وزارة المواصلات والاتصالات
MINISTRY OF TRANSPORT AND COMMUNICATIONS

Cyber Security Guidelines for

Information Asset Management: Roles and Responsibilities

Version: 1.1

Author: Cyber Security Policy and Standards

Document Classification: Public

Published Date: May 2018

Document History:

Version	Description	Date
1.0	Published V1.0 document	April 2017
1.1	Changing MOTC logo	May 2018

Table of Contents

Legal Mandate(s)

Emiri decision No. (8) for the year 2016 sets the mandate for the Ministry of Transport and Communication (hereinafter referred to as "MOTC") provides that MOTC has the authority to supervise, regulate and develop the sectors of Information and Communications Technology (hereinafter "ICT") in the State of Qatar in a manner consistent with the requirements of national development goals, with the objectives to create an environment suitable for fair competition, support the development and stimulate investment in these sectors; to secure and raise efficiency of information and technological infrastructure; to implement and supervise e-government programs; and to promote community awareness of the importance of ICT to improve individual's life and community and build knowledge-based society and digital economy.

Article (22) of Emiri Decision No. 8 of 2016 stipulated the role of the Ministry in protecting the security of the National Critical Information Infrastructure by proposing and issuing policies and standards and ensuring compliance.

This guideline has been prepared taking into consideration current applicable laws of the State of Qatar. In the event that a conflict arises between this document and the laws of Qatar, the latter, shall take precedence. Any such term shall, to that extent be omitted from this Document, and the rest of the document shall stand without affecting the remaining provisions. Amendments in that case shall then be required to ensure compliance with the relevant applicable laws of the State of Qatar.

1. Overview:

Information today is one of the most important assets within a company. The evolution of its importance comes riddled with issues pertaining its management. Organizations are grappling with issues to identify who really "owns" the data? Who is the "custodian"? Who is responsible for what?

This document is a step in the direction to help agencies in Qatar understand the various roles and responsibilities pertaining to information and the roles and responsibilities of the various functions within an organization.

The document is a complementing tool to assist organizations in Qatar in their pursuit to comply with NIA Policy.

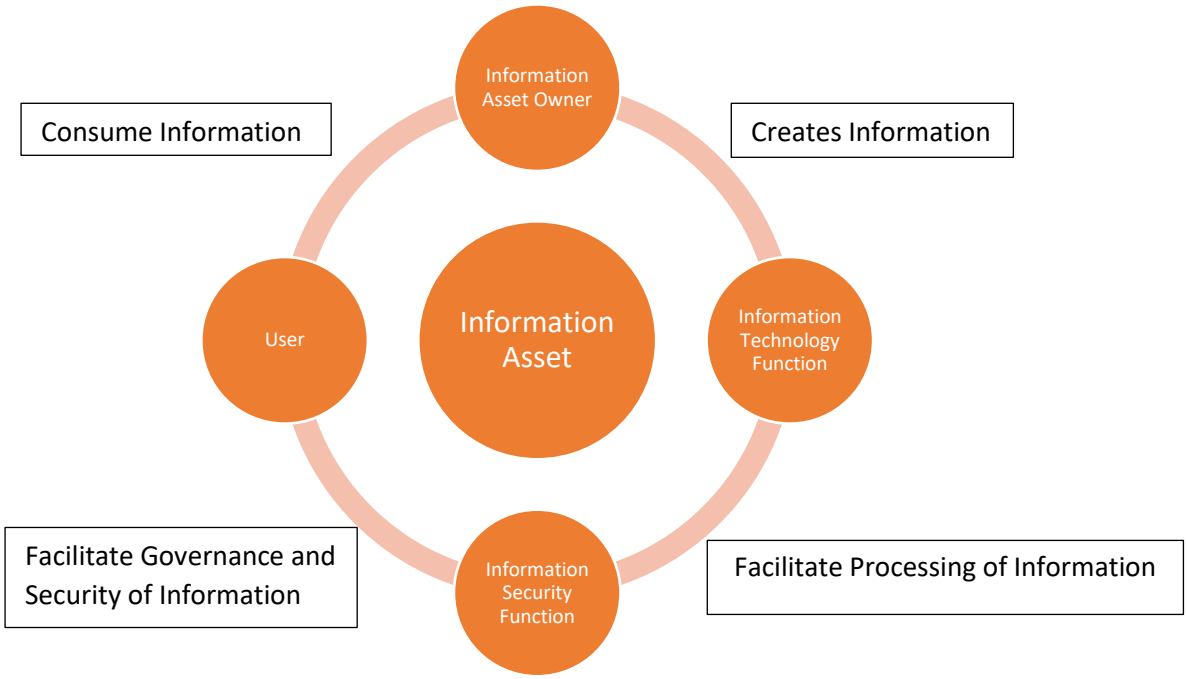

Figure (1): Asset's information cycle through different roles

2. Audience

All employees within an organization, who either create, manage or consume information.

