

Sultanate of Oman
Ministry of Education

Legal and Regulations For Information Security

First Edition
2009

Prepared by: Amna bent Eshaq AL Balushi

Revised By: Sameer ben Khalifa AL Orimi

Direcorate General of Information Technology



المبادرات التعليمية

Introduction

The purpose of the Security Guidance Manual is to deal with Information Systems Security at the Ministry of Education, Oman. It aims to provide all Directorates under the Ministry with instructions and guidance on how to deal with information, computer programs and electronic correspondence using the computer. In addition, this guide will show how to maintain necessary security levels between different departments. All Ministry employees, including computer users, have been provided with a copy of this guide. The heads of all directorates will provide a copy to all new employees. The Ministry will host an updated copy of this guide on its website “www.mow.gov.om”.

Classification of Information

The definition of information:

Information is an asset like other important asset which is essential to an organization's business and consequently it needs to protect it appropriately.

Information can exist in many forms:

- Information stored on computer.
- Information transferred across communication networks
- Written information on the cards
- Information sent via fax
- Information stored on hard disks or mobile devices
- Information stored on the mobile disk storage
- Information that will be telecommunicated.

Note:

You must take into account the provision of an appropriate method to protect, preserve the transfer and circulation of information.

Which should deal with the matters of the country with some confidentiality , according to that there is a need of finding a clear classification of the

categories of information that the government wants to protect The Security classifications and the rules of government secrets are explained in the following:

a. **Highly confidential:** This classification is the highest security rating is used to protect vital information, whether political, economic or defensive in nature or security that disclosure would cause serious harm to the Sultanate.

b. **Confidential:** This classification is used to protect the information of political, economic or defence or the information which has a security nature the disclosure of it would cause serious harm to the Sultanate.

c. **Prohibited:** This classification protects the information that should not be included in the categories of (highly confidential) or (confidential) and circulated more widely within the government, but to put in mind the lack of disclosure to unauthorized persons.

d. **Private:** This classification is used to protect the personal information withheld from the staff to keep non-authorized.

Information security

His Excellency, the Minister of Education is fully aware of the need for an effective security system to protect information exchanged between the offices of the Ministry. As a result of the tireless efforts of the Ministry to provide it's entire staff with the latest computer technologies and tools to assist them in their, all efforts are being made to protect information and assets from the dangers that threaten it in order to achieve the following objectives:

- Business continuity
- Reduce environmental risks
- Increase and motivate efficiency in staff

The aspects that must be taken into account on information security:-

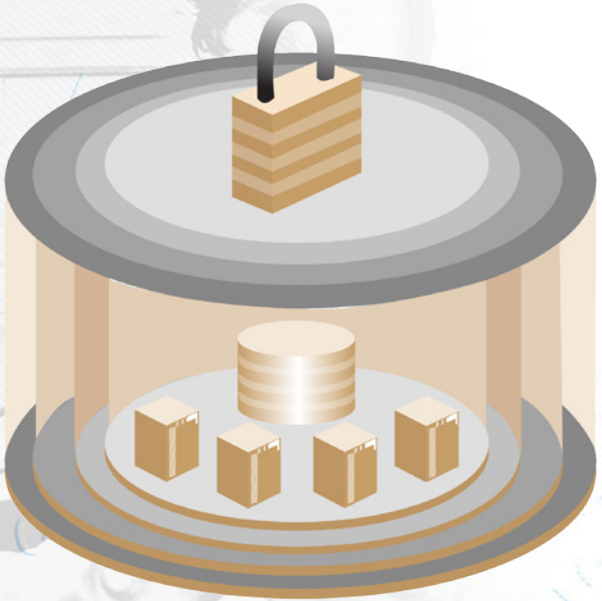
- Information stored in computer files must be password protected. Printed documents must be stored in secure cabinets.



- Do not use live chat software utilities to pass confidential or official documents. Such documents must be sent by an

authorized person in a sealed envelope to the respective department.

