



## ***Information Technology Policy Manual***

***October 25<sup>th</sup> 2011***

***201110 – SPV1.0***

© **Amon Technologies** 2011 - All Rights Reserved

**Table of Contents**

Executive Summary.....	6
Introduction .....	6
About Amon Technologies LLC.....	6
Structure .....	7
Summary of Policies .....	8
Committees and Teams .....	9
IT Steering Committee .....	9
Technology Planning and Risk Management Team .....	10
IT Project Management Team.....	10
<b>1 IT Policies &amp; Procedures .....</b>	<b>11</b>
<b>1.1 ITec01 / Organization.....</b>	<b>11</b>
1.1.1 Purpose .....	11
1.1.2 Scope.....	11
1.1.3 Statement.....	11
1.1.4 Related Policies .....	14
1.1.5 Compliance.....	14
1.1.6 Waiver .....	14
1.1.7 Owner .....	15
1.1.8 Custodians .....	15
1.1.9 Domain.....	15
<b>1.2 ITec02 / Strategic Planning.....</b>	<b>16</b>
1.2.1 Purpose .....	16
1.2.2 Scope.....	16
1.2.3 Statement.....	16
1.2.4 Related Policies .....	19
1.2.5 Compliance.....	19
1.2.6 Waiver .....	20
1.2.7 Owner .....	21
1.2.8 Custodians .....	21
1.2.9 Domain.....	21
<b>1.3 ITec03 / Infrastructure Planning.....</b>	<b>22</b>
1.3.1 Purpose .....	22
1.3.2 Scope.....	22
1.3.3 Statement.....	22
1.3.4 Related Policies .....	25
1.3.5 Compliance.....	26
1.3.6 Waiver .....	27
1.3.7 Owner .....	27
1.3.8 Custodians .....	27
1.3.9 Domain.....	28
<b>1.4 ITec04 / Risk Management.....</b>	<b>29</b>
1.4.1 Purpose .....	29
1.4.2 Scope.....	29
1.4.3 Statement.....	29
1.4.4 Related Policies .....	32
1.4.5 Compliance.....	32
1.4.6 Waiver .....	33

1.4.7	Owner .....	33
1.4.8	Custodians .....	33
1.4.9	Domain .....	34
<b>1.5</b>	<b>ITec05 / Asset Management .....</b>	<b>35</b>
1.5.1	Purpose .....	35
1.5.2	Scope .....	35
1.5.3	Statement .....	35
1.5.4	Related Policies .....	38
1.5.5	Compliance .....	38
1.5.6	Waiver .....	39
1.5.7	Owner .....	39
1.5.8	Custodians .....	39
1.5.9	Domain .....	40
<b>1.6</b>	<b>ITec06 / Investment Management .....</b>	<b>41</b>
1.6.1	Purpose .....	41
1.6.2	Scope .....	41
1.6.3	Statement .....	41
1.6.4	Related Policies .....	43
1.6.5	Compliance .....	44
1.6.6	Waiver .....	44
1.6.7	Owner .....	45
1.6.8	Custodians .....	45
1.6.9	Domain .....	45
<b>1.7</b>	<b>ITec07 / Personnel Management .....</b>	<b>46</b>
1.7.1	Purpose .....	46
1.7.2	Scope .....	46
1.7.3	Statement .....	46
1.7.4	Related Policies .....	51
1.7.5	Compliance .....	51
1.7.6	Waiver .....	52
1.7.7	Owner .....	52
1.7.8	Custodians .....	52
1.7.9	Domain .....	53
<b>1.8</b>	<b>ITec08 / Project Management .....</b>	<b>54</b>
1.8.1	Purpose .....	54
1.8.2	Scope .....	54
1.8.3	Statement .....	54
1.8.4	Related Policies .....	58
1.8.5	Compliance .....	58
1.8.6	Waiver .....	59
1.8.7	Owner .....	59
1.8.8	Custodians .....	59
1.8.9	Domain .....	60
<b>1.9</b>	<b>ITec09 / Change Management .....</b>	<b>61</b>
1.9.1	Purpose .....	61
1.9.2	Scope .....	61
1.9.3	Statement .....	61
1.9.4	Related Policies .....	66
1.9.5	Compliance .....	66
1.9.6	Waiver .....	67
1.9.7	Owner .....	67

