



e-Government Program (Yesser)

Recommended ICT Security Policy Guidelines for Governmental Agencies

Disclaimer

The Saudi e-Government Program (Yesser) has exerted its best effort to achieve the quality, reliability, and accuracy of the information contained in this document. Yesser assumes no liability for inaccurate, or any actions taken in reliance thereon. Yesser encourages readers/visitors to report suggestions on this document through the "Contact Us" on Yesser website.

Version 1.0
Date: 3/12/2007

Table of Contents

1. Introduction	3
1.1. Purpose	3
1.2. Responsibilities	4
2. Policies	5
2.1. Information Security Policy	5
2.2. Risk Assessment Policy	5
2.3. Asset Management Policy	6
2.4. Organization of Information Security	7
2.5. Human Resources Policy	7
2.6. Access Policy	8
2.7. Physical and Environmental Security	8
2.8. Communication and Operation Management	9
2.9. Information System Acquisition, Development and Maintenance	10
2.10. Information Security Incident Management Policy	11
2.11. Business Continuity Management Policy	12
2.12. Compliance Policy	13
3. Check List	14

1. Introduction

The selection and employment of appropriate security controls for information systems are important tasks that can have major implications on the operations and assets of any Governmental Agency as well as the benefit of individuals. Security controls are the management, operational, and technical safeguards or countermeasures prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

Governmental Agencies are required to employ security controls to meet security requirements defined by Saudi laws through Executive Orders, directives, policies, standards, or regulations.

The challenge for Government Agency is to determine the appropriate set of security controls, which if implemented and determined to be effective in their application, would most cost-effectively comply with security requirements.

Selecting the appropriate set of security controls to meet the specific, and sometimes unique, security requirements of a Government Agency is an important task—a task that demonstrates the Agency's commitment to security and the due diligence exercised in protecting the confidentiality, integrity, and availability of their information and information systems.

To assist Agencies in making the appropriate selection of security controls for their information systems, the concept of baseline controls is introduced. Baseline controls are the minimum security controls recommended for an information system.

1.1. Purpose

The purpose of this document is to provide guidelines for employing and specifying security controls for information systems supporting the Governmental Agencies in the Kingdom of Saudi Arabia, as declared by rule (21) from e-Government Implementation Rules issued by Council of Ministers Resolution no. (40) Dated 27/3/2006 (To view e-Government Implementation Rules, visit: <http://www.yesser.gov.sa>).

This document applies to all components of any information system that process, store, or transmit governmental information and it helps to achieve more secure information systems within the government agencies by:

- Facilitating a more consistent, comparable, and repeatable approach for selecting and specifying security controls for information systems.
- Providing a recommendation for minimum security controls for information systems within governmental Information systems.
- Providing a stable, yet flexible catalog of security controls for information systems to meet current agencies protection needs and the demands of future protection needs based on changing requirements and technologies.
- Creating a foundation for the development of assessment methods and procedures for determining security control effectiveness.

1.2. Responsibilities

As a baseline to protect Public and National Information, all Government Agencies must develop, disseminate, and periodically review/update:

1. A formal, documented, policy that addresses purpose, scope, roles, responsibilities, and compliance.
2. Formal, documented procedures to facilitate the implementation of the policy and associated controls.

2. Policies

Below are the security policies as per the ISO 27001 security standards, government agencies can start with these policies as a baseline and then based on the requirements and selection of the policies, they can develop corresponding procedures.

2.1. Information Security Policy

Information security is vital to all Governmental Agencies; it aims to the protection of data resources against loss arising from breaches of confidentiality, integrity and availability. It should not be seen as preventative or restrictive of day to day operations, but rather as an enabling mechanism for sharing information safely.

Information security protects information from a wide range of threats in order to ensure business continuity, minimize damage and maximize the utilization of information systems. This policy **must** cover but not limited to the following categories:

- Update of Information Security Documentation.
- Modification of Information Security Documentation
- Control changes of Documentation.
- Track of documentation.

