



هيئة تنظيم الاتصالات  
Telecommunications Regulatory Authority

## Information Management Policy

## 1. Policy Overview

Information is an essential component of effective management across departments and in informing all stakeholders. The availability of high-quality, authoritative information to decision makers supports the delivery of our work program and services, thus enabling departments to be more responsive and accountable to our stakeholders.

## 2. Policy Objectives

The objective of the policy is to achieve efficient and effective information management and dissemination to support program and service delivery; foster informed decision making; facilitate accountability, transparency, protection of confidentiality and collaboration; and preserve and ensure access to information and records for the benefit of present and future employees and stakeholders. Through achieving the above TRA should meet its obligations under the Telecommunications Law.

## 3. Policy Requirements

The TRA Information Management Policy will serve as guidance and point of reference for the establishment of several supporting policies and procedures to govern the management, storage, dissemination, processing and access of information assets.

Such underlying policies should allow for the following:

- 3.1. Departmental programs and services integrate information management requirements into development, implementation, evaluation, and reporting activities;
- 3.2. Decisions and decision-making processes are documented to account for and support the continuity of departmental operations, permit the reconstruction of the evolution of policies and programs, and allow for independent evaluation, audit, and review;
- 3.3. Information is shared within and across departments to the greatest extent possible, while respecting security and privacy requirements;
- 3.4. All information is managed to respect user agreements, licensing conditions, or both and for ensuring the relevance, authenticity, quality, and cost-effectiveness of the information for as long as it is required to meet operational needs and accountabilities;
- 3.5. Electronic systems are the preferred means of creating, using, and managing information;
- 3.6. Departmental participation in setting direction for information and recordkeeping is facilitated;
- 3.7. Establishing, measuring and reporting on a departmental program or strategy for the improvement of the management of information;
- 3.8. Making available appropriate information to each person from Board Members downwards and from consumers to licensees.

## 4. Proposed Information Management Policies

The following policies must be established to support the above policy requirements:

### 4.1. Exchange of information

TRA will move to exchanging information with all internal and external stakeholders by electronic means only. This will be achieved before the end of December 2009. Exceptions will be only allowed for consumers who do not have an email address and are not connected to the internet.<sup>1</sup>

### 4.2. Information Classification Policy

Information should be classified to indicate the need, priorities and degree of protection. Information has varying degrees of sensitivity and criticality. Some items may require an additional level of protection or special handling. An information classification policy should be used to define an appropriate set of protection levels, and communicate the need for special handling measures.

### 4.3. Asset Classification and Control Policy

All major information assets should be accounted for and have a nominated owner. Accountability for assets helps to ensure that appropriate protection is maintained. Owners should be identified for all major assets and the responsibility for the maintenance of appropriate controls should be assigned. Responsibility for implementing controls may be delegated. Accountability should remain with the nominated owner of the asset.

### 4.4. Policy for the Storage, Dissemination and Destruction of Information

Information must be properly managed throughout the various stages of its existence; ranging from creation to storage and destruction, if necessary. TRA staff must be provided with clear and concise procedures for handling information assets regardless of the required operation. A Policy for the storage, dissemination and destruction of information should provide the specifications and expectations for such activities and more. The Policy should not result in information being duplicated other than for security reasons.

### 4.5. Automation Policy

Several routine tasks and operations should not take a large share of an employee's time, and should be automated whenever possible. The Automation Policy will set the framework for internal workflow

---

<sup>1</sup> Legislative Decree Number 28 of the year 2002 afforded Electronic Records legal recognition. For more details, see <http://www.moic.gov.bh/NR/rdonlyres/A8FBAA02-9B7D-49F1-90A8-1A75C64BFDA6/734/ElectronicTransactionsLaw.pdf>

processes and specify a number of tasks and operations that must be automated.

#### 4.6. Information Security Policy

The TRA must establish and maintain a security program that ensures three requirements for all information assets: the availability, integrity, and confidentiality of the organization's information resources. The combination of integrity, availability, and confidentiality in appropriate proportions to support the TRA's goals can provide users with a trustworthy system – that is, users can trust it will consistently perform according to their expectations.

#### 4.7. Communications and Operations Management Policy

Responsibilities and procedures for the management and operation of all information processing facilities should be established. This includes the development of appropriate operating instructions and incident response procedures. This includes documented operating procedures and change control procedures amongst others.

#### 4.8. Access Control Policy

Access to information, and business processes should be controlled on the basis of business and security requirements. This should take account of policies for information dissemination and authorization.

#### 4.9. Availability of information

Information assets should be accessible for at least 99.9% of the time, or higher, from local or remote devices (Given the right access rights). This percentage is calculated based on the total number of work days per year. The purpose of this policy is to ensure sufficient continuity of critical assets to successfully meet the required availability level through applying quality thresholds and/or performance metrics across all business and operational levels.

The policy on information availability/assurance can be included within the corporate information security policy, or as a stand-alone policy.

#### 4.10. Compliance Policy

To avoid breaches of any criminal and civil law, statutory, regulatory or contractual obligations and of any security requirements. The design, operation, use and management of information systems may be subject to statutory, regulatory and contractual security requirements.

Advice on specific legal requirements should be sought from the organization's legal advisors.