its business partners to adopt equivalent information security principles and safeguards, promoting the responsible management of information throughout the entire business relationship.

3. PRINCIPLES OF INFORMATION SECURITY

Empower Consulting Limited considers information security to be a fundamental element of its corporate governance and recognizes that protecting its information assets is essential to ensuring business continuity, service quality, regulatory compliance and the confidence of clients, business partners and stakeholders.

The Company adopts a systematic approach to information security based on the principles of confidentiality, integrity and availability, ensuring that information is accessible only to authorized individuals, remains accurate, complete and reliable, and is available whenever required to support business operations.

All information managed by the Company shall be protected throughout its entire lifecycle, from creation and storage to use, sharing, archiving and secure disposal, through organizational and management measures proportionate to the level of risk and the criticality of the information concerned.

Empower Consulting Limited promotes a corporate culture in which information security is recognized as a shared responsibility. Every individual acting on behalf of the Company is expected to contribute actively to the protection of its information assets by adopting responsible behaviours consistent with this Policy and the Company's applicable procedures.

The Company applies a risk-based approach when defining its information security measures, periodically assessing threats, vulnerabilities and potential impacts on information assets and implementing controls proportionate to the identified level of risk.

Through the periodic review of its policies, procedures and organizational measures, **Empower Consulting Limited** promotes the continual improvement of its Information Security Governance Framework, ensuring that it remains aligned with the evolution of the Company's business activities, operating environment and internationally recognized best practices.

4. INFORMATION PROTECTION PRINCIPLES

Empower Consulting Limited implements organizational, procedural and management measures designed to ensure a level of information protection proportionate to the nature of its business activities, the criticality of the information processed and the associated risks.

The Company considers the protection of information to be a shared responsibility and promotes the implementation of appropriate controls throughout the entire information lifecycle, from its creation and use through to its retention and secure disposal.

The measures adopted are intended to ensure the confidentiality, integrity, availability and appropriate use of information, reducing the risk of unauthorized access, loss, improper disclosure, alteration or misuse.

The following provisions establish the principal principles adopted by the Company to protect its own information and the information entrusted to it by clients, business partners and other stakeholders.

4.1 INFORMATION CLASSIFICATION

Empower Consulting Limited applies information classification criteria to ensure that all information is managed in accordance with a level of protection appropriate to its nature, sensitivity and business value.

Information classification defines the requirements governing access, use, storage, transmission and retention of information, thereby contributing to the protection of the Company's information assets.

All individuals acting on behalf of **Empower Consulting Limited** are expected to handle information in accordance with its assigned classification and the applicable corporate procedures.

4.2 ACCESS CONTROL

Access to information shall be granted exclusively to authorized individuals and limited to legitimate business needs arising from their assigned responsibilities.

Empower Consulting Limited applies authorization principles based on the concept of business necessity, ensuring that each recipient has access only to the information required to perform their professional duties.

Access rights shall be reviewed periodically and updated to reflect changes in organizational structure, responsibilities and operational requirements.

4.3 CONFIDENTIAL INFORMATION MANAGEMENT

Confidential information represents a strategic asset of the Company and shall be protected against unauthorized use, disclosure or access.

Every recipient of this Policy is responsible for ensuring that confidential information is used exclusively for legitimate business purposes and in accordance with contractual obligations, applicable legal requirements and the Company's procedures.

Particular care shall be taken when handling information belonging to clients, business partners or any other party that entrusts information to **Empower Consulting Limited**.

4.4 PERSONAL DATA PROTECTION

Empower Consulting Limited processes personal data in accordance with applicable legal and regulatory requirements and implements organizational measures designed to ensure its protection, confidentiality and appropriate use.

Personal data shall be processed solely for legitimate purposes and in accordance with the principles of fairness, proportionality and accountability.

The protection of personal data forms an integral part of the Company's commitment to safeguarding information.

4.5 USE OF INFORMATION ASSETS

The Company's information assets shall be used exclusively for legitimate business purposes and in accordance with applicable corporate policies and procedures.

Every recipient is responsible for the appropriate use of the information and information assets made available by the Company, avoiding any conduct that could compromise their security, availability, integrity or reliability.

4.6 INFORMATION SECURITY INCIDENT MANAGEMENT

Any event that may compromise the confidentiality, integrity or availability of information shall be reported promptly in accordance with the Company's established procedures.

Empower Consulting Limited promotes a structured approach to the management of information security incidents in order to minimize their impact, identify their root causes and implement appropriate corrective and preventive actions.

All recipients are expected to cooperate actively in the reporting and management of incidents that may affect the Company's information assets.

4.7 RISK MANAGEMENT

Empower Consulting Limited adopts a risk-based approach to identify, assess and manage risks that may affect the security of its information assets.

Information protection measures are reviewed periodically to reflect changes in business activities, the operating environment and emerging threats, ensuring that controls remain proportionate to the identified level of risk.

Risk management forms an integral part of the Company's decision-making process and supports the continual improvement of the measures adopted to protect its information assets.

5. ROLES AND RESPONSIBILITIES

Protecting information is a shared responsibility involving everyone acting on behalf of **Empower Consulting Limited**.

Management defines the strategic direction for information security, promotes a culture of information security awareness and ensures the implementation of the organizational measures necessary to maintain a level of protection appropriate to the Company's activities.

All recipients of this Policy are responsible for the proper management of the information to which they have access in the course of their professional activities and are expected to operate in accordance with the principles, procedures and security measures adopted by the Company.

Consultants, contractors, suppliers, subcontractors and business partners processing information on behalf of **Empower Consulting Limited** are required to comply with the same principles of confidentiality, integrity and information protection established by this Policy and by the applicable contractual arrangements.

The Company promotes awareness, training and the continual development of information security competencies, recognizing that individual behaviour represents one of the most important safeguards for protecting the Company's information assets.

6. REVIEW AND CONTINUAL IMPROVEMENT

This Information Security Policy shall be subject to periodic review to ensure its continued suitability, effectiveness and alignment with the evolution of the Company's business activities, applicable legal and regulatory requirements, emerging risks and internationally recognized best practices in information security.

Any revisions or updates to this Policy shall be approved by Management and communicated to all relevant recipients through the Company's established communication channels.

Empower Consulting Limited considers the continual improvement of information protection to be an essential element of its corporate governance and is committed to periodically reviewing its organizational, procedural and management measures in order to strengthen organizational resilience, business continuity and the confidence of its clients, business partners and stakeholders.

DOCUMENT INFORMATION

FIELD	CONTENT
Document Title	Information Security Policy
Document Code	ECL-CMP-003
Revision	Rev.00
Effective Date	15TH May, 2026
Approved By	Managing Director
Document Owner	Empower Consulting Limited
Document Status	Approved
Classification	Public
Review Period	Every two years, or earlier if required by changes in legislation, organizational requirements or business operations.
Next Review Date	15TH May, 2028