

## Professional Services

### Information Security Policies & Procedures

#### Summary Scope

Following is the list of information security policies that are formulated for our clients. The listing for each policy also includes its various components. The sequence and order of listing of policies and areas of coverage is not significant. The IS Policy Manual will cover the following (15) fifteen distinct *IS related* areas:

#### Information Security

- A. Users' general security responsibilities
- B. Information Security Policies and Procedures revision

#### Organization

- A. Internal Organization of Information Security
- B. Information Security Co-ordination and Responsibilities
- C. Information Security Authorization processes and Confidentiality Agreements
- D. Contacting with Authorities and special interest groups
- E. Identifying risks related to external parties
- F. Addressing security for external parties

#### Data Management & Classification

- A. Data Verification and Authorization
- B. Data Classification

#### Personnel Security

- A. Prior to employment checks and induction
- B. Adherence to Employment Terms and Conditions
- C. During employment responsibilities, training and disciplinary processes
- D. Termination or Change of Employment

#### Training & Awareness

- A. Security Awareness
- B. Users' security education and training

#### Physical & Environmental Security

- A. Securing areas
- B. Securing equipment

## Professional Services

### Information Security Policies & Procedures

#### Communications & Operations Management

- A. Operating Procedures and Responsibilities
- B. Third Party Service Delivery Management
- C. System Planning and Acceptance
- D. Protection against Malicious and Mobile Codes
- E. Back-up
- F. Network Security Management
- G. Media Handling
- H. Exchange of Information
- I. Electronic Commerce Services
- J. Monitoring

#### Internet & Intranet Security

- A. Security Issues related to Internet
- B. Security Issues related to Intranet

#### Email

- A. E-mail Usage
- B. E-mail Security Settings
- C. E-mail Retention
- D. E-mail Attachments

#### Virus Protection

- A. Prevention of Virus/Malicious Code
- B. User Responsibilities
- C. Detection of Virus/Malicious Code
- D. Removal of Virus/Malicious Code

#### Logical Access Security

- A. Business requirement for access control
- B. User Access Management
- C. User Responsibilities
- D. Network Access Control
- E. Operating System Access Control
- F. Application and Information Access Control

#### Acquisition Development & Maintenance

- A. Security Requirements of Information Systems
- B. Correct Processing In Applications

## Professional Services

### Information Security Policies & Procedures

- C. Cryptographic Controls
- D. Security of System Files
- E. Security in Development and Support Processes
- F. Technical Vulnerability Management

#### Incident Management

- A. Reporting Information Security Events and Weaknesses
- B. Management of Information Security Incidents and Improvements

#### Business Continuity Management

- A. Information Security Aspects of Business Continuity Management

#### Compliance

- A. Compliance with Legal Requirements
- B. Compliance with Security Policies and Standards, and Technical Compliance
- C. Information Systems Audit Considerations

For each of the fifteen IS Policies, the following details will be provided:

- **Purpose** of the policy
- **Scope** of the policy
- **Statement** of the policy, sub policy components and list of associated procedures
- **Related policies** within the same IS group policies
- **Related policies** within the IT group of policies
- **Compliance** measurement
- **Waiver** criteria
- **Owner** of the policy
- **Custodian(s)** of the policy and each related sub policy
- **Domain** of the policy (COBIT)

## Professional Services

### Information Security Policies & Procedures

The IS Policy Manual will be customized for our clients in a manner that suitably addresses their organization's environment and operation specific aspects. The IS Policy Manual will enable adequate control over all information systems and typically help manage information system risks effectively. The manual will take into account the recommendations of Control Objectives for Information and Related Technology (COBIT, ISO 27001) as well as prior experiences in conducting similar assignments

For each policy, general guidelines for developing associated procedures will be provided. The resulting IS Policy Manual is a structured, professionally prepared document that should be adhered to by all IT users and any individuals/groups using the information systems resources of the client.