2.2. Risk Assessment Policy

The increased usage of technology and the deteriorating security landscape brings growing security concerns due to a variety of existing and emerging threats and risks. This can cause information unavailability, breach of its confidentiality or integrity resulting in the loss of/impact to the revenue, customer service, operations or the reputation.

Risk management function assists in identifying the various risks to which a government agency is exposed to and includes the process of managing the risks to maximize business benefits.

This policy **must** cover but not limited to the following categories:

- **IT Asset Inventory**

Any Governmental Agency must maintain a complete and comprehensive inventory of all its information assets at all times. Assets that must be logged into this inventory include:

- Information assets.
- Software assets.
- Hardware assets.
- Human Resources.
- Physical assets.
- Services.

- **Risk Assessment**

All governmental Agencies **must** identify reasonably foreseeable internal and external threats to the integrity of information on the Information systems. In addition, all agencies should assess the likelihood and potential damage of these threats, taking into consideration the criticality and/or sensitivity of the information systems.

▪ **Risk classification**

Risk classification will enable All Governmental Agencies to focus asset protection mechanisms on those assets that are most susceptible to specific risks. Information assets will be assigned classifications based on their susceptibility to risk. The risks affecting information assets are:

- a. Loss of Confidentiality.
- b. Loss of Integrity.
- c. Loss of Availability.

▪ **Acceptable Risk level**

In All Governmental Agencies, its management responsibility to determine the acceptable level of risk because they intimately understand the agency's operational drivers and the corresponding impact if these operational objectives are not met. Also, it is management's ultimate responsibility to ensure that the agency meets these operational objectives and goals. The "Information security Officers" job to illustrate to management how underlining security threats can negatively affect objectives of the government agency.

2.3. Asset Management Policy

All assets are not equally important for all governmental agencies operations, and for achieving its vision and mission. Some assets are more important than others and therefore need additional care and protection. This requires Information Systems assets to be accordingly classified.

Risk classification will enable the governmental agency to focus on asset protection mechanisms on those assets that are most susceptible to specific risks. Information assets will be assigned classifications based on their susceptibility to risk

This policy **must** cover but not limited to the following categories:

▪ **Asset Classification Criteria**

All assets are not equally important for the Governmental Agency's operations and for achieving its vision and mission. Some assets are more important than others and therefore need additional care and protection to keep the Agency's operation. This document should provide the criteria based on which the assets are to be classified.

▪ **Levels of Classification**

All data and data documentation shall be classified strictly according to its level of confidentiality, sensitivity, value and criticality.

▪ **Classification Scheme**

Information should be classified to indicate the need, priorities, and degree of protection. A defined scheme should be identified and adopted in order to classify assets that already exist in the environment or are to be introduced in to the environment.

2.4. Organization of Information Security

This policy aims to manage information security within any governmental agency and maintain appropriate security controls in the information processing facilities within the agency or outsourced to third parties.

This policy **must** cover but not limited to the following categories:

- **Management Security Forum**

All Governmental Agencies should establish an Information Security Committee (ISC) to ensure that there is proper direction and management support for all security initiatives.

- **Information Security Roles and Responsibilities**

The ISC within all Governmental Agencies should formalize the process of assigning roles and responsibilities for information security across the organization.

- **Information Security Authorizations**

In all Governmental Agencies, Management authorization should be sought for any change or addition of information processing facilities.

2.5. Human Recourses Policy

An important part of Information Security relies on policies related to Human Resources Management. The objectives of information security can largely be achieved with the insertion of specific clauses to the personnel contracts, with the implementation of appropriate measures in the processes of personnel hiring, departure and dismissal, with the appropriate allocation of duties and responsibilities as well as with the continuous training and awareness of personnel.

This policy **must** cover but not limited to the following categories:

- **Personnel Screening and Record Keeping**

Personnel screening is required when an employee joins All Governmental Agencies. All the personal details of a potential employee must be checked before he joins the agency. The Human Resources (HR) department is responsible for performing personnel screening.

