
INTEGRATED TECHNOLOGY GROUP
*Empowering People through Technology...*

# *Information Security Policy Manual*

***March 22nd 2012*** *201203 – SPV1.0*



www.dakessian-cnslt.com
Email: info@amontechnologies.jo
P.O.Box 9444, Amman - 11191 – Jordan
Suite 301, Oasis II Building, Sweifieh
www.amontechnologies.jo

**Table of Contents**

# Executive Summary

## *Introduction*

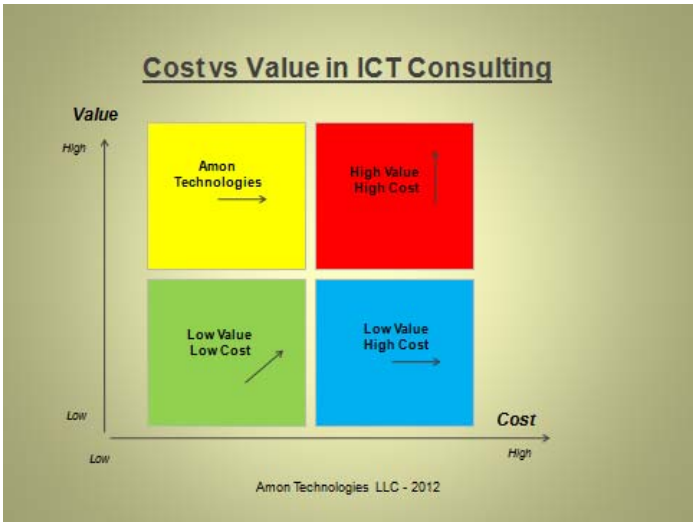
This Information Security Policies & Procedures manual was compiled and developed for ***ITG*** in a manner that suitably addresses the organization's environment and operation specific aspects. This manual enables adequate control and security over information systems and helps manage the risks of such systems effectively. This manual was prepared taking into account the recommendations of Control Objectives for Information and Related Technology (COBIT), ISO 27001 as well as our prior experiences in conducting similar assignments. which jointly act as a framework for setting the relevant control objectives within this manual.

This manual is to be adhered to by all IT users and any individuals/groups using the information systems resources of ***ITG***. These policies and procedures are applicable to all ***ITG*** staff as well as contractors, consultants, third party associates and any temporary staff having access to ***ITG***'s information assets.

***ITG*** selected ***Amon Technologies LLC*** to compile and prepare Information Technology (IT) and Information Security (IS) policies and procedures manuals in accordance with international standards and best practice in the field.

## *About Amon Technologies LLC*

***Amon Technologies LLC*** is a limited liability company registered in Amman Jordan. The company is dedicated to and specialized in a wide range of ICT related consulting services. In 2007, ***Amon Technologies LLC*** merged with ***Dakessian Consulting*** (established in 1981), combining over 30 years of experience in quality ICT consulting services in the local, regional and international markets.



We coined the term "***controlled outsourcing***" and strongly believe in the concept. Our commitment is to quality and excellence; we place ourselves at the forefront of providing high quality services at reasonable cost benefit ratios. Our services include:

- IT Policies & Procedures – COBIT based
- IS Policies & Procedures – ISO 27001:2 based
- IT Risk Assessments and Audits
- IT Infrastructure Assessments
- Technical Specifications & RFPs
- ICT Strategies & Business Plans
- ICT Project & Implementation Management
- Technical Arbitration Services

## *Structure*

The manual is composed of four main sections:

- Executive Summary
- Information Security Policies
- Policy Lists and Definitions
- Policy Relation Tables

A standardized general structure is used for all policies in this manual. For each policy, the structure contains the following elements:

**Identifier:** This is the identification number for a particular policy document and the domain. This is reflected as ***ITec##*** for Information Technology related policies and ***ISec##*** for Information Security related policies in the manual.