1.9.8	Custodians .....	68
1.9.9	Domain .....	68
<b>1.10</b>	<b>ITec10 / Operations Management.....</b>	<b>69</b>
1.10.1	Purpose .....	69
1.10.2	Scope.....	69
1.10.3	Statement.....	69
1.10.4	Related Policies .....	72
1.10.5	Compliance.....	72
1.10.6	Waiver .....	73
1.10.7	Owner .....	73
1.10.8	Custodians .....	73
1.10.9	Domain .....	74
<b>1.11</b>	<b>ITec11 / Facilities Management .....</b>	<b>75</b>
1.11.1	Purpose .....	75
1.11.2	Scope.....	75
1.11.3	Statement.....	75
1.11.4	Related Policies .....	78
1.11.5	Compliance.....	78
1.11.6	Waiver .....	79
1.11.7	Owner .....	79
1.11.8	Custodians .....	79
1.11.9	Domain .....	80
<b>1.12</b>	<b>ITec12 / Monitoring IT Processes .....</b>	<b>81</b>
1.12.1	Purpose .....	81
1.12.2	Scope.....	81
1.12.3	Statement.....	81
1.12.4	Related Policies .....	83
1.12.5	Compliance.....	83
1.12.6	Waiver .....	84
1.12.7	Owner .....	84
1.12.8	Custodians .....	84
1.12.9	Domain .....	85
<b>1.13</b>	<b>ITec13 / Supplier Management .....</b>	<b>86</b>
1.13.1	Purpose .....	86
1.13.2	Scope.....	86
1.13.3	Statement.....	86
1.13.4	Related Policies .....	89
1.13.5	Compliance.....	90
1.13.6	Waiver .....	90
1.13.7	Owner .....	91
1.13.8	Custodians .....	91
1.13.9	Domain .....	91
<b>2</b>	<b>Policy Lists And Definitions.....</b>	<b>92</b>
<b>2.1</b>	<b>List of Information Technology Policies .....</b>	<b>92</b>
ITec01	Organization.....	92
ITec02	Strategic Planning .....	92
ITec03	Infrastructure Planning .....	92
ITec04	Risk Management .....	93
ITec05	Asset Management .....	93
ITec06	Investment Management.....	93
ITec07	Personnel Management.....	93

ITec08	Project Management.....	94
ITec09	Change Management.....	94
ITec10	Operations Management.....	94
ITec11	Facilities Management.....	95
ITec12	Monitoring of IT Processes.....	95
ITec13	Supplier Management.....	95
<b>2.2</b>	<b>List of Information Security Policies .....</b>	<b>96</b>
ISec01	Information Security .....	96
ISec02	Organizing Information Security.....	96
ISec03	Data Management & Classification .....	96
ISec04	Personnel Security .....	97
ISec05	Training & Awareness .....	97
ISec06	Physical & Environmental Security .....	97
ISec07	IS Communications & Operations Management.....	97
ISec08	Internet & Intranet Security .....	98
ISec09	Email .....	98
ISec10	Virus Protection .....	98
ISec11	Logical Access Security .....	99
ISec12	Information System Acquisition Development & Maintenance.....	99
ISec13	Information Security Incident Management.....	99
ISec14	Business Continuity Management .....	99
ISec15	Compliance .....	100
<b>2.3</b>	<b>Suggested Rules, Guidelines and Waiver Form .....</b>	<b>101</b>
2.3.1	IT Asset Classification .....	101
2.3.2	Suggested Review Process.....	104
2.3.3	ITec Policy Waiver Request Form.....	106
<b>3</b>	<b>Policy Relations Matrix.....</b>	<b>107</b>
<b>3.1</b>	<b>Policy Relations within ITec Group .....</b>	<b>107</b>
<b>3.2</b>	<b>Policy Cross Reference with ISec Group.....</b>	<b>107</b>
<b>3.3</b>	<b>Policy Owners Table .....</b>	<b>108</b>
<b>3.4</b>	<b>Policy Custodians Reference List .....</b>	<b>109</b>
3.4.1	DG .....	109
3.4.2	Chief Technology Officer .....	109
3.4.3	ICT Department .....	110
3.4.4	Admin Department.....	111
3.4.5	HR Department .....	111
3.4.6	Business Departments / Users.....	111
3.4.7	IT Steering Committee.....	112
3.4.8	IT Project Management Team .....	112
3.4.9	Technology Planning & Risk Management Team .....	112
3.4.10	Risk Department.....	113
3.4.11	Procurement Department .....	113
3.4.12	Business Process Owners.....	113
<b>4</b>	<b>List Of Reviewed Documents .....</b>	<b>114</b>
<b>4.1</b>	<b>ACC Organization Chart.....</b>	<b>115</b>
<b>4.2</b>	<b>ACC ICT Department Organization Chart .....</b>	<b>117</b>
<b>4.3</b>	<b>Current Information Technology Policy .....</b>	<b>118</b>