- **General Employment Rules**

Human Resources department within any Governmental Agency should ensure that all users "job descriptions" will document that they are required to comply with all security policies in the agency.

- **User Awareness and Training**

All Governmental Agencies employees should receive security awareness training and should follow best security practices at their jobs.

- **Change of Duties or Employee Departure**

Formal documented instructions should be available in HR department of All Governmental Agencies, which include appropriate security measures, for the duty changing or ending of an employee's employment.

- **Legal and Contractual Issues**

All Governmental Agencies employees should be familiarized with all Legal/ Contractual issues/ consequences in the terms of not properly following the security guidelines, violating the security policy or leaking sensitive information outside of the agency.

2.6. Access Policy

All Government Agencies own and operate information systems which are used by users to support its operations. Information systems include personal computers, servers, networks, applications and data stored in systems are all property of the Agency. All users should use the systems in an efficient, ethical and legal manner.

This policy **must** cover but not limited to the following categories:

- **Proper use of Information Systems**

Access to information will be controlled on the basis of operations and security requirements, in addition to access control rules defined for each information system.

- **Internet Services and Email Systems**

The usage of Internet and email within All Governmental Agencies are explicitly for work purposes only, authorized users must comply with the respective Security Policy.

- **Encryption Mechanisms**

All personnel using remote access must be provided with a secure connection (E.g.: Secure Socket Layer, IPSec, Virtual Private Network, encryption) to any Governmental Agency's information system networks.

- **Passwords**

All users of the Governmental Agencies must follow the agency's password policy regarding their passwords usage and management.

- **Corporate Information Disclosure**

Governmental Agencies must establish all the security access controls within their environment to ensure non disclosure of the corporate information.

- **Storage**

Governmental Agencies must ensure that all the security access controls have been implemented to limit the accessibility to the storage facility within its environment.

2.7. Physical and Environmental Security

The purpose of this policy is to prevent unauthorized physical access to the agency facilities, information assets and information systems, as well as to address physical and environmental threats that can harm the confidentiality, integrity and availability of agency information and information systems.

This policy **must** cover but not limited to the following categories:

- **Physical and Environmental Security General Issues**

The physical layout of all Governmental Agencies information processing facilities must be segregated into perimeter zones. Each zone will have a different level of access restrictions and access authorization requirements.

- **Facility Construction and Design**

All Governmental Agencies facilities should be provided with adequate provisions for fire detection and control and air conditioning systems which should be implemented to ensure an adequate operational environment.

- **Monitoring and Controlling Physical Access**

All Governmental Agencies should ensure that monitoring systems are deployed to track any suspicious activity within the agency's premises.

- **Controlling Incoming and Outgoing Objects**

Materials, supplies and equipments entering and leaving any Governmental Agency's premises must be inspected and where necessary registered in accordance with Agency's Physical Security Policy.

- **Workplace Security**

All governmental agencies must ensure that all work must be done under supervision of the respective department management.

2.8. Communication and Operation Management

This policy aims to ensure the right and secure operation of information processing facilities; to minimize risk due to system failures and to safeguard the integrity of information processing facilities and software. This policy also suggests guidelines to ensure secure network operations and exchange of information within the government agency.

This policy **must** cover but not limited to the following categories:

- **Operational Management**

All Governmental Agencies must ensure the existence of all operating procedures needed to support/implement the security policies and it will be documented and maintained. Changes to all information systems should be controlled through a formal change management process.

- **Separation of Test and Operational Facilities**

In all Governmental Agencies, new systems must be tested in a testing/staging environment before introducing them to operation. Testing/Staging environment must be completely separated from operational environment.

- **Operator Logs**

Operational staff of all Governmental Agencies corporate network as well as in the Network Operation Center staff should maintain a log of their activities. These Operator logs should be subject to regular checks to ensure compliance with Operating procedures.

