



Information Security Policy Manual

October 26th 2011 201110 – SPV1.0

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

Table of Contents

EXECUTIVE SUMMARY	7
Introduction	7
About Amon Technologies LLC.....	7
Structure.....	8
Summary of Policies.....	9
Committees and Teams	10
IS Steering Committee	10
1 INFORMATION SECURITY POLICIES	11
1.1 ISec01 / Information Security	11
1.1.1 Purpose.....	11
1.1.2 Scope.....	11
1.1.3 Statement	11
1.1.4 Related Policies	13
1.1.5 Compliance	13
1.1.6 Waiver.....	14
1.1.7 Owner.....	14
1.1.8 Custodians.....	15
1.1.9 Domain.....	15
1.2 ISec02 / Organizing Information Security.....	16
1.2.1 Purpose.....	16
1.2.2 Scope.....	16
1.2.3 Statement	16
1.2.4 Related Policies	22
1.2.5 Compliance	23
1.2.6 Waiver.....	24
1.2.7 Owner.....	24
1.2.8 Custodians.....	24
1.2.9 Domain.....	25
1.3 ISec03 / Data Management & Classification.....	26
1.3.1 Purpose.....	26
1.3.2 Scope.....	26
1.3.3 Statement	26
1.3.4 Related Policies	28
1.3.5 Compliance	28
1.3.6 Waiver.....	29
1.3.7 Owner.....	29
1.3.8 Custodians.....	29
1.3.9 Domain.....	29
1.4 ISec04 / Personnel Security	30

1.4.1	Purpose.....	30
1.4.2	Scope.....	30
1.4.3	Statement	30
1.4.4	Related Policies	34
1.4.5	Compliance	35
1.4.6	Waiver.....	35
1.4.7	Owner.....	36
1.4.8	Custodians.....	36
1.4.9	Domain.....	36
1.5	ISec05 / Training & Awareness	37
1.5.1	Purpose.....	37
1.5.2	Scope.....	37
1.5.3	Statement	37
1.5.4	Related Policies	40
1.5.5	Compliance	40
1.5.6	Waiver.....	41
1.5.7	Owner.....	41
1.5.8	Custodians.....	41
1.5.9	Domain.....	42
1.6	ISec06 / Physical & Environmental Security	43
1.6.1	Purpose.....	43
1.6.2	Scope.....	43
1.6.3	Statement	43
1.6.4	Related Policies	51
1.6.5	Compliance	51
1.6.6	Waiver.....	53
1.6.7	Owner.....	53
1.6.8	Custodians.....	53
1.6.9	Domain.....	54
1.7	ISec07 / IS Communications & Operations Management.....	55
1.7.1	Purpose.....	55
1.7.2	Scope.....	55
1.7.3	Statement	55
1.7.4	Related Policies	66
1.7.5	Compliance	66
1.7.6	Waiver.....	67
1.7.7	Owner.....	68
1.7.8	Custodians.....	68
1.7.9	Domain.....	69
1.8	ISec08 / Internet & Intranet Security	70
1.8.1	Purpose.....	70
1.8.2	Scope.....	70
1.8.3	Statement	70
1.8.4	Related Policies	73
1.8.5	Compliance	73
1.8.6	Waiver.....	74
1.8.7	Owner.....	74
1.8.8	Custodians.....	74
1.8.9	Domain.....	75

1.9	ISec09 / Email.....	76
1.9.1	Purpose.....	76
1.9.2	Scope.....	76
1.9.3	Statement	76
1.9.4	Related Policies	80
1.9.5	Compliance	80
1.9.6	Waiver.....	81
1.9.7	Owner.....	81
1.9.8	Custodians.....	81
1.9.9	Domain.....	82
1.10	ISec10 / Virus Protection	83
1.10.1	Purpose.....	83
1.10.2	Scope.....	83
1.10.3	Statement.....	83
1.10.4	Related Policies.....	87
1.10.5	Compliance	87
1.10.6	Waiver.....	88
1.10.7	Owner.....	88
1.10.8	Custodians.....	88
1.10.9	Domain.....	89
1.11	ISec11 / Logical Access Security	90
1.11.1	Purpose.....	90
1.11.2	Scope.....	90
1.11.3	Statement.....	90
1.11.4	Related Policies.....	101
1.11.5	Compliance	102
1.11.6	Waiver.....	103
1.11.7	Owner.....	103
1.11.8	Custodians.....	103
1.11.9	Domain.....	104
1.12	ISec12 / IS Acquisition, Development & Maintenance	105
1.12.1	Purpose.....	105
1.12.2	Scope.....	105
1.12.3	Statement.....	105
1.12.4	Related Policies.....	112
1.12.5	Compliance	112
1.12.6	Waiver.....	113
1.12.7	Owner.....	113
1.12.8	Custodians.....	114
1.12.9	Domain.....	114
1.13	ISec13 / Information Security Incident Management.....	115
1.13.1	Purpose.....	115
1.13.2	Scope.....	115
1.13.3	Statement.....	115
1.13.4	Related Policies.....	118
1.13.5	Compliance	119
1.13.6	Waiver.....	119
1.13.7	Owner.....	120
1.13.8	Custodians.....	120