- Information store on different forms of media, such as Floppy Disk, CD-ROMs, Printed Matter, etc; and which is no longer required to be kept must be disposed off using the prescribed guidelines of the Ministry Security Department.
- It is strictly forbidden to take confidential material from the ministry unless authorization is give by the security office of the Ministry.



- Proper backup of data on all computers is the responsibility of the staff using that computer. Any information, copied or printed must not be left open. Such information must be stored away after use in secure storage areas in that office. If a staff's computer is to be sent for service, all information considered official and confidential must be properly backed up first and then deleted from the computer before it is sent out of the Ministry premises
- All employees must not discuss or speak on any official topic with unauthorized people.



Use of the Internet

Why do we use the Internet?



Using the Internet in the workplace is primarily for the following reasons:

- Communication between staff and other organizations on relevant matters within the duties and scope of work.
- To gain information for enrichment of job performance and skills to carry out the duties and development.
- To help achieving a fast task complete.
- To obtain and enhance staff knowledge and awareness of emerging technologies related to his work.

Internet Security Policy

- Only authorized employees will get access to the internet.
- Download/upload any files type are not allowed unless having the permission from Information Security Section.



- All the types of chatting are forbidden in MOE unless Authorized.



- User should not leave their name or identification methods, including the address of the used computer, which may still allow others to locate the organization that you work for. As part of our routine security measures, all sites visited are centrally logged.

- User should not engage in any illegal activities using the MOE internet and MOE computer.
- User internet usage should not have a noticeable effect on the availability and network bandwidth.
- User should not participate in online games or have active any web channels that broadcast frequent updates to PC, such as BBC news except the permitted program by the MOE, like LMS.

- User should not visit web sites that display material of a pornographic nature or which contain material that may be considered offensive.



- User should not enter e-mail address on a web site unnecessarily. If giving address when filling in surveys or other questionnaires user may be at risk of receiving unwanted junk messages.

- The person logged on a computer will be considered to be the person browsing the internet. User must log-out from or lock the computer they are away from their desk. Under no circumstances user must not browse the internet from a PC that she/he has not logged into.
- The Network security team monitors and logs all internet users and reserves the right to report to the top management seeking decision.

Password and Email Policy



- Password should be very long, because some create passwords from 5 or 7 letters but it better be more than that.
- Password should contain different symbols, numbers and letters for example. MYO~QM/+_^%BO*ZP37.
- Password should not be a serial numbers or random numbers that you may see them hard but they would be easy for such a program that produces serial or random numbers.
- Password should be far from any real information belongs to you like your phone number, name, city, country, date of birth because some create a password from their country or city then their date of birth and so in the other hand you should make

it far than any information known about you in a forum you participate in even if its related to your faked name.

- You should not trust the person that you are emailing because after some time from your conversations will be able to gather information about you that may help to discover you password.
- Changing password is required from time to time because maybe there will be someone who really got into your email but did not change the password and just waiting to receive an important letter in your mail or might be spying to know more about you ! To check whether your letter has not been read you'll find the headline active and if it would be read already the headline won't be active.
- Never use your office email in your private stuff like participating in special forums or receiving daily news and etc.



- Never use your personal email for sending important data or letters related to work.
- Never use your office email for sending viruses and threats to destroy purpose for others in your office or outside either.

Regulations for the Equipment and Devices section

First article: Applications for Devices

- Every MOE employee has the right to receive a computer with its accessories based on the requirements of his/her work he and according to the specifications of the Technical Support and operation Department.
- Any MOE employee is eligible to receive a laptop if the nature of his/her works

- Requires /demand long working hours outside the premises of MOE. The Technical Support and operation Department will study individual application and provide necessary recommendation.
- All new devices for the staff of all directorates in the regions will be distributed according to the annexed disclosures form the Technical Support and Operation Department.
- MOE employee in any department does not have the right any kind of interference in the distribution of IT devices unless approved by Technical Support and operation Department or Information and Technology Section in the region.
- The Technical Support and Operation Department is Authorized to approve or reject any application .The decision will be based on the nature of employee work in MOE.