- **Security of System Documentation**

All Governmental Agencies must ensure that system or application documentation that supports the Agency's departments, and which is used by programming, operations, and user personnel, must be developed, maintained, and protected.

2.9. Information System Acquisition, Development and Maintenance

The purpose of this policy is to set the principles used in the acquisition, the development and the maintenance of agency information assets. This policy addresses IT asset development and maintenance conducted either by Agency personnel or by external partners.

Security has to be a primary property of the information systems developed and used by the Agency. Information systems must be designed, developed, connected to other systems, managed, monitored and operated in such a way that client trust is promoted, compatibility with the regulatory framework is ensured and the Government Agency goals are supported.

This policy **must** cover but not limited to the following categories:

- **Acquisition / Development of Information Systems and Applications**

In All Governmental Agencies, the development of information systems must make use of established methodologies, technologies and tools in accordance with international best practices.

- **Information Systems Design Principles**

In the case of a new information system acquisition or development in All Governmental Agencies, by an external partner the IT Systems Development Division conducts a thorough study to determine the requirements.

- **Source Code**

In order to minimize the threat of partial or total destruction of all Governmental Agencies applications due to unauthorized changes (on purpose or not) there must be strict control in accessing the source code.

- **Information Systems Testing and Acceptance**

In all Governmental Agencies, once the acquisition / development of an information system has been completed and before it is placed in the production environment, a Security Review/ Testing must be conducted using possible threat scenarios according to the system's criticality.

- **Information Systems Installation**

In all Governmental Agencies, the placement of an information system in a production environment must be conducted by employees that were not responsible for the system development.

- **Information Systems Manuals**

System and application manuals must be developed prior to their placement on the production environment in all Governmental Agencies.

- **Information Systems Operation and Maintenance**

All Governmental Agencies systems should be operated according to approve policy as well as the process of maintenance must be documented and approved.

- **Information Systems Decommissioning**

The decommissioning of all Governmental Agencies information systems must only be conducted when their use is no longer necessary and there is no requirement (e.g. legal, business, etc.) to restore files produced on those systems.

2.10. Information Security Incident Management Policy

The purpose of this policy is to develop a framework for timely and effective handling of information security incidents. An information security incident is a suspected or confirmed violation of the integrity, availability or confidentiality of the government information that could cause or has caused harm to the agency.

The detection of potential information security incidents constitutes an action according to which it is timely identified and at the same time protects against real incidents intended to compromise the security posture of the government agency.

This policy **must** cover but not limited to the following categories:

- **Identification of Security Incidents**

In All Governmental Agencies, user and IT personnel should be responsible for identifying and reporting any incidents.

- **Limitation of Security Incidents**

In All Governmental Agencies, the Security Incident Handling Team in cooperation with the Information Owners must prioritise the tasks that have to be performed in order to handle the incident.

- **Incident Detection and Elimination**

In All Governmental Agencies, the Security Incident Handling Team must perform an IT Security Audit of the involved information systems in order to detect potential vulnerabilities that caused the incident, or were caused by the incident.

- **Recovery of Information Systems**

In All Governmental Agencies, when a security incident has been successfully handled, the IT manager in corporation with the System Administrators must check the security settings so that the adequacy of the security mechanisms can be confirmed.

- **Analysis of Security Incidents**

In all Governmental Agencies, when a security incident has been successfully handled, a full analysis and documentation thereof must be conducted, covering causes, direct or indirect impacts and actions that have been followed.

- **Legal and Disciplinary Procedures**

In all Governmental Agencies, when a security incident has been confirmed to have been caused by an employee, the case must be examined and the appropriate disciplinary / legal actions must be taken.

- **Third Parties Update**

In all Governmental Agencies, information related to security incidents must never be communicated to third parties (e.g. public, journalists, etc.).

2.11. Business Continuity Management Policy

The purpose of this policy is to establish the framework for the proper operational continuity management of the agency, in order to restrict, to the possible extent, the impacts derived from potential interruption to its business activities and ensure the continuity of critical operations in case of partial or total destruction.