3. What is an Information Asset?

An information asset is a body of information, defined and managed as a single unit, so that it can be understood, shared, protected and utilized effectively. Information assets have recognizable and manageable value, risk, content and lifecycles.

Information assets could come in any media form i.e. paper or electronic format (e.g. CDs, USBs, HDDs etc). It could be structured (e.g. databases) or unstructured (e.g. emails). It could be personal information or official. It could have different classifications i.e. Public, Restricted, Confidential etc.

Following table is an illustration of what typical information assets could include. This is a non-exhaustive list.

Personal Information	Applications
Databases and data files Back-up and archive data Audit data Paper records (Resumes, Health records etc) Paper reports	Applications and System Software System tools and management utilities Databases and data files Back-up and archive data
Other Information Content	**Hardware**
Audit data Paper records and reports Audio / Video People skills and experience	Information Processing Systems Smart Phones and Digital Tablets Hardware Tokens / Keys / Dongles Networks and Printers
System/Process Documentation	
System information and documentation Operations and support procedures Manuals and training materials Contracts and agreements Networks Diagram and Configuration System Configuration Disaster Recovery and Business continuity plans	

Table (1): illustration of typical Assets contents

4. Who is the Information Asset Owner?

The owners of an information asset are those individuals who have primary responsibility for the viability and survivability of the asset. The owner is a senior person within an organization with sufficient authority and officially designated as accountable for a specific business process / function within an organization.

The owner must determine what information assets are they responsible for. The responsibility is not restricted to the information systems within their domain and should go beyond in defining the information that needs to be managed within those systems. Such information may include Personally Identifiable Information (PII) along with critical business data in both electronic and non-electronic formats.

It is the owner's responsibility to set the security requirements for information assets and communicate those requirements to all of the assets' custodians. Owners are also responsible to assess these requirements from time to time based on the changing threat profiles and / or the value of information with passage of time. Owners should ensure that the defined security requirements are implemented and maintained by the data custodians. Further, the effectiveness of the controls implemented should be assessed at regular intervals (e.g. through audits).

An owner may delegate these security responsibilities, but the owner remains ultimately responsible for the protection of the asset.

5. Who is the Custodian of an Information Asset?

The term "custodian" refers to any individual in the organization who has the responsibility to protect an information asset as it is stored, transported, or processed in line with the requirements defined by the information asset owner.

"Custodians" includes users from the Information Technology / Information Security function along with the staff who may be responsible for transporting information (e.g. paper records / CDs / USBs etc) from one place to another or even the facilities or security staff who may have physical access to information processing and storing facilities.

Certain roles within the organization such as IT staff with administrative / root privileges may have unlimited access to the agency's information system, these are critical roles and sufficient controls and procedures must be developed for such privileged access.

Data Users also have a critical role to protect and maintain an organization's information systems and data. For the purpose of information security, a Data User is any employee, contractor or third-party provider who is authorized by the Data Owner to access information assets.

At times, the data custodian may play the role of a trusted advisor to the owner advising him on the risks and controls suitable for the information asset. However, the ultimate responsibility lies with the Owner and in no circumstances, the data custodian shall deem the role of an owner.

6. Risks to Information Assets

An Information Asset Owner should assess the risks to the information assets and ensure adequate controls to protect against:

Loss of Confidentiality: Inappropriate access to, or disclosure of, protectively marked or personal data by Data users, public and / or malicious actors, whether accidental or deliberate

Loss of Integrity: Data users acting in error or deliberately, or external parties accessing your information illegally, acting maliciously to compromise the integrity of your data with an intention to defraud you or your customers or to cause reputation damage to your organization

Loss of Availability: This could be either temporary or permanent.

Information loss - particularly during transfer or movement of information, or because of business change (mergers, acquisitions, restructuring).

Loss of access to information due to system / network outages caused due to errors or deliberate actions.

Loss of digital continuity - i.e. losing the ability to use your information in the way required when needed. By use we mean being able to find, open, work with, understand and trust your information. The lifecycle of a piece of information - how long you need to use and keep it - is often different to the lifecycle of the IT system used to access and support it.

Information Currency: Business needs change, systems change, the value of an information asset may change or the organization's information risk appetite may change. An organization's processes should be agile to manage the information security of the asset in accordance to the changing business environment.

7. Guidelines for an Information Asset Owner

Information asset owner are individuals who are responsible and accountable for the information assets within an organization. Information asset owners shall define the controls necessary for the information asset and work with information custodians to ensure that they are implemented and effective.

Classification: Asset owner should support the ISM in the task of asset classification by explaining the need and importance for all information asset assigned under his /her responsibility. [IAP-NAT-DCLS]

Labelling: Asset owner SHOULD identify the appropriate labels for all assets as per their classification to support the Need-To-Know requirement and data labelling education and awareness for the staff, employees and contractors. DL

Controls allocation: Owner SHOULD ensure the application of all baseline controls as specified in the NIAP to all classified assets. Additional, stronger controls MAY be applied, if necessary and based on the risk assessment conducted. The controls shall consistently protect the Information Asset throughout their life cycle.

