FUTURE METTLE
PRIVATE VOCATIONAL
TRAINING INSTITUTE

Data Protection Policy

1. Introduction

Future Mettle Training institute in the Sultanate of Oman approved and regulated by the Ministry of Higher Education, Research, and Innovation Sultanate of Oman. FMI recognizes it has a major role to play in achieving high Quality of Standards in educating its trainees to achieve the necessary skills and underpinning knowledge to contribute to the Sultanate's economic and social development plans.

2. Purpose

FMI recognizes standardization of policies and practices as essential to an efficient system. It is the intent of this policy to establish guidelines for the eligible users (Employees and Trainees) using the FMI computing facilities, including computer hardware, printers, software, email, and Internet and intranet access, collectively called "Information Technology".

3. Policy Statements

- All eligible users share the Information Technology facilities at FMI.
- These facilities are provided to eligible users for the purpose of conducting FMI training operation and training operation activities. The Institute does permit a limited amount of personal use of these facilities, including computers, printers, email, and Internet access. However, these facilities must be used responsibly by everyone, since misuse by even a few individuals has the potential to negatively impact productivity, disrupt Institute business and interfere with the work or rights of others. Therefore, all eligible users are expected to exercise responsible and ethical behavior when using the FMI Information Technology facilities.

- The use of the FMI information technology facilities in connection with Institute business and limited personal use is a privilege but not a right, extended to various FMI Users. Users also agree to comply with applicable country and local laws and to refrain from engaging in any activity that would subject the Institute to any liability.

- To protect the integrity of FMI's computing facilities and its users against unauthorized or improper use of those facilities, and to investigate possible use of those facilities in violation of rules and policies, FMI reserves the right, without notice, to limit or restrict any individual's use, and to inspect, copy, remove, or otherwise alter any data, file, or system resource which may undermine the authorized use of any computing facility, or which is used in violation of rules or policies.

- FMI also reserves the right periodically to examine any system and other usage and authorization history as necessary to protect its computing facilities.

- FMI disclaims any responsibility for loss of data or interference with files resulting from its efforts to maintain the privacy and security of those computing facilities or from system malfunction or any other cause.

These policies cover the usage of all of the FMI's Information Technology resources, including, but not limited to:

I. All computer related equipment, including desktop personal computers (PCs), portable PCs, terminals, workstations, wireless computing devices, telecom equipment, networks, databases, printers, servers and shared computers, and all networks and hardware to which this equipment is connected

II. All electronic communications equipment, including telephones, email, wired or wireless communications devices and services, Internet and intranet and other online services

III. All software including purchased or licensed business software applications, FMI written applications, employee or vendor/supplier written applications, computer operating systems, firmware, and any other software residing on Institute owned equipment

IV. All intellectual property and other data stored on FMI equipment

V. All of the above are included whether they are owned or leased by the Institute or are under the Institute possession, custody, or control

VI. These policies also apply to all users, whether on FMI property, connected from remote via any networked connection, or using FMI IT equipment and resources.

3.1 IT Guidelines

These guidelines apply to all IT users of FMI using the IT facilities of hardware, software and Networks provided by the Institute.

3.1.1 Access

- Each eligible user will be given a login Id and Password. This will allow the user to enter into the Institute network to store and access files and other network resources. Once logged in the system, it will allow the user to store files in the private file area Home folder
- (H drive).
- The users should keep the login ID and Password secure.
- The users are allowed to login only with their login ID and password.

3.1.2 Network

- Users are strictly prohibited from physically tampering with network connections/equipment, sending disruptive signals, or making excessive use of network resources.

- The Users are not allowed to do any changes in the computer accessories and equipment like Computer Network cabling, access point, router, mouse, Keyboards etc.

3.1.3 Data Storage, Backup and Recovery

- All staff and trainees are requested to store important documents in the Home folder (H drive) in the server which will be backed up regularly to avoid any data loss.
- All organizational information must be stored on the Institute network. Users must not store organizational information on individual computers or devices unless exceptional circumstances apply, following advice from IT department. The IT department staff should back up the files and information stored on the network to ensure it is available for use as and when required. As a safety measure, monthly backup is sent to external storage location(offsite).

3.1.4 Destruction and disposal of equipment

Any equipment or media used to store personal data or other organizational information must be disposed of securely and in a sustainable way. No equipment or media containing or used to access organizational information must be disposed of or sent for resale without ensuring that all information has been removed and is irrecoverable.

3.1.5 Social Networking

Social networking facilities such as Facebook ,Twitter and LinkedIn are used for official purposes as well as privately by employees in a personal capacity. Employees must not use their Institute email addresses on their private social media accounts as this may compromise the security and privacy of the FMI email system and the information it contains. The information in the social media is updated regularly to ensure the viewers will get the updated information.

3.1.6 Privacy

- Users should not intrude on privacy of other users. Users are prohibited to access others computer, files, documents, information without their approval.

