Sultanate of Oman
Information Technology Authority

e.oman

Basic Security Controls

Governance and Standards Division

VALIDATION & DISTRIBUTION:

	Name	Email	Issue date
Issued by	Governance & Standards Division	standards@ita.gov.om	30/7/2017
Verified by	ISD		
Approved by	Steering Committee		

Distribution List	
1.	ITA
2.	All concerned government agencies
3.	Online publishing

DOCUMENT REVISION HISTORY:

Version	Date	Author	Remarks
1.0	30/7/2017	Governance & Standards Division	Creation of document

1 Table of Contents

2 Glossary

Access Control

The process of granting or denying specific requests to: 1) obtain and use information and related information processing services; and 2) enter specific physical facilities (e.g., federal buildings, military establishments, border crossing entrances).

Audit

Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.

Baseline configuration

A set of specifications for a system, or Configuration Item (CI) within a system, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures. The baseline configuration is used as a basis for future builds, releases, and/or changes

Denial of Service (DoS)

The prevention of authorized access to resources or the delaying of time-critical operations. (Time-critical may be milliseconds or it may be hours, depending upon the service provided.)

Malware

A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim’s data, applications, or operating system or of otherwise annoying or disrupting the victim.

Incidnet

A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.

Incident Reponse Plan

The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyber attacks against an organization’s information system(s).

Marking

	Human-readable information affixed to information system components, removable media, or output indicating the distribution limitations, handling caveats, and applicable security markings
Media Sanitization	A general term referring to the actions taken to render data written on media unrecoverable by both ordinary and extraordinary means.
Patch Management	The systematic notification, identification, deployment, installation, and verification of operating system and application software code revisions. These revisions are known as patches, hot fixes, and service packs.
Remediation Plan	A plan to perform the remediation of one or more threats or vulnerabilities facing an organization's systems. The plan typically includes options to remove threats and vulnerabilities and priorities for performing the remediation.
Risk Management	The process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system, and includes: 1) the conduct of a risk assessment; 2) the implementation of a risk mitigation strategy; and 3) employment of techniques and procedures for the continuous monitoring of the security state of the information system
Security Impact Analysis	The analysis conducted by an organizational official to determine the extent to which changes to the information system have affected the security state of the system.
Vulnerability	A weakness in a system, application, or network that is subject to exploitation or misuse.

Related Documents

This document is to be used in accordance to the below list of documents:

- Government Network Security Arcitucture Framework
- Government Application and eServices Security Arcitucture Framework
- End Point and Smart Devices Security Arcitucture and Configuration Framework
- ITA Information Seurity Policy Manual

3 Purpose

The purpose of this document is to establish security baselines for government organizations in Oman in order to provide proper security measures to safeguard the valuable information assets within the organization. This document provide a list of controls under selected domains that are considered to be key elements of a complete security program inside the organization.

4 Audience

These guidelines were designed to assist several Security Professionals including Information Security Officers (ISOs), IT Security Operations staff, Security Assessors and Auditors. It serves as a valid reference to solutions architects and developers as well for integrating security basic elements within their product design.

5 Basic Security Controls

Government organizations should be able to cover the minimum security controls required to reach a comprehensive level of security protection. Focusing on the technical controls alone for instance will not guarantee effective prevention of security threats. These guidelines have covered the wider spectrum of security to include all aspects related to this domain. There are twelve areas considered to be very essential and thus were set as baselines that need to be implemented and maintained by government entities. Several controls under each one of those areas were listed to ensure minimum protection levels (summarized as a checklist in the appendix).

5.1 Access Controls

Access at all levels should be well controlled to allow only authorized access to the organization`s resources. Proper policies and procedures should be defined and well maintained. Users and systems accounts should be managed and monitored. Access and Information flow should be effectively enforced. There has to be certain measures to ensure separation of duties and users need to be given the least privileges on their accounts to carry their duties. Systems use notifications should be enabled and used for monitoring. Certain measures need to be implemented to ensure secure communication via remote and wireless connections. Mobile devices use at the organization`s network should be controlled through a defined acceptable use Wireless Access

5.2 Awareness and Training

Government organizations should develop user security policies that describe acceptable and secure use of the organization’s ICT systems. These should be formally acknowledged in employment terms and conditions. All users should receive regular training on the security risks they face as employees and individuals. Security related roles (such as system administrators, incident management team members and forensic investigators) will require specialist training.

