

## Information Security Policy

The Telecommunications and Digital Government Regulatory Authority (TDRA) is an independent Federal Government entity entrusted to oversee the Telecommunications and ICT sector in the UAE.

TRA is committed towards securing the Confidentiality, Integrity and Availability of information for the day-to-day Business and Technical operations. The security of information and other assets is therefore regarded as fundamental for the successful business operation of TDRA.

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

The management of TDRA is committed to ensure that:

- Regulatory and legislative requirements related to TDRA are met
- The confidentiality of information is protected and prevent disclosure of valuable or sensitive information
- The integrity of information is maintained to ensure its accuracy and completeness
- The availability of information is maintained to meet business needs and client's requirements
- Business continuity plans are developed, maintained and tested
- Information security awareness is provided to all TDRA employees
- Incident management process is established and implemented to ensure that all breaches of information security, actual or suspected are reported and investigated
- Risks are mitigated to an acceptable level through a risk management framework
- The information security management system is continually improved
- Appropriate resources are allocated in order to implement, operate and review an effective Information Security Management System
- All stakeholders are responsible for implementation of respective security policies and procedures within their area of operation, and oversee adherence by their team members

TRA management acknowledges the need of **continual improvement** and has introduced various methods to ensure that effectiveness and continual improvement of the processes are achieved.

TRA shall follow a formal **disciplinary process** for employees who have allegedly violated the information security policies and procedures.

TRA shall ensure that the **review** of the Information Security Policy and related documents is performed at least on an annual basis or when significant changes occur to ensure suitability, adequacy, and effectiveness of the ISMS framework.