ISO 27001: 2013 – SECURITY POLICY

It is policy of iENGINEERING to create, maintain and continually improve the Information Security Management System and to adhere to Security practices in compliance with best practices for Software development industry and information security needs of the customer. iENGINEERING works within the framework of the Local & Federal Government, while fulfilling the contractual obligation of the client. This is to ensure protection of its information assets from all threats – internal or external, deliberate or accidental and natural disasters. Furthermore, to achieve this objective iENGINEERING will ensure the following:

- Confidentiality of information assets will be assured for, but not limited to third parties, Company Operational, personal and electronic or physical communications data.
- A Business Continuity Management Framework shall be made available and Business Continuity plans will be produced to counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters. Business continuity plans should be maintained and tested.
- All breaches of information security, actual or suspected, will be reported to, and investigated by the relevant authorities not limited to System Administration and Incident Response team.
- Appropriate access control will be maintained and information will be protected against unauthorized access. Such as but not limited to:
    - Confidentiality, Integrity and Availability of information is maintained throughout a systematic process.
    - Policies, Procedures and Guidelines not limited to Information Security will be made available in online format through an intranet system to support the Security Policy as deemed appropriate.
    - ISO Steering team has direct responsibility for maintaining the Security Policy and involved with writing and/or managing the development of relevant policies, procedures and guidelines not limited to information security.
    - All managers are directly responsible for implementing the Security Policy within their teams, and for adherence by their staff.
    - It is the responsibility of each member of staff to adhere to the Security Policy.
    - Information security is managed through iENGINEERING Risk Management framework.
    - The availability of information and information systems will be met as required by the core and supporting business operations.
- Risk management framework will define risk and its treatment to all corporate assets (tangible/intangible and human). The risk against each are assessed and against all risks, appropriate controls are implemented to mitigate risk and contingency plans are defined for all assets with unacceptable levels of residual risk.
- All corporate assets (tangible/intangible and people) have a secure and safe environment.
- Human resources are provided conducive work environment, free from accidental and occupational hazards.
- All personnel are trained in information security practices, roles and responsibilities.
- Commitment to continually improve and satisfy applicable requirements related to information security system.
- Physical, Logical and Remote access to all the corporate assets (tangible/intangible), information and physical locations are monitored and controlled.