# Executive Summary

## Introduction

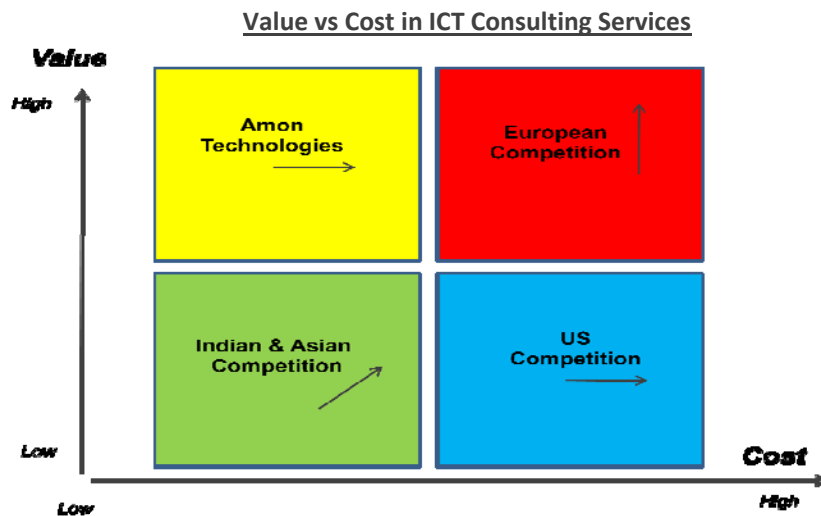
This Information Technology Policies & Procedures manual was compiled for **ACC** in a manner that suitably addresses the organization's environment and operation specific aspects. This manual (together with the Information Security Policy Manual) enables adequate control and security over information 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), as well as prior experiences in conducting similar assignments. This manual is to be adhered to by all IT users and any individuals/groups using the information systems resources of **ACC**. These policies and procedures are applicable to all **ACC's** staff as well as contractors, consultants, third party associates and any temporary staff/visitors having access to **ACC's** information assets

**ACC** 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 was registered in Amman Jordan as. The company is dedicated to and specialized in 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 Technology Policies
- 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 for ACC 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

**Executive 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 (for IT) and ISO27001 (for IS) 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 thirteen separate information technology policies (*ITec*) were formulated for ACC:

- *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




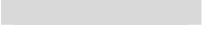
In addition to the thirteen (13) *ITec* policies in this manual, fifteen (15) separate information security policies (*ISec*) were prepared and compiled for ACC:

- *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

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

Overall compliance levels and disciplinary actions are classified as follows. Specific actions need to be developed by ACC's Human Resources and 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 technology policies and procedure guidelines formulated for ACC 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 this manual:

### IT Steering Committee

This committee is composed of the Director General (DG) as the chairman with the membership of the following:

- Head of Finance
- Head of Membership Services
- Chief Technology Officer
- Head of Risk & Compliance (or external consultant)

The IT Steering Committee oversees the proper alignment of IT processes with ACC's business goals and objectives. The IT Steering Committee also reviews and recommends

approval of IT policies, procedures and projects and reviews long and short range IT strategies and plans to ensure that they are in accordance with ACC's strategic goals and objectives. The IT Steering Committee also selects and prioritizes the implementation of IT projects.

## Technology Planning and Risk Management Team

This team is formed and led by the Chief Technology Officer. It consists of representative from Finance, Membership Services and Information Security. The team also includes key business process owners in order to assess the existing technology resources at ACC as well as managers representing ACC's department directors to identify the potential impact on the goals of the organization caused by an unplanned event whereby it shall be identified, analyzed and assessed.

## IT Project Management Team

This team is formed and led by the Chief Technology Officer in order to maintain the program of projects related to the portfolio of ACC's IT investment projects, by identifying, defining, evaluating, initiating and managing and controlling projects. All project management teams shall have a representative of the external project funding agency (if one exists).

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