Article II: Custody of Devices

- All computer devices and their accessories, given to any employee belong to the Ministry of Education
- The employee is fully responsible of any loss or damage of his/her computer devices and their accessories.
- Computer devices or their accessories are registered with the employee's name and his/her ID in a database represented in the technical support program.
- MOE employees are not permitted to any kind of sharing or exchange of computer
- Devices under any circumstances unless approved by Technical Support and Operation Department or the respected IT department in the region .The employee are fully responsible of otherwise.
- If any employee stopped working temporarily, his \her device remains in his department in MOE, computer devices and their accessories will be and taken back in from employee. The following cases:

a. scholarship

b. Travelling to accompany a student aboard.

c. If the leave period exceeds six months

- Any computer device taken from employee on temporary or long leave through Technical Support and Operation Department in HQ or IT department in the regions
- Will remain in his\her department custody.
- The department of an employee who is on leave can shift his/her device to another employee after receiving an official letter from the requesting department.
- It is prohibited to use any device not adopted by the Information Systems
- An employee who's was on temporary leave and whose device has been transferred to the custody of another employee, can request another device in accordance with the established procedures in the Technical Support and operation Department.

- In the case of changing a desktop computer with a portable computer for any employee, the desktop computer should be returned back to the Technical Support and Operation Department in the HQ or IT Department in the educational regions, or the computer services section in the Supervision offices in the regions.
- Educational directorates or departments that are responsible at any center (i.e. o examination, training centers or computer labs) are not entitled at any point to dispose the devices in the custody of these centers to another centre or transfer the custody to any employee without the consent of the Technical Support and Operation Department in the HQ or IT Department in the educational regions, or the computer services section in the Supervision offices in the regions.
- The computer devices given to any labs or centers are in the custody of the employee and his\her director are fully responsible of these devices, for any deliberate damage, loss transfer or lending without the approval Technical Support and Operation

Department in the HQ or IT Department in the educational regions.

- All damaged device and there need replacing should be listed by the authorized technician in the respected educational regions and should be returned to the educational regions Stores.

Article III: Transferring Devices

- Any device in the custody of an employee is transferred with him/her in case he/she was transferred to another section within the Cabinet the Technical Support and Operation Department in the HQ or IT Department in the educational regions, or the computer services section in the Supervision offices in the regions.
- All the devices in the custody of the employee should be returned to the Technical Support and Operation Department in the HQ or IT Department in the educational regions, or the computer services section in the Supervision offices in the regions.
- All devices in the custody of the employee should be returned back to the computer

services section in the regions in case of transfer of the employee to the ministry or to another educational region or to the supervision offices in the region.

- All devices in the custody of the employee should be returned to the computer services in the region's supervision office in case of transfer of the employee from the supervision office in the region to the directorate headquarter, ministry headquarter or to another region.

Fourth Article: Releasing

- Any employee should not be released permanently or temporarily unless s/he returns all devices and accessories in his custody to the Technical Support and Operation Department in the HQ or IT Department in the educational regions, or the computer services section in the Supervision offices in the regions.
- In case of temporally or permanently termination of employment of any educational director or his\her transfer to

another department ,all computer devices which have been in his\her custody should be handed over to the new director taking place.

Legal texts on how to deal with programs and information

First, the Civil Service Act promulgated by Royal Decree No. 120/2004

Article (103) of the Civil Service Act, which stipulates the following:

The public posts objective is to serve the citizens in the public interest; the employee must take into account the provisions of this Act and other laws and regulations, and must in particular:

a. That the person concerned by the work, should do it accurately and honestly.

b. To maintain the dignity of the post and take the appropriate course of actions.

Article (104), paragraph "b" of the Civil Service Act states that: the employee is prohibited:

Disclosure of matters he suppose to handle and has confidential nature or under the instructions issued by This prohibition will continue to exist after the end of the employment relationship.

