

Information Security Policy

Policy Statement

The Information Security Policy of the Community Development Authority (CDA) has been established in accordance with the Information Security Regulations (ISR v3.1) of the Government of Dubai, issued by Executive Council Resolution No. (13) of 2012, and **ISO/IEC 27001:2022 – Information Security Management Systems (ISMS)**.

This policy demonstrates CDA's commitment to protecting information assets against all threats, whether internal or external, deliberate or accidental, to ensure confidentiality, integrity, and availability of information.

This policy considers internal and external issues, as well as the requirements and expectations of relevant interested parties.

Purpose of the Policy

The purpose of this policy is to define the overall direction, principles, and management commitment for information security within CDA. The policy aims to:

Establish and maintain an effective Information Security Management System (ISMS)

Protect information assets from unauthorized access, disclosure, alteration, or destruction

Support business objectives and service continuity

Ensure compliance with applicable legal, regulatory, and contractual requirements

Enable continual improvement of information security practices

Scope

This policy applies to:

- All CDA employees, management, and temporary staff
- All contractors, consultants, suppliers, and third parties with access to CDA information
- All information assets, systems, applications, networks, and devices
- All locations, including on-premises, remote working environments, and cloud-based services

Information Security Principles

CDA recognizes that effective information security is achieved through adherence to the following core principles:

- **Confidentiality:** Ensuring information is accessible only to authorized individuals
- **Integrity:** Safeguarding the accuracy and completeness of information and processing methods
- **Availability:** Ensuring authorized users have access to information when required

Leadership Commitment

Top Management is committed to:

- Establishing, implementing, maintaining, and continually improving the ISMS
- Integrating information security requirements into CDA's business processes
- Providing adequate resources to support information security objectives

- Assigning and communicating roles, responsibilities, and authorities related to information security
- Promoting a culture of information security awareness across the Authority

Information Security Objectives

CDA shall establish, implement, monitor, and review **information security objectives** at relevant functions and levels.

These objectives shall:

- Be consistent with this Information Security Policy
- Be measurable where practicable
- Consider applicable information security risks and opportunities
- Be monitored and reviewed periodically
- Be updated based on changes in risk, technology, regulatory requirements, and business needs

Risk Management

CDA shall maintain a systematic risk management approach to identify, assess, and treat information security risks in accordance with the ISMS risk management methodology.

Controls and Compliance

- Information security controls shall be implemented to mitigate identified risks
- Compliance with applicable UAE laws, regulations, and Government of Dubai policies shall be ensured
- Internal audits shall be conducted periodically to verify ISMS compliance and effectiveness
- Nonconformities shall be addressed through corrective actions

Incident Management

All information security incidents, suspected incidents, and weaknesses shall be reported, investigated, and managed in a timely manner to minimize impact and prevent recurrence.

Awareness and Training

CDA shall ensure that employees and relevant external parties receive appropriate information security awareness, education, and training commensurate with their roles and responsibilities.

Continual Improvement

CDA is committed to the **continual improvement of the Information Security Management System (ISMS)** through performance monitoring, audits, management reviews, and corrective actions.

Policy Review

This policy shall be reviewed at least annually, or upon significant changes to business operations, risks, regulatory requirements, or information security environment.