Acceptable Use of Assets

Acceptable Use of Assets Policies

1.1. Purpose and Objective:

Purpose of this policy is to define the allowed practices or rules in the organization with subject to use of information Assets/information Systems and Services of MOE to protect from loss, theft, damage, unauthorized- disclosure/modification/copying, misuse to prevent Financial Risk, Legal issues, Operational Risks and Reputational Risks.

1.2. Scope:

The policy applies to all permanent / contractual employees, vendors, suppliers or any third parties irrespective of their position who are using the Assets and Resources of the Ministry.

1.3. Asset Ownership:

The Ministry of education (Oman) is the legal owner of all the Tangible and Intangible Assets and only shall have sole property rights on the assets.

1.4. Acceptable and Non Acceptable Use of Assets:

1.4.1. User will be the custodian of the asset (laptop, mobile phone, IP Phone, Telephones, Tablets, Notebooks, software and Workstation-etc.) which is given to him/her for operational or business use to perform his/her job duties.

1.4.2. No individual should use the Moe resources or assets to engage with any illegal activity or any unlawful conduct, or abuse of Intellectual property or any unauthorized collection and disclosure of personal data or confidential Information of the organization that flouts or breaches the Cyber Crime Law –Royal Decree No 12/2011, Law of copyrights and neighboring rights-Royal Decree no. 65/2008., E-transaction law 69/2008 Article number (43)-Protection of Private Data.

1.4.3. User should only use MOE provisioned licensed software and shall not install or run pirated software on the Assets given to him/her.

1.4.4. Users shall not use Moe resources and assets to copy or reproduce the Copyrighted Material without the written approval from the copyright owner.

1.4.5. No individual should store his/her personal data on the Moe assets which is given to him/her for job related use.

1.4.6. No individual should access any Moe resources or assets or secure areas which He/ She is not authorized to access it.

1.4.7. No individual should hack or destroy, modify or install or run hacking tools or do penetration testing of the network or Application or servers or systems or perform such activities on any assets of MOE.(Exception to this policy statement is only to the authorized department which requires to perform the vulnerability testing or Penetration Testing of the information systems with a written approval from information security officer/Department).

1.4.8. User shall not copy or store the Moe-data or information into their personal media or any third party cloud storage; instead, the user should copy or store the data into the organization's file storage servers.

1.4.9. User shall not share the data or information assets with other departments or any other third parties without the approval from Head of Department or from the Information security Department.

1.4.10. User shall not destroy data or any asset belonging to Moe.

1.4.11. User shall be responsible to immediately report to the information security department for any theft, loss or unauthorized disclosure of MOE assets.

1.4.12. Users shall report technical help desk on detection of virus or any malicious software or any software bugs or malfunctioning of the assets which they are handling.

1.4.13. Users/employees/contractors shall handover or return all the assets upon termination of job/contract or shifting/ transfer to another offices of MOE.

1.4.14. The Head of the department shall make sure the assets are returned when the employee is resigning or shifting from the department and should be documented.

1.5. Use of Secret Authentication Information (Password Policy)

1.5.1. Keep the secret authentication information confidential, ensuring that it is not divulged to any other parties, including the people of authority.

1.5.2. Avoid keeping a record (e.g. on paper, software file or hand-held device) of secret authentication information, unless this can be stored securely and the method of storing has been approved (e.g. password vault).

1.5.3. Users should not give passwords over the phone or through Email.

1.5.4. Change secret authentication information every 60days or whenever there is any indication of its possible compromise.

1.5.5. when passwords are used as secret authentication information, select quality passwords with sufficient minimum length of (8) characters which should have following characteristics:

a) Easy to remember.
b) Should not be based on anything which someone else could easily guess or obtain using a person's related information, e.g. names, telephone numbers and dates of birth etc.
c) Should not be vulnerable to dictionary attacks (i.e. do not consist of words included in dictionaries).
d) Free of consecutive identical, all-numeric or all-alphabetic characters.
e) Password should be combination of one upper letter,special character and a number.
f) If temporary, change at the first log-on;.
g) The password should not be same as the Username.
h) A password should be different from the last 12 passwords.

1.5.6. Never use the same secret authentication information for business and non-business purposes.

1.6. Clear Desk and Clear Screen Policy

The purpose of this policy is to reduce the risk of unauthorized access, loss and damage to information during the time frame when workstations/laptops/servers are left unattended for some time.

1.6.1. Clear Desk Policy

1.6.1.1. Paper and computer removable media shall be stored in suitable locked safes, cabinets, etc.

1.6.1.2. In case of unavailability of lockable safes, cabinets, drawers, etc., then the entrance doors of that location shall be locked if left unattended. At the end of each work session, all sensitive information shall be removed from the work place and stored in a safe place. This includes all personal identifiable information as well as business critical information such as salaries and contracts, etc.

