# INFORMATION SECURITY POLICY

## Policy Statement

Digital Dubai Authority (DDA)is committed towards securing the Confidentiality, Integrity and Availability of information and information processing facilities used in the day-to-day business operations. The security of information and other assets is therefore regarded as fundamental for the successful business operation of Digital Dubai Authority. Information security policy is a key component of DDA's overall information security management framework and should be considered along with Digital Dubai Authority's specific and more detailed information security policies, procedures, standards and guidelines. Adherence to this policy will help to protect information and information processing facilities of DDA and its customers from information security threats, whether internal or external, deliberate or accidental. Digital Dubai Authority is committed in improving the security posture of the environment, reducing the security risks by implementing appropriate security controls.

## Scope

The scope covers the Information Security management system related to Design, Development, Provision and Support of Information Technology Services offered by Digital Dubai Authority as defined in the service catalogue provided in https://connect.smartdubai.ae.

## Core Principles

Digital Dubai Authority recognizes that secure and continuous operations of Digital Dubai Authority services are dependent upon securing three core organizational elements, which are people, process and technology. Thus, all DDA activities must adhere to the general principles laid down. Digital Dubai Authority has thus formulated the following to ensure that information security requirements implemented effectively across the organization.

## General Information Security Principles:

- Comply with the UAE regulatory, statutory, legislative requirements, and Information Security Regulations (ISR)
- Comply with information security management, business continuity management and payment card data security international standard's controls and requirements
- Establish 'Information Security Steering Committee' representing the Management of Digital Dubai to demonstrate management commitment towards information security management and maintain the confidentiality, integrity and availability of Information and Information assets
- Maintain Information Security Management System Charter that define the responsibilities of the information security program stakeholders
- Establish Comprehensive Risk Management across Digital Dubai
- Handle, report and investigate all incidents and suspected breaches related to Information Security
- Provide appropriate Information Security Training and awareness to all employee and users
- Design appropriate controls and procedures to support the implementation of this Information Security Policy
- Ensure all stakeholders are responsible for the implementation of respective security policies and procedures within their area of operation, and oversee adherence by their team members
- Continually improve Information Security through implementation of corrective and preventive actions
- Formulate an Internal Audit function for providing independent assurance to Digital Dubai Management on ISMS and business continuity processes and controls