This policy **must** cover but limited to the following categories:

- **Development of a Business Continuity Planning Framework**

A single strategy / framework for the continuity plans should be maintained to ensure consistency and establish priorities within all Governmental Agencies. Each continuity plan should state clearly the criteria for activation and list the individuals (with deputies) responsible for executing the plan.

- **Business Continuity Plan (BCP) Development and Disaster Recovery Planning (DRP)**

All Governmental Agencies should maintain a managed process for developing and maintaining business continuity and Disaster recovery plans throughout the agency. It should bring together all the key elements of business continuity and disaster recovery management that should be consistent with the agreed agency objectives and priorities.

- **Recovery Mechanisms Development & Implementation**

Each plan for all Governmental Agencies should contains essential information for preparing, and recovering from, an incident. This could include: recovery strategy, Business Impact Analysis (BIA) results and Detail of recovery teams, members and tasks etc...

- **Backup Management**

Backup for Governmental Agencies should be taken regularly to ensure that data can be recovered when required. Components which need to be backed up should be defined for each application and the backup scheduling should be done to ensure that all critical data is backed up without affecting system operations.

2.12. Compliance Policy

Information processing and design, operation, use and management of information systems are subject to regulatory controls, as well as to obligations derived from agreements of the Governmental Agency with third parties. This policy addresses the basic obligations that derived from the current regulatory framework concerning information security.

The policy aims to cover

The design, operation, use and management of information systems may be subject to statutory, regulatory and contractual requirements. Appropriate policies should be defined and followed to ensure such compliance. The objective for ensuring compliance is to avoid breaches of any criminal and civil law, and statutory, regulatory or contractual requirements. It also ensures that the technology implemented in all Governmental Agencies is compliant against a standard and periodic reviews and audit are conducted for:

- Defining the Regulatory Framework about Information Security.
- Protection of Personal Data.
- Communications Secrecy.
- Intellectual Property.
- Software Licensing.
- Encryption.
- Information Protection.
- Monitoring and Auditing System Use.
- Collection of Evidence.
- Employment Contracts.
- Third Party Agreements.
- Other Issues.

3. Check List

Policy Name	Policy Criticality	Policy Version	Policy Owner
Information Security Policy			
Risk Assessment Policy			
Asset Management Policy			
Inventory of Assets			
Information Classification			
Information Labeling and Handling			
Organization of Information Security			
Management Commitment to Information Security			
Allocation of Information Security Responsibilities			
Addressing Security in Third Party Agreements			
Human Resources Policy			
Information Security Responsibility in Employee Handbook and Contract			
Information Security Awareness			
Disciplinary Process			
Access Policy			
User Registration			
User Password Management			
Review of User Access Rights			
Clear Desk and Clear Screen Policy			
Mobile Computing and Communications			
Physical & Environmental Security			
Physical Entry Controls			
Securing Offices, Rooms, and Facilities			
Public Access, Delivery, and Loading Areas			
Secure Disposal or Re-use of Equipment			
Communication & Operation Management			
Documented Operating Procedures			
Change Management			
Separation of Development, Test, and Operational Facilities			
Monitoring and Review of Third Party Services			
Controls Against Malicious Code			
Information Back-Up			
Information Exchange Policies and Procedures			
Electronic Messaging			
Information System Acquisition, Development & Maintenance			
Security Requirements Analysis and Specification			
Control of Operational Software			
Information Security Incident Management Policy			
Reporting Information Security Events and Weaknesses			

Policy Name	Policy Criticality	Policy Version	Policy Owner
Business Continuity Management Policy			
Developing and Implementing Continuity plans Including Information Security			
Compliance Policy			
Identification of Applicable Legislation			
Intellectual Property Rights (IPR)			
Data Protection and Privacy of Personal Information			
Compliance with Security Policies and Standards			
Information Systems Audit Controls			