5.3 Incident Management

The organization should establish an incident response and disaster recovery capability that addresses the full range of incidents that can occur. All incident management plans (including disaster recovery and business continuity) should be regularly tested. An incident response team may need specialist training across a range of technical and non-technical areas. Incident reporting mechanism should be defined and followed across the organization to allow corrective actions and remediation, as well as assist in learning threats patterns which helps in defining the required incident response plan.

5.4 Media Protection

Removable media policies that control the use of removable media for the import and export of information should be defined and implemented. Where the use of removable media is unavoidable, limit the types of media that can be used together with the users, systems, and types of information that can be transferred. Scan all media for malware using a standalone media scanner before any data is imported into your organization's system. Marking should be done for all Medias. Media storage and transport should be secured to protect the information carried within. When the data within media is no longer needed effective sanitization methods should be used.

5.5 Configuration Management

The organizations should develop, document, and maintain under configuration control, a current baseline configurations. That should cover all information systems and network devices. They should maintain a proper defined change management process with a defined approval workflow. Security Impact analysis should be done for any change to minimize risks associated with implementing the changes.

5.6 Risk Assessment

Government oorganizations are responsible to assess the risks of its information assets with the same level it does for legal, regulatory, financial or operational risks. To achieve this, they should embed an Information Risk Management Regime across the organization, supported by the Board, senior managers and an empowered information assurance (IA) structure. They should consider communicating their risk management policy across the organization to ensure that employees, contractors and suppliers are aware of the organization's risk management boundaries. They should run regular security assessments and run a vulnerability scanning on scheduled basis to monitoring their technical controls status. Those assessments should consider security categorizing scheme to highlight the major findings that need to be addressed in the reporting.

5.7 Network Security

Organizations should follow recognized network design principles defined in “Government Network Security Architecture Framework” that has been released by ITA when configuring perimeter and internal network segments, and ensure all network devices are configured to the secure baseline build. They should filter all traffic at the network perimeter so that only traffic required to support their business is allowed, and monitor traffic for unusual or malicious incoming and outgoing activity that could indicate an attack (or attempted attack).

5.8 Systems and Communication Protections

Organizations should have a defined policy to enforce the implementation of security controls that safeguard systems and communications. They should have a clear defined map of its boundaries to defined all required controls and monitoring to protect any incoming communication from external to their key internal systems. They should be segregating their internal environment from the public network. They should as well implement sufficient controls to limit or minimize impact of any Denial of Service attack that could interrupt their systems. Government organizations. Government organizations can use cryptography can be employed to support different security solutions including (i.e. the protection of classified and controlled unclassified information, the provision of digital signatures, and the enforcement of information separation when authorized individuals have the necessary clearances for such information but lack the necessary formal access approvals).

Organizations should ensure having an effective patch management controls on all of their systems and devices to maintain up-to-date systems. They should implement active malware protection on exposed computers and devices as well. Organizations can refer to “End Point Security Framework” realised by ITA for more details on systems protection.

5.9 Security Assessment and Authorization

Government organizations should have a defined policy for security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. Either they have it as a separate policy or include it within the general security policy of the organization. Associated authorization controls for conducting the security assessment should be implemented.

The security assessments should be run regularly to assess different components of the IT environment following defined procedures as per the ministrial circular (1/2017). Authorization controls for conducting the required tests should be set along with that. Verification tests should be conducted to follow up on the remediation plan.

5.10 Physical and Environmental Protection

Government Organizations should define a policy and procedures for Physical and Environmental Protection. It should implemented the required controls to ensure secure and authorized access with effective monitoring. It should install deduction and prevention systems such as Emergency Lighting, Fire Protection, and Temperature and Humidity Controls.

5.11 Personnel Security

Organizations should have a defined policy and procedures for handling Personnel Security. Security controls should be implemented for all stages of employment that includes: screening process, termination of the staff, and Transfer from one unit to another inside the organization. Access controls for personnel should be verified at any change of the employment status. The personnel security should also cover controls related to third party staff who may require different considerations.