Access Control and Physical Security: Asset Owner must authorize access to only those who have a business need for the information, and ensure that access is removed for those who no longer have a

business need for the information. The Access control shall include physical as well as logical access to the information asset. The controls shall be chosen based on an assessment of risk. AM and PH

Logging & Security Monitoring: The asset owner shall identify suitable technical controls and processes to log and monitor systems for potential malicious activities or system disruptions. SM

Awareness: The asset owner shall ensure that all personnel having access to the information asset are aware of the organization's security requirements and any legal or regulatory responsibilities. SA

Retention & Archival: The asset owner shall determine and document the retention periods of information assets governed by the organization's policies and regulatory requirements. DR

Incident Handling: The asset owner shall be responsible for the information asset. Any incident that compromises the confidentiality, integrity or availability of data should be reported and managed. IH

Business Continuity: The information asset owner shall ensure the availability of information as and when required for the continuance of business. BC

Ensure compliance: The asset owner shall ensure that the information asset is secured in compliance with the organizational security policy and state of Qatar laws and regulations. AC

8. Guidelines for the Information Asset Custodian

Information asset custodians are individuals in physical or logical possession of information. Information asset custodians are expected to work with information asset owners to gain a better understanding of these requirements. The information security controls implemented by the custodian must be documented and shared with the asset owner.

8.1 Information Technology Manager (IT Function)

Classification: Assist the Asset owner along with the ISM in the task of asset classification. [IAP-NAT-DCLS]

Labelling: Implement the data labeling as identified by the Asset owner. Advise the owner on technical limitations if any and possible technical mitigating solutions. DL

Controls allocation: Identify and apply all controls (baseline and additional) as specified in the NIAP to all information assets to protect the confidentiality, integrity, and availability of the information asset. The controls shall consistently protect the Information Asset throughout their life cycle. AC

Access Control and Physical Security: Implement the necessary processes and controls to manage access control to information assets. Access shall be provided to only those who have a business need for the information, and ensure that access is removed for those who no longer have a business need for the information. The Access control shall include physical as well as logical access to the information asset. The controls shall be chosen based on an assessment of risk. AM and PH

Logging & Security Monitoring: Implement suitable technical controls and processes to log and monitor systems for potential malicious activities or system disruptions. SM

Retention & Archival: Design and implement systems that shall ensure that information assets and the information life cycle are managed in line with the document retention policy. DR

Incident Handling: Implement procedures for managing incidents. This should include incident reporting and incident response. IH

Business Continuity: Design and implement the necessary procedures and controls to ensure the availability of information as and when required for the continuance of business. BC

8.2 Information Security Manager (Information Security Function)

Information Governance: The Information Security Manager will manage the information security program of the organization. The ISM will develop information security policies to ensure that the organization's information assets are secured adequately in line with the Information owner requirements and corporate policies and national regulations such as NIA Policy, Information Privacy Protection Law and Cyber crime law amongst others. IG and AC

Information Classification: Assist the information owner in identifying assets and classifying them. The ISM should also assist the information asset owner and the ITM in selecting appropriate controls to provide the necessary assurance to information asset owners. [IAP-NAT-DCLS], IG and SS

Controls: Ensure the application of all baseline controls as specified in the NIAP to all information assets.

Risk Management: Conduct a Risk assessment in association with the information asset owner and prepare an appropriate Risk treatment plan. Monitor the effectiveness of risk treatment processes and plans periodically. RM

Awareness: Design and deliver an information security awareness to all personnel having access to the information assets. The awareness shall elevate amongst the users an understanding of the organization's security requirements and any legal or regulatory responsibilities. SA

Incident Management: Define an Incident Management policy and necessary procedures. Work with the ITM to detect, respond and contain incidents. Inform and report senior management about critical incidents.

Maintain co-ordination with government and law enforcement agencies such as QCERT, to report and manage critical incidents. IM

8.3 Guidelines for Data User

Information Governance: The Data user shall be responsible for the information assets (systems / infrastructure) provided to them to carry out their official responsibilities. IG

Information Classification: The Data User shall adhere to the information classification scheme approved by the management and maintain the classification (label) provided by the information asset owner. [IAP-NAT-DCLS]

Acceptable Usage: The Data user shall handle the information assets with due care and operate them in line with the vendor / organization's Acceptable usage policy. The Data user shall exercise due diligence when accessing the web and browsing the web. They shall strictly follow organization's principles and guidelines on accessing the internet. SU

Information Exchange: The Data user shall ensure that when information traverses the boundaries of the organization (whether physical or logical) it shall retain the information classification markings and will be suitably secured as defined by the Information asset owner. IE

Incident Management: The Data user shall report any incident or malicious activity that may impact the information assets. IM