

# Information Technology Policies

---

<b>Client</b>	<i>Client Name</i>
<b>Project</b>	<i>client/Amon Technologies/2009 -</i>
<b>Document</b>	IT Policy Manual
<b>Prepared By</b>	Vatche G. Dakessian
<b>Version</b>	Draft V1.0
<b>Circulation</b>	<i>client Internal Use Only</i>
<b>Date</b>	April 2009

**Table of Contents**

- Executive Summary ..... 6**
- Introduction ..... 6**
- Structure ..... 6**
- Summary of Policies ..... 7**
- Committees and Teams ..... 8**
  - IT Steering Committee ..... 8
  - Technology Planning Team ..... 8
  - Risk Management Team ..... 9
  - Project Management Team ..... 9
- 1 Information Technology Policies ..... 10**
  - 1.1 ITec01 / Organization ..... 10**
    - 1.1.1 Purpose ..... 10
    - 1.1.2 Scope ..... 10
    - 1.1.3 Statement ..... 10
    - 1.1.4 Related Policies ..... 12
    - 1.1.5 Compliance ..... 12
    - 1.1.6 Waiver ..... 13
    - 1.1.7 Owner ..... 13
    - 1.1.8 Custodians ..... 13
    - 1.1.9 Domain ..... 14
  - 1.2 ITec02 / Strategic Planning ..... 15**
    - 1.2.1 Purpose ..... 15
    - 1.2.2 Scope ..... 15
    - 1.2.3 Statement ..... 15
    - 1.2.4 Related Policies ..... 18
    - 1.2.5 Compliance ..... 18
    - 1.2.6 Waiver ..... 19
    - 1.2.7 Owner ..... 19
    - 1.2.8 Custodians ..... 19
    - 1.2.9 Domain ..... 19
  - 1.3 ITec03 / Infrastructure Planning ..... 20**
    - 1.3.1 Purpose ..... 20
    - 1.3.2 Scope ..... 20
    - 1.3.3 Statement ..... 20
    - 1.3.4 Related Policies ..... 23
    - 1.3.5 Compliance ..... 23
    - 1.3.6 Waiver ..... 24
    - 1.3.7 Owner ..... 24
    - 1.3.8 Custodians ..... 24
    - 1.3.9 Domain ..... 25
  - 1.4 ITec04 / Risk Management ..... 26**
    - 1.4.1 Purpose ..... 26
    - 1.4.2 Scope ..... 26
    - 1.4.3 Statement ..... 26
    - 1.4.4 Related Policies ..... 28
    - 1.4.5 Compliance ..... 29
    - 1.4.6 Waiver ..... 29
    - 1.4.7 Owner ..... 30
    - 1.4.8 Custodians ..... 30
    - 1.4.9 Domain ..... 30
  - 1.5 ITec05 / Asset Management ..... 31**
    - 1.5.1 Purpose ..... 31
    - 1.5.2 Scope ..... 31
    - 1.5.3 Statement ..... 31
    - 1.5.4 Related Policies ..... 33
    - 1.5.5 Compliance ..... 34
    - 1.5.6 Waiver ..... 34

1.5.7	Owner .....	35
1.5.8	Custodians.....	35
1.5.9	Domain .....	35
<b>1.6</b>	<b>ITec06 / Investment Management.....</b>	<b>36</b>
1.6.1	Purpose .....	36
1.6.2	Scope.....	36
1.6.3	Statement .....	36
1.6.4	Related Policies.....	38
1.6.5	Compliance.....	38
1.6.6	Waiver.....	39
1.6.7	Owner .....	39
1.6.8	Custodians.....	39
1.6.9	Domain .....	40
<b>1.7</b>	<b>ITec07 / Personnel Management .....</b>	<b>41</b>
1.7.1	Purpose .....	41
1.7.2	Scope.....	41
1.7.3	Statement .....	41
1.7.4	Related Policies.....	45
1.7.5	Compliance.....	45
1.7.6	Waiver.....	46
1.7.7	Owner .....	46
1.7.8	Custodians.....	46
1.7.9	Domain .....	47
<b>1.8</b>	<b>ITec08 / Project Management.....</b>	<b>48</b>
1.8.1	Purpose .....	48
1.8.2	Scope.....	48
1.8.3	Statement .....	48
1.8.4	Related Policies.....	51
1.8.5	Compliance.....	51
1.8.6	Waiver.....	52
1.8.7	Owner .....	53
1.8.8	Custodians.....	53
1.8.9	Domain .....	53
<b>1.9</b>	<b>ITec09 / Change Management .....</b>	<b>54</b>
1.9.1	Purpose .....	54
1.9.2	Scope.....	54
1.9.3	Statement .....	54
1.9.4	Related Policies.....	58
1.9.5	Compliance.....	58
1.9.6	Waiver.....	59
1.9.7	Owner .....	60
1.9.8	Custodians.....	60
1.9.9	Domain .....	60
<b>1.10</b>	<b>ITec10 / Operations Management.....</b>	<b>61</b>
1.10.1	Purpose .....	61
1.10.2	Scope.....	61
1.10.3	Statement .....	61
1.10.4	Related Policies.....	63
1.10.5	Compliance.....	64
1.10.6	Waiver.....	64
1.10.7	Owner .....	65
1.10.8	Custodians.....	65
1.10.9	Domain .....	65
<b>1.11</b>	<b>ITec11 / Facilities Management .....</b>	<b>66</b>
1.11.1	Purpose .....	66
1.11.2	Scope.....	66
1.11.3	Statement .....	66
1.11.4	Related Policies.....	69
1.11.5	Compliance.....	69
1.11.6	Waiver.....	69
1.11.7	Owner .....	70
1.11.8	Custodians.....	70