1.6.1.3. Sensitive or classified information should be taken away from printers immediately after printing.

1.6.1.4. Employee or the user desk shall be kept clear at all times; in particular personal records, postal mails or other identifiable information should not be kept on a desk or within the reach/sight of visitors.

1.6.2. Clear Screen Policy

1.6.2.1. Computer terminals shall not be left unattended and shall be locked and should be password protected.

1.6.2.2. If possible, Computer screens shall be angled away from the view of unauthorized persons or passersby.

1.6.2.3. The windows log-on dialog box shall be displayed if the system remains inactive for 5 minutes.

1.6.2.4. Users shall log off from their machines before leaving the premises.

1.7. Information Transfer

1.7.1. All the information related but not limited to the following information should be treated as confidential and shall not be allowed to disclose or transfer or declare or publicize these data or information.

a) Students marks
b) Teachers
c) Parents
d) financial information
e) HR. details
f) Network diagrams
g) Source code
h) Service level agreements

1.7.2. Wireless communication shall not be used for transferring any sensitive information unless the communication is encrypted.

1.7.3. Transferring the information over the Email shall be compliant with Email Policy.

1.7.4. Sensitive information in messages should not be left on answering machines as it can be overheard.

1.8. Mobile Devices

1.8.1. Bring your own Devices (BYOD) or personal electronic devices should not be used or connect to the infrastructure or Network without written approval from the Head of the department.

1.8.2. The mobile devices such as Laptops, mobile phones, tabs-etc given by the Moe for Business purpose should not be kept as check in luggage when flying and should always be with its custodian.

1.8.3. Back up all the critical data on given mobile devices to the Moe backup server.

1.8.4. Encrypt all critical data on mobile devices.

1.8.5. User should use Remote wiping feature of data in mobile phones in case of the theft or loss of the device to prevent the risk of loss of critical data to unauthorized persons.

1.8.6. Users should make sure the End point security is installed and enabled on the mobile device which is given to them.

1.9. Internet Usage Policy

1.9.1. Only official Internet connections should be used. No individual is allowed to connect to the Internet through a PC or 3G or 4G modem, as this would open an unsecured backdoor to MOE.

1.9.2. Internet facilities will be provided only to those employees who need them for business use. No Internet usage for personal purposes will be facilitated.

1.9.3. While using the Internet, no individual should abuse, defame, stalk, harass or threaten any other person that violates local laws and Regulations.

1.9.4. No individual should view, upload, download, post, publish or distribute any inappropriate, indecent, pornography, obscene, movies, profane, infringing, defamatory or unlawful information or material on the Internet while using the organization resources.

1.9.5. No individual is allowed to post personal advertisements or offer any goods or services using MOE resources.

1.9.6. A visit to any obscene or socially unacceptable site will be considered as a serious offence will be referred to legal department as per cybercrime law.

1.9.7. No individual should use Moe-internet services to make personal financial transaction.

1.10. E-Mail Usage Policy

1.10.1. The e-mail facility is for business use only. The e-mail address allocated to an employee should not be used for personal purposes.

1.10.2. The employee or the user shall not use email system for harassing or defaming anybody.

1.10.3. Non-business-related newsgroup should not be added to MOE e-mail address book.

1.10.4. NO user or individual is allowed to use Email facility to forward or send spam, scam or Malicious files to others users, whether inside or outside MOE.

1.10.5. No harassing or insulting messages or abuse emails should be sent inside or outside of MOE.

1.10.6. Information or data belonging to MOE should not be sent to his/her personal account.

1.10.7. Any confidential data, Sensitive data or attachments or Documents belongs to MOE should not be sent through Email; instead the employees should use MOE internal Correspondence system for this purpose.

1.10.8. If sensitive information needs to be sent to someone outside MOE, proper measures should be taken as specified by the Information Security Officer.

1.10.9. The user should backup all his/her Emails for his/her email account.

1.10.10. The email account creation is only by the approval from the head of the Department and shall be removed when the employee or the user gets his duties released from the MOE.

1.10.11. The email reply shall be only to the person or individual or group to whom the information is intended.

1.10.12. All the MOE Email users should use disclaimer “This message is intended only for the individual named. If you are not the named addressee, you should not disseminate, distribute or copy this e-mail. Please notify the sender immediately by e-mail if you have received this e-mail by mistake and delete this email from your system “.

1.10.13. Users are prohibited from using third-party email systems and storage servers such as Google, Yahoo, and MSN Hotmail etc. to conduct business transactions.

1.10.14. MOE is the sole owner of all the Moe domain emails (@moe.om and @moe.gov.om) and employees shall have no expectation of privacy in anything they store, send or receive on the MOE email system.