3.1.7 Virus

- Users should be aware of the need to protect FMI network and computers from virus and spam mails. If the user suspects the mail is infected or attachment from unreliable source, it has to be deleted without opening it.
- User should attempt to keep the computer free from viruses, worms, Trojans, and other similar programs by not using infected devices and downloading malicious software.

3.1.8 Software

- Unauthorized copying of any software or documents owned by FMI are prohibited

- Installing software which are not useful for the FMI are prohibited.
- Downloading movies, songs are prohibited unless it is approved by the IT Department.
- Software's licensed to FMI should be used only for academic purposes and not to be shared with anyone.

3.1.9 Email

- The Users should use the email facility mainly for the official , purpose.
- Unsolicited mailings, unauthorized mass mailings, Spoofing from the FMI network/email system are prohibited.
- The Users are prohibited to use email system or other FMI IT facilities to harass, spoofing, annoy other users.

3.1.10 Security Best Practice

The following guidelines are helpful for the users:

- Lock your screen (using CTRL+ALT+DEL) when leaving your computer unattended for a short time.
- Log off computers when you have finished using system.
- Keep your password confidential and make sure it is not easy for others to guess easily.
- Never leave any computing equipment including laptops, notebooks, USBs, or external storage disks anywhere they can be accessed by others or stolen.

- Beware of emails like lottery, request personal details such as account names, account number and passwords they could be scams.

3.2 IT Procedures

3.2.1 Creation of staff accounts

The User accounts are created once their appointment is processed through the HR & Administration Department and communicated to IT Department by the Department Head. On request staff can obtain permission from IT section for accessing email account through outlook web access from outside the Institute. Learners can access their email from FMI as well as from outside through outlook web access.

3.2.2 Staff Password

The password initially created by the IT Department can be changed by the User at any point of time.

3.2.3 Access to IT Facilities

Once an account is created the User can access emails and communicate with others. They will be added in the All-Users list and the department distribution list and any other list to which the user belongs. The staff and learners can access their Home folder in the server to store important documents.

3.2.4 Creation of Learner Accounts

New Learner accounts are created after the learner ID is created and after completing enrollment fees.

3.2.5 Resetting Passwords

Account holders who forget their password, can have their password reset by the IT department. The Head of IT Services is responsible for the process of resetting passwords for both learner and staff accounts.

3.2.6 Disabling and deletion of accounts

The network login account will be disabled after 1 week when a member of staff resigns from the Institute and will be deactivated after 2 months. For the learners who exit FMI, the login account will be deactivated after 2 months.

3.2.7 Reporting of Service, Security, connectivity Issues

All Users are responsible to

- Report any IT issues, security weakness or threat and network connectivity to the IT department.
- Report lost, stolen or non-working computers or other IT equipment to the IT department as soon as possible.
- It is the responsibility of the IT department to attend to the Reporting Call and solve the issue at the earliest.

3.2.8 Data Security

The FMI maintains its IT Resources and facilities in such a way that its IT facilities and data are protected from the following:

- Malicious damage or any activity undertaken to purposely bypass security controls intrusion on Institute IT facilities,
- Spam emails, virus infection and malicious software
- The Institute maintains its IT facilities and data in such a way that they are
- Accurate, secured, and complete,
- Available and accessed only by authorized Users, when required, and
- Recovered as soon as practicable in the event of Hardware failures or disasters.

3.2.9 Disaster prevention

Disaster prevention is concerned with preventing a disaster from ever happening or at least minimizing its effects if one does occur. The following precautions must be implemented to mitigate disaster impact:

- Data back-up systems must be fully implemented, be tested regularly and be available for use if files need to be restored. There is no benefit to creating a back-up file of valuable data if this information is not transferred via a secure method and stored in an offsite data storage center with foolproof protection. As a security measure the backup of the documents, emails database is backed up and sent to offsite every month. Backup is also taken on a daily basis and kept in the server room.

- The servers and networking equipment are located in secure locked rooms to which access is restricted to authorized persons.
- Critical equipment must be covered by Uninterruptible Power Supplies to protect against power supply problems.
- Appropriate fire detection/prevention systems will be installed in the server computer rooms.

3.2.10 Business continuity planning

A Business Contingency Plan has been formulated to ensure key personnel and resources are available to expedite recovery when a disaster does occur.

- Inform the employees about the disaster occurred and tentative time required to recover
- Inform the key staff about the procedure to access the email externally
- Keep the backup tapes and necessary software ready
- Inform the support Engineers
- Make necessary installation, changes in the configuration files etc.
- Testing for few users
- Inform the employees about the recovery once completed

3.2.11 Assessments

vocational training Assessments ,the information is kept in the server with high level security permissions.

4 Breaches of Policy

Any action that may expose FMI to risks of unauthorized access to data, disclosure of information, legal liability, potential system failure or intentional damage to FMI IT resources are prohibited and may result in disciplinary action up to and including termination of employment and/or criminal prosecution.