5.12 Audit and Acountability

Organizations should have a defined policy and procedures for Audit and Accountability. They should conduct regular audits on all aspects covered by their security policies. The content of audit reports should be proactively set as audit logs need to be enabled on all systems and devices with configured reporting mechanism to obtain the required audit events and records. Audit information should be protected and should be available for review and analysis. Reporting of the audit results should be communicated to enhance the security levels and ensure mature culture.

6 Appendix

6.1 Basic Security Controls Checklist

Control ID	Access Control	Status
AC.1	Access Control Policy and Procedures	
AC.2	Account Management	
AC.3	Access Enforcement	
AC.4	Information Flow Enforcement	
AC.5	Separation of Duties	
AC.6	Least Privilege	
AC.7	System Use Notification	
AC.8	Remote	
AC.9	Wireless Access	
AC.10	Access Control for Mobile Devices	
AC.11	Use of External Information Systems	
Control ID	Security Awareness and Training	Status
SAT.1	Security Awareness and Training Policy and Procedures	
SAT.2	Security Awareness Training	
SAT.3	Role-Based Security Training	
Control ID	Audit and Accountability	Status
AA.1	Audit and Accountability Policy and Procedures	
AA.2	Audit Events	
AA.3	Content of Audit Records	

AA.4	Audit Storage Capacity	
AA.5	Response to Audit Processing Failures	
AA.6	Audit Review, Analysis, and Reporting	
AA.7	Time Stamps	
AA.8	Protection of Audit Information	
AA.9	Audit Generation	
Control ID	Security Assessment and Authorization	Status
SAA.1	Security Assessment and Authorization Policies and Procedures	
SAA.2	Security Assessments	
SAA.3	System Interconnections	
Control ID	Configuration Management	Status
CM.1	Configuration Management Policy and Procedures	
CM.2	Baseline Configuration	
CM.3	Configuration Change Control	
CM.4	Security Impact Analysis	
CM.5	Configuration Settings	
CM.6	Least Functionality	
CM.7	Information System Component Inventory	
CM.8	Software Usage Restrictions	
Control ID	Incident Response	Status
IR.1	Incident Response Policy and Procedure	
IR.2	Incident Response Training	
IR.3	Incident Handling	
IR.4	Incident Monitoring	

IR.5	Incident Reporting	
IR.6	Incident Response Assistance	
IR.7	Incident Response Plan	
Control ID	Media Protection	Status
MP.1	Media Protection Policy and Procedures	
MP.2	Media Access	
MP.3	Media Marking	
MP.4	Media Storage	
MP.5	Media Transport	
MP.6	Media Sanitization	
MP.7	Media Use	
Control ID	Physical and Environmental Protection	Status
PEP.1	Physical and Environmental Protection Policy and Procedures	
PEP.2	Physical Access Authorizations	
PEP.3	Physical Access Control	
PEP.4	Monitoring Physical Access	
PEP.5	Emergency Lighting	
PEP.6	Fire Protection	
PEP.7	Temperature and Humidity Controls	
PEP.8	Water Damage Protection	
PEP.9	Delivery and Removal	
Control ID	Personnel Security	Status
PS.1	Personnel Security Policy and Procedures	
PS.2	Personnel Screening	

PS.3	Personnel Termination	
PS.4	Personnel Transfer	
PS.5	Access Agreements	
PS.6	Third-Party Personnel Security	
Control ID	Risk Assessment	Status
RA.1	Risk Assessment Policy and Procedures	
RA.2	Security Categorization	
RA.3	Risk Assessment	
RA.4	Vulnerability Scanning	
Control ID	System and Communications Protection	Status
SCP.1	System and Communications Protection Policy and Procedures	
SCP.2	Boundary Protection	
SCP.3	Denial of Service Protection	
SCP.4	Public Key Infrastructure Certificates	
SCP.5	Malware Protection	
SCP.6	Patching Management	

7 References

1. Royal Decree 1/2017 on Conducting Security Assessment for applications and e-services.
2. Kisse. R, “Glossary of Key Information Security Terms”, NISTIR 7298, Revision 2, 2013.