Quality & Information Security Policy

Quality Policy

POLICY STATEMENT

It is the policy of this company to operate our business in a manner that consistently meets or exceeds the requirement set by our stakeholders. To achieve this, we are committed to continuous improvement of our management systems, operations and the products and services provided by our company.

AIMS AND OBJECTIVES

To achieve this goal, we recognise that the quality of our products and services are determined by our client's needs and expectations. Our objectives are to:

- Identify the changing needs and expectations of our clients
- Develop and maintain processes and procedures that ensure that these changes are accommodated
- Achieve efficiency in our operations, attention to detail, and responsiveness to client priorities
- Provide quality products and services on time, and at a competitive price
- Provide an employment environment where continuous improvement is encouraged

RESPONSIBILITIES

We, as a company will:

- Train all employees to identify areas where improvement can be achieved
- Remove wasted and non-value-added steps and time in our processes where feasible
- Strive to ensure that client and stakeholder satisfaction is achieved at all times, and in all things
- Support the adoption of appropriate quality systems and management principles in order that all stakeholders benefit from this commitment to quality

Employees are expected to:

- Assist and cooperate in ensuring that this policy is followed
- Actively participate in the adherence of this company to the achievement of the goals and objectives of this policy

Information Security Policy

Rockwell is committed to understanding and effectively managing risks related to Information Security to provide greater certainty and confidence for our security holders, employees, clients, suppliers and for the communities in which we operate. This commitment also extends to continuous improvement of our management systems, operations, and the products and services provided by our company. Finding the right balance between Information Security risk and business benefit enhances our business performance and minimises potential future exposures.

This policy applies to all information, computer and network systems governed, owned by and/or administered by Rockwell.

It is the policy of Rockwell to ensure:

- Information will be protected against unauthorised access
- Confidentiality of information will be maintained
- Information will not be disclosed to unauthorised persons through deliberate or careless action
- Integrity of information is maintained through protection from unauthorised modification
- Availability of information to authorised users when needed

- Information Security training is completed by all staff
- All suspected breaches on Information Security will be reported and investigated

Any individual dealing with information at Rockwell, no matter what their status (e.g. employee, contractor, or consultant), must comply with the Information Security policies and related documents

AIMS AND OBJECTIVES

The aims and objectives of these policies are to:

- Reduce the opportunity for mistakes and misunderstandings to occur when dealing with IT assets and information of Rockwell
- Educate staff to allow them to independently make informed decision with regards to the secure handling of IT assets and information which is owned by Rockwell, within the framework of the Information Security policies
- Ensure Information Security is addressed for all projects, regardless of type, by way of risk assessments and objectives
- Assist in the identification and investigation of fraudulent Information Security related activities and co-operate with relevant legal agencies
- Defend IT assets and information that Rockwell governs, owns, manages, maintains, or controls which are both tangible and intangible
- Safeguard IT related records and documents that exist in all forms – paper and electronic
- Comply with the needs of the Regulatory Authorities, internal or external
- Comply with legislation and industry best practices that apply to Rockwell
- Have Information Security controls in the framework of Information Security policies so as to provide a secure environment for the operation of Rockwell business
- Identify, through appropriate risk assessment, the value of information assets and to understand their vulnerabilities and the threats that may expose them to risk
- Manage the risks to an acceptable level through the design, implementation and maintenance of appropriate security processes and controls

All personnel have a responsibility to report perceived and actual information relating to Information Security breaches and/or IT incidents either to the Management Representative or to their immediate Manager/Supervisor. Management and employees are responsible for embedding Information Security risk management in our core business activities, functions, and processes. Information Security risk awareness and our tolerance for risk are key considerations in our decision making. Failure to comply with Security Policy, Standards, or Practices result in disciplinary action including termination and criminal and/or civil actions.