Second: The Official Secrets Act and the function of protected areas of Royal Decree No. 36/75:

Article (3) of the Official Secrets Act and the function of protected areas which stipulates the following:

Is that he has committed an offense punishable by the competent judicial authorities to a fine not exceeding twenty riyals or imprisonment for a term not exceeding six months Or both of these, each staff member:

Transfer document or official information to any person or persons other than the person or persons allowed to transfer to them or who impose duties and transfer them.

Or retain any document or official information in the possession or under his supervision to be allowed to do so, or when it is retained in violation of his duties.

Article (4) of the Official Secrets Act provides for the job and places to:

Is that he has committed an offense punishable by the competent judicial authorities a fine of not less than twenty riyals and not more than two

hundred riyals, or imprisonment for a term not exceeding three years, or both together, each staff member:

Transfer any official document or classified information to any person or persons other than the person or persons allowed to transfer to them or who impose duties and transfer them.

Or retain any official information or document in the possession or under his supervision to be allowed to do so, or when it is retained in violation of his duties.

Article (5) of the Official Secrets Act and the function of protected areas provided for:

Each partner or intervening in crimes stipulated in Articles 3 and 4 of this law will be punished as if it were the original offender.

Third: Electronic Transactions Act, promulgated by Royal Decree No. 69/2008

Chapter nine: Penal

Article (52):

Without prejudice to any heavier penalty provided for by the Omani Penal Code or any other law,

shall be punished with imprisonment for a term not exceeding two years and fine not exceeding 5000 RO (five thousand riyals) in one or both of these two penalties:

Purposely causing unauthorized modification of the contents of any computer in order to weaken its effectiveness or to prevent or hinder access to any program or data saved in or weaken the effectiveness of the program or weaken reliance on such statements, if the edit was one of the following ways:

Delete any program or data stored in the computer.

Addition of any program or data to the contents of the computerAny action that cause the modification.

Hack a computer or computer system or Internet sites or the Internet has resulted in this:

Disrupt the operating system of a computer system or computer.

Destruction of software or computers and the content of the information.

Use of the information contained in the outputs of computers for illegal purposes.Entering wrong data.

Entered by fraud or to an information database for the purpose of tampering with electronic signatures.

To illegally disclose encryption keys or to break up the resolution of encoding information credited to him.

Use illegal elements relating to personal encryption signing elsewhere.

Penetration or interception of information or data or the encrypted code, whatever, without legal justification purposely, the penalty is doubled if the information or data concerning the secret of the secrets of the country.

Purposely intended to decrypt the information or data encrypted in any way other than in circumstances permitted by law.

Creation, publication of a certificate or provided incorrect electronic information on purpose for an illegal work.

Submitted incorrect data on the identity or the mandate identity to the provider of certification services in order to request the issuance, cancellation or suspension of the certificate.

Revealing confidential data on purpose without legal title to be able to reach them with its powers under this law or any other law.

Practicing the activity of certification service provider without a license.

Using a tool without a legal permission to create a signature of another person.

The illegal entry to a computer with intent to commit a crime or facilitate the commission of the crime of which done by the same person or by another one.

False electronic record or electronic signature or use any of that with knowledge of fraud.

Purposely intended to publish illegally or to facilitate the dissemination or use of an electronic record or electronic signature or blade and the resolution of the penalty shall be doubled if the offender is faithful to that record or signature in accordance with his or her profession and job.

Article (53):

Without prejudice to any heavier penalty provided by the Omani Penal Code or any other law, shall be punished with imprisonment for a term not exceeding

one year and a fine not exceeding 1500 Omani Rials (One thousand and five hundred Omani Rials) Or with one of these two punishments:

1. Any person that has created acquired or received an information system or program to counterfeit a digital signature without the permission of the owner of the signature.

2. Any ciphering key owner that refused to turn it in to the authorized personal assigned by the authorities.

3. Any certification service provider or one of his colleagues that refused to provide assistance to the assigned authority or one of its personal to monitor, supervise or inspect any computer system, database server or any other equipment related to the computer system in the certification service provider.