1.13.9	Domain.....	120
1.14	I Sec14 / Business Continuity Management	121
1.14.1	Purpose.....	121
1.14.2	Scope.....	121
1.14.3	Statement.....	121
1.14.4	Related Policies.....	126
1.14.5	Compliance	126
1.14.6	Waiver.....	127
1.14.7	Owner.....	127
1.14.8	Custodians.....	127
1.14.9	Domain.....	128
1.15	I Sec15 / Compliance	129
1.15.1	Purpose.....	129
1.15.2	Scope.....	129
1.15.3	Statement.....	129
1.15.4	Related Policies.....	135
1.15.5	Compliance	135
1.15.6	Waiver.....	136
1.15.7	Owner.....	136
1.15.8	Custodians.....	136
1.15.9	Domain.....	137
2	POLICY LISTS AND DEFINITIONS.....	138
2.1	List of Information Security Policies	138
I Sec01	Information Security	138
I Sec02	Organizing Information Security.....	138
I Sec03	Data Management & Classification	138
I Sec04	Personnel Security	138
I Sec05	Training & Awareness.....	139
I Sec06	Physical & Environmental Security	139
I Sec07	IS Communications & Operations Management	139
I Sec08	Internet & Intranet Security.....	140
I Sec09	Email	140
I Sec10	Virus Protection.....	140
I Sec11	Logical Access Security	140
I Sec12	Information System Acquisition Development & Maintenance	141
I Sec13	Information Security Incident Management	141
I Sec14	Business Continuity Management.....	141
I Sec15	Compliance	141
2.2	List of Information Technology Policies.....	142
ITec01	Organization.....	142
ITec02	Strategic Planning.....	142
ITec03	Infrastructure Planning	142
ITec04	Risk Management.....	142
ITec05	Asset Management.....	143
ITec06	Investment Management.....	143
ITec07	Personnel Management.....	143
ITec08	Project Management	143

ITec09	Change Management	144
ITec10	Operations Management.....	144
ITec11	Facilities Management.....	144
ITec12	Monitoring of IT Processes	144
ITec13	Supplier Management.....	144
2.3	Suggested Rules Guidelines and Forms.....	146
2.3.3	Isec Policy Waiver Request Form	146
3	POLICY RELATIONS MATRIX.....	147
3.1	Policy Relations Within ISec group	147
3.2	Policy Cross Reference with ITec group.....	147
3.3	Policy Owners Table	148
3.4	Policy Custodians Reference List	149
3.4.1	Risk & Compliance Division / IS.....	149
3.4.2	Human Resources Department.....	154
3.4.3	IS Steering Committee	155
3.4.4	Department Directors	155
3.4.5	Legal Department	155
3.4.6	Internal Audit Division.....	156
3.4.7	Business Process Owners	156
3.4.8	ICT Department.....	156
3.4.9	Information Asset Owners.....	157
3.4.10	Email Users.....	157
3.4.11	System Administrators	158
3.4.12	Users.....	158
3.4.13	Network Administrators	158
4	LIST OF REVIEWED DOCUMENTS.....	159
4.1	ACC Organization Chart	160
4.2	ACC ICT Department Organization Chart.....	161
4.3	ACC Current IS Policy	162
4.3.1	IS Policy Statement Paper	162

Executive Summary

Introduction

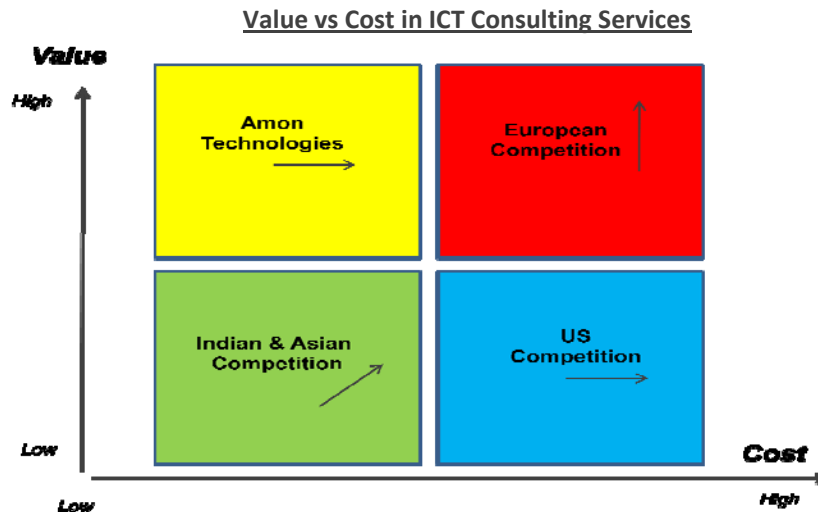
This Information Security Policies & Procedures manual was compiled and developed for ACC in a manner that suitably addresses the organization's environment and operation specific aspects. This manual enables adequate control and security over information systems and helps manage the risks of such systems 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 ACC. These policies and procedures are applicable to all ACC staff as well as contractors, consultants, third party associates and any temporary staff 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 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 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

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 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

In addition to the above fifteen (15) **ISec** policies, thirteen (13) separate information technology (**ITec**) policies 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

These are 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 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 security policies and procedure guidelines formulated for ACC 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 DG as the chairman with the membership of the following:

- Head of Risk & Compliance
- Head of HR
- Chief Technology Officer
- IS Manager

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 ACC'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 ACC'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.