Information Security Policy of PRISMA CONSULTING ENGINEERS S.A.

1. Management Statement

It is the policy of the organisation to ensure that Information will be protected from a loss of:

- **Confidentiality:** so that information is accessible only to authorised individuals.
- **Integrity:** safeguarding the accuracy and completeness of information and processing methods.
- **Availability:** that authorised users have access to relevant information when required.

The Head of IT will review and make recommendations on the security policy, policy standards, directives, procedures, Incident management and security awareness education.
Regulatory, legislative and contractual requirements will be incorporated into the Information Security Policy, processes and procedures.
The requirements of the Information Security Policy, processes, and procedures will be incorporated into the organisation's operational procedures and contractual arrangements.
The organisation will work towards implementing the ISO27000 standards, the International Standards for Information Security.
Guidance will be provided on what constitutes an Information Security Incident. All breaches of information security, actual or suspected, must be reported and will be investigated.
Business continuity plans will be produced, maintained and tested.
Information security education and training will be made available to all staff and employees.
Information stored by the organisation will be appropriate to the business requirements.

2. Information Security Coordination

The security of information will be managed within an approved framework through assigning roles and co-ordinating implementation of this security policy across the organisation and in its dealings with third parties.
Specialist external advice will be drawn upon where necessary so as to maintain the Information Security Policy, processes and procedures to address new and emerging threats and standards.

3. Information Security Responsibilities

The Head of IT is the designated owner of the Information Security Policy and is responsible for the maintenance and review of the Information Security Policy, processes and procedures.
Heads of Department are responsible for ensuring that all staff and employees, contractual third parties and agents of the organisation are made aware of and comply with the Information Security Policy, processes and procedures.
The organisation's auditors will review the adequacy of the controls that are implemented to protect the organisation's information and recommend improvements where deficiencies are found.
All staff and employees of the organisation, contractual third parties and agents of the organisation accessing the organisation's information are required to adhere to the Information Security Policy, processes and procedures. Failure to comply with the Information Security Policy, processes and procedures will lead to disciplinary or remedial action.

4. Asset Management

The organisation's assets will be appropriately protected. All assets (data, information, software, computer and communications equipment and service utilities) will be accounted for and have an owner. Owners will be identified for all assets and they will be responsible for the maintenance and protection of their assets.

5. Human Resources Security

The organisations security policies will be communicated to all employees, contractors and third parties to ensure that they understand their responsibilities. Security responsibilities will be included in job descriptions and in terms and conditions of employment.
Verification checks will be carried out on all new employees, contractors and third parties.

6. Physical and Environmental Security

Critical or sensitive information processing facilities will be housed in secure areas.
The secure areas will be protected by defined security perimeters with appropriate security barriers and entry controls.
Critical and sensitive information will be physically protected from unauthorised access, damage and interference.

7. Communications and Operations Management

The organisation will operate its information processing facilities securely.
Responsibilities and procedures for the management, operation and ongoing security and availability of all data and information processing facilities will be established.
Appropriate operating procedures will be put in place.
Segregation of duties will be implemented, where appropriate, to reduce the risk of negligent or deliberate system misuse.

8. Access Control

Access to all information will be controlled.
Access to information and information systems will be driven by business requirements. Access will be granted or arrangements made for employees, partners, suppliers according to their role, only to a level that will allow them to carry out their duties.
A formal user registration and de-registration procedure will be implemented for access to all information systems and services.

9. Information Systems Acquisition, Development, Maintenance

The information security requirements will be defined during the development of business requirements for new information systems or changes to existing information systems.
Controls to mitigate any risks identified will be implemented where appropriate.

10. Information Security Incident Management

information security incidents and vulnerabilities associated with information systems will be communicated in a timely manner. Appropriate corrective action will be taken.
Formal incident reporting and escalation will be implemented.
All employees, contractors and third party users will be made aware of the procedures for reporting the different types of security incident, or vulnerability that might have an impact on the security of the organisation's assets.
Information security incidents and vulnerabilities will be reported as quickly as possible to the CISO or IT responsible person.

11. Business Continuity Management

The organisation will put in place arrangements to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.
A business continuity management process will be implemented to minimise the impact on the organisation and recover from loss of information assets. Critical business processes will be identified.
Business impact analysis will be undertaken of the consequences of disasters, security failures, loss of service, and lack of service availability.

12. Compliance

The organisation will abide by any law, statutory, regulatory or contractual obligations affecting its information systems.
The design, operation, use and management of information systems will comply with all statutory, regulatory and contractual security requirements.