**Purpose:** This section clearly states the purpose of the policy

**Scope:** This section defines various internal and external entities as well as the people to which a particular policy applies

**Statements:** This section describes the policies of ***ITG*** for any given domain. It also describes the guidelines for implementing each policy. This is not a process flow description or detailed implementation process description

**Related Policies:** This section mentions other Information Technology Policies, which the user can refer to along with this policy document

**Compliance:** This section contains a statement that Information Technology & Information Security Policies will be complied with and that violations may result in disciplinary action

**Waiver:** This section provides a formal process for obtaining approval for a waiver to a policy. Waivers shall only be used in exceptional situations when communicating non-compliance with the policy for a specific period of time

**Owner:** The person responsible for maintenance and accuracy of a policy

**Custodians:** The person(s) responsible for implementation of a policy In addition to the above owner.

**Domain:** This element is applicable to both IT and IS sections and identifies the COBIT and ISO27001 domains related to this policy, e.g. IT Strategic Planning, Organization of Information Security, Human Resources Security, Asset Management, etc.

## *Summary of Policies*

The following fifteen separate information security policies (***ISec***) were formulated for ***ITG***:

- *ISec01* Information Security
- *ISec02* Organizing Information Security
- *ISec03* Data Management & Classification
- *ISec04* Personnel Security
- *ISec05* Training & Awareness
- *ISec06* Physical & Environmental Security
- *ISec07* IS Communications & Operations Management
- *ISec08* Internet & Intranet Security
- *ISec09* Email
- *ISec10* Virus Protection
- *ISec11* Logical Access Security
- *ISec12* IS Acquisition Development & Maintenance
- *ISec13* Information Security Incident Management
- *ISec14* Business Continuity Management
- *ISec15* Compliance

In addition to the above fifteen (15) ***ISec*** policies, thirteen (13) separate information technology (***ITec***) policies are ready to be formulated for ***ITG*** if requested***:***

- *ITec01* Organization
- *ITec02* Strategic Planning
- *ITec03* Infrastructure Planning
- *ITec04* Risk Management
- *ITec05* Asset Management
- *ITec06* Investment Management
- *ITec07* Personnel Management
- *ITec08* Project Management
- *ITec09* Change Management
- *ITec10* Operations Management
- *ITec11* Facilities Management
- *ITec12* Monitoring of IT Processes
- *ITec13* Supplier Management

These will be covered in a separate Information Technology Policy manual.

Overall compliance levels and disciplinary actions are classified as follows. Specific actions need to be developed by ***ITG***'s Human Resources as well as Administration Departments:

| Level | Class | Colour Code | Disciplinary Action |
|---|---|---|---|
| 1 | Critical | | Termination of Employment & Legal Action |
| 2 | Severe | | Termination of Employment & Penalty |
| 3 | Serious | | Severe Formal Reprimand & Penalty |
| 4 | Major | | Formal Reprimand |
| 5 | Minor | | Verbal Notice |

The final section of this manual provides a graphical interpretation of policy relations, owners and custodians for ease of reference.

## *Committees and Teams*

The information security polices and procedure guidelines formulated for ***ITG*** together with the information technology policies and procedures stipulate the formation of a number of committees and teams. Details of the scope and mandate of each committee or team are given in the relevant policies and procedures in the relevant manuals:

### IS Steering Committee

The committee is composed of the CEO as the chairman with the membership of the following:

- Chief Operating Officer
- Chief Technology Officer
- Head of Internal Audit
- Head of Legal
- Head of HR
- Information Security Manager (officer)

The IS Steering Committee oversees the definition of the specific information security responsibilities of users in all levels based on information security policies and procedures requirements and their proper with ***ITG****'s* business goals and objectives. The IS Steering Committee also reviews and recommends approval of IS policies, procedures and projects and reviews long and short range IS strategies and plans to ensure that they are in accordance with ***ITG***'s strategic goals and objectives.

The IS Steering Committee also selects and prioritizes the implementation of IS projects and shall seek advice from the Legal Department whenever a legal dimension or impact is evident in its operational decisions.

Other committees and teams related to information technology policies and procedure guidelines are listed the Information Technology Policy Manual.