



INFORMATION SECURITY MANAGEMENT SYSTEM

POLICY

Al Ghurair Printing and Publishing LLC is committed towards securing the Confidentiality, Integrity and Availability of all the physical and electronic information assets throughout organization In order to preserve its Customer Satisfaction, reputation, competitive edge, profitability, legal, regulatory and contractual compliance.

AGPP has adopted an Information Security Management System (ISMS) comprising of the Information Security Policies, Procedures and Processes to effectively protect data/information of AGPP and its customers from information security threats, whether internal or external, deliberate or accidental. ISMS in AGPP is aligned to the requirements of ISO/IEC 27001: 2013 Standard.

VISION

Continue to be one of the pioneers in the
SECURITY PRINTING INDUSTRY
by providing Security Printing Products and Services.

Mission

Continually upgrade infrastructure, Technical capabilities and invest in innovative technologies. To be a responsive institution committed in building win-win situation for customers and external service providers to develop strong relationships.

AGPP Management is committed to ensure that:

- Maintaining the Established / Implemented Information Security Management System (ISMS) to comply with the requirements of the standard ISO 27001:2013, all the applicable statutory and regulatory requirements which are specified by the client are determined, understood and consistently met.
- Assess all the identified risks and mitigated to an acceptable level through a risk management framework.
- Confidentiality of the information is protected, Integrity of the information is maintained and Availability of information is maintained to meet the business needs and customer requirements.
- Business continuity plans are developed, maintained and tested. Incident management process is established and implemented to ensure that all breaches of information security, actual or suspected are reported and investigated

AGPP Management shall:

- Take accountability for the effectiveness of ISMS and ensure Security Policy and Objectives are established / monitored / measured/ reviewed which are in line with the Context and strategic direction of the company and promotes the use of process approach and risk-based thinking.
- Ensure that the Resources needed for the ISMS are available; including training, and Support other relevant management roles to demonstrate their leadership. Communicate the importance of effective Information Security Management System and conforming to the requirements of ISO 27001:2013
- This policy is communicated to the employee, displayed and made available to all interested parties upon request. Policy will be reviewed annually and where deemed necessary, will be amended and re-issued.