1.11.9	Domain .....	70
<b>1.12</b>	<b>ITec12 / Monitoring IT Processes .....</b>	<b>71</b>
1.12.1	Purpose .....	71
1.12.2	Scope.....	71
1.12.3	Statement .....	71
1.12.4	Related Policies.....	73
1.12.5	Compliance.....	73
1.12.6	Waiver.....	73
1.12.7	Owner .....	74
1.12.8	Custodians.....	74
1.12.9	Domain .....	74
<b>1.13</b>	<b>ITec13 / Supplier Management .....</b>	<b>75</b>
1.13.1	Purpose .....	75
1.13.2	Scope.....	75
1.13.3	Statement .....	75
1.13.4	Related Policies.....	78
1.13.5	Compliance.....	78
1.13.6	Waiver.....	79
1.13.7	Owner .....	79
1.13.8	Custodians.....	79
1.13.9	Domain .....	80
<b>2</b>	<b>Policy Lists And Definitions .....</b>	<b>81</b>
<b>2.1</b>	<b>List of Information Technology Policies .....</b>	<b>81</b>
ITec01	Organization .....	81
ITec02	Strategic Planning .....	81
ITec03	Infrastructure Planning .....	81
ITec04	Risk Management .....	82
ITec05	Asset Management .....	82
ITec06	Investment Management.....	82
ITec07	Personnel Management.....	82
ITec08	Project Management .....	82
ITec09	Change Management.....	83
ITec10	Operations Management.....	83
ITec11	Facilities Management .....	83
ITec12	Monitoring of IT Processes .....	83
ITec13	Supplier Management .....	83
<b>2.2</b>	<b>List of Information Security Policies .....</b>	<b>85</b>
ISec01	Information Security .....	85
ISec02	Organizing Information Security.....	85
ISec03	Data Management & Classification.....	85
ISec04	Personnel Security .....	85
ISec05	Training & Awareness .....	86
ISec06	Physical & Environmental Security .....	86
ISec07	IS Communications & Operations Management.....	86
ISec08	Internet & Intranet Security .....	86
ISec09	Email.....	86
ISec10	Virus Protection .....	87
ISec11	Logical Access Security .....	87
ISec12	Information System Acquisition Development & Maintenance.....	87
ISec13	Information Security Incident Management .....	87
ISec14	Business Continuity Management .....	88
ISec15	Compliance.....	88
<b>2.3</b>	<b>Suggested Rules, Guidelines and Forms.....</b>	<b>89</b>
2.3.1	IT Asset Classification .....	89
2.3.2	ITec Policy Waiver Request Form.....	92
<b>3</b>	<b>Policy Relation Tables.....</b>	<b>93</b>
<b>3.1</b>	<b>Policy Relations within ITec Group.....</b>	<b>93</b>
<b>3.2</b>	<b>Policy Cross Reference with ISec Group .....</b>	<b>93</b>
<b>3.3</b>	<b>Policy Owners Table .....</b>	<b>94</b>
<b>3.4</b>	<b>ITec Policy Custodians Reference List .....</b>	<b>95</b>
3.4.1	CEO .....	95
3.4.2	IT Manager .....	95

- 3.4.3 IT Department..... 95
- 3.4.4 Procurement Department ..... 96
- 3.4.5 Admin/HR Department ..... 97
- 3.4.6 Business Departments / Users..... 97
- 3.4.7 IT Steering Committee ..... 97
- 3.4.8 IT Project Management Team..... 97
- 3.4.9 IT Risk Management Team ..... 98
- 3.4.10 Technology Planning Team ..... 98
- 3.4.11 Business Process Owners ..... 98
- 4 List Of Reviewed Documents ..... 99**
  - 4.1 client Organization Chart ..... 99**
  - 4.2 client Information Security Policy 2007..... 99**

## Executive Summary

---

### *Introduction*

This IT and Security Policies & Procedures manual was compiled and developed for *the client* 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 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 *client*. These policies and procedures are applicable to all *the client's* staff as well as contractors, consultants, third party associates and any temporary staff having access to *the client's* information assets.

### *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 the *client* 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 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 thirteen separate information technology policies (**ITec**) were formulated for *the client*.

- **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, fifteen (15) separate information security policies (**ISec**) were formulated for *the client*.

- **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 are 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 *the client's* Human Resources and Administration Departments:

Level	Class	Colour Code	Disciplinary Action
1	Critical		
2	Severe		
3	Serious		
4	Major		
5	Minor		

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 *the client* 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

The committee is composed of the CEO; as the chairman, IT Manager, Procurement Director, Internal Audit Director and the Finance Director. It oversees the proper aligning of IT processes with business goals and objectives, review and approve IT policies, procedures and projects and review long and short range IT plans to ensure that they are in accordance with *the client's* strategic goals and objectives.

### Technology Planning Team

This team is formed and led by the IT Manager. It consists of key business process owners in order to assess the existing technology resources at *the client*.

## Risk Management Team

This team is formed and led by the IT Manager, it includes managers representing *the client's* department directors to identify the potential impact on the goals of the organization caused by an unplanned event shall be identified, analyzed and assessed.

## Project Management Team

This team is formed and led by the IT Manager to maintain the program of projects related to the portfolio of *the client's* IT investment projects, by identifying, defining, evaluating, prioritizing, selecting, initiating and